

What is Information Security ?

- Protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction.

(SANS)

What is Information Security ?

- **IT Security** is information security applied to technology
- **Information security** also covers physical security, human resource security, legal & compliance, organizational, and process related aspects

What is Information Security ?

- **IT Security functions:**
 - Network security
 - Systems security
 - Application & database security
 - Mobile security
- **InfoSec functions:**
 - Governance
 - Policies & procedures
 - Risk management
 - Performance reviews

What is Information Security ?

Cybersecurity is the protection of internet-connected systems such as hardware, software and data from cyberthreats. The practice is used by individuals and enterprises to protect against unauthorized access to data centers and other computerized systems.

- **What is Cyber Security ?**
 - Precautions taken to guard against unauthorized access to data (in electronic form) or information systems connected to the internet
 - Prevention of crime related to the internet

What is Information Security ?

- Three Pillars of Information Security:
 - **Confidentiality:** keeping information secret
 - **Integrity:** keeping information in its original form
 - **Availability:** keeping information and information systems available for use

Why Is Information Security Needed ?

- **Bangladesh Bank SWIFT Hack – Feb 2016:** Hackers used SWIFT credentials of Bangladesh Central Bank employees to send more than three dozen fraudulent money transfer requests

REF: WIRED.COM

Why Is Information Security Needed ?

Contd...

- Requests sent to the Federal Reserve Bank of New York asking the bank to transfer millions of the Bangladesh Bank's funds to bank accounts in the Philippines, Sri Lanka and other parts of Asia.
- USD 81 million stolen
- Total impact could have been USD 1 billion

Why Is Information Security Needed ?

NHS

Recent Cyber Attack – May 2017

NHS cyberattack is 'biggest ransomware outbreak in history'

The NHS hack using Wanna Decryptor ransomware has shut down IT systems with 75,000 attacks in 99 countries

Ransomware attack hits 99 countries with UK hospitals among targets – live updates

Why Is Information Security Needed?



Screenshot of the suspected ransomware message on a GP's computer in the Greater Preston area CREDIT: PA

Why Is Information Security Needed ?

- **The Importance Of Information**
 - IT is pervasive in our society & critical to the Ops & Mngmt of all organizations
 - IT is an enabler for business and govt
 - Personal information is vital for individuals to function in society
 - Information holds value

Why Is Information Security Needed ?

IMPORTANCE OF INFORMATION SECURITY

Top 3 most commonly reported types of economic crime in 2016



- As per PWC Global Economic Crime Report 2016, Cyber Crime was amongst the top 3 most commonly reported types of economic crime

- As per Europol 2013 report, Cyber Crime is now more profitable than the drug trade

EUROPOL

Home | Cookies | FAQ | Sitemap | Contact

Enter search terms

As reported by the 2013 Europol Serious & Organized Threat Assessment, the "Total Global Impact of CyberCrime [has risen to] US \$3 Trillion, making it more profitable than the global trade in marijuana, cocaine and heroin combined."

MEDIA CORNER

Europol Media Corner

Press releases

News

Events

Home - Media Corner - Corporate Publications - EU Serious and Organized Crime Threat Assessment (SOCTA 2013)

EU SERIOUS AND ORGANISED CRIME THREAT ASSESSMENT (SOCTA 2013)

19 March 2013

Who Is Information Security For ?

- **Personal:**
 - Social media passwords and safe usage
 - Online banking and email account passwords
 - Home PC/laptop security
 - Mobile security

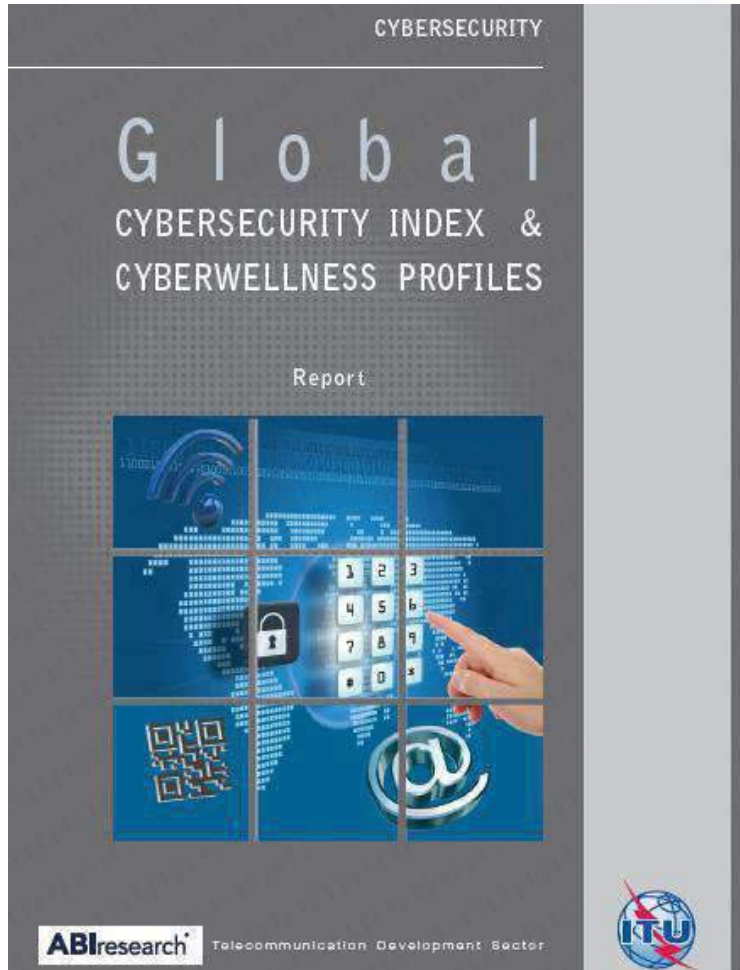
Who Is Information Security For ?

- **Organizational:**
 - Board and executive leadership (management commitment)
 - CISO (responsible to drive security program)
 - IT staff and business users (following information security policies & procedures)

Who Is Information Security For ?

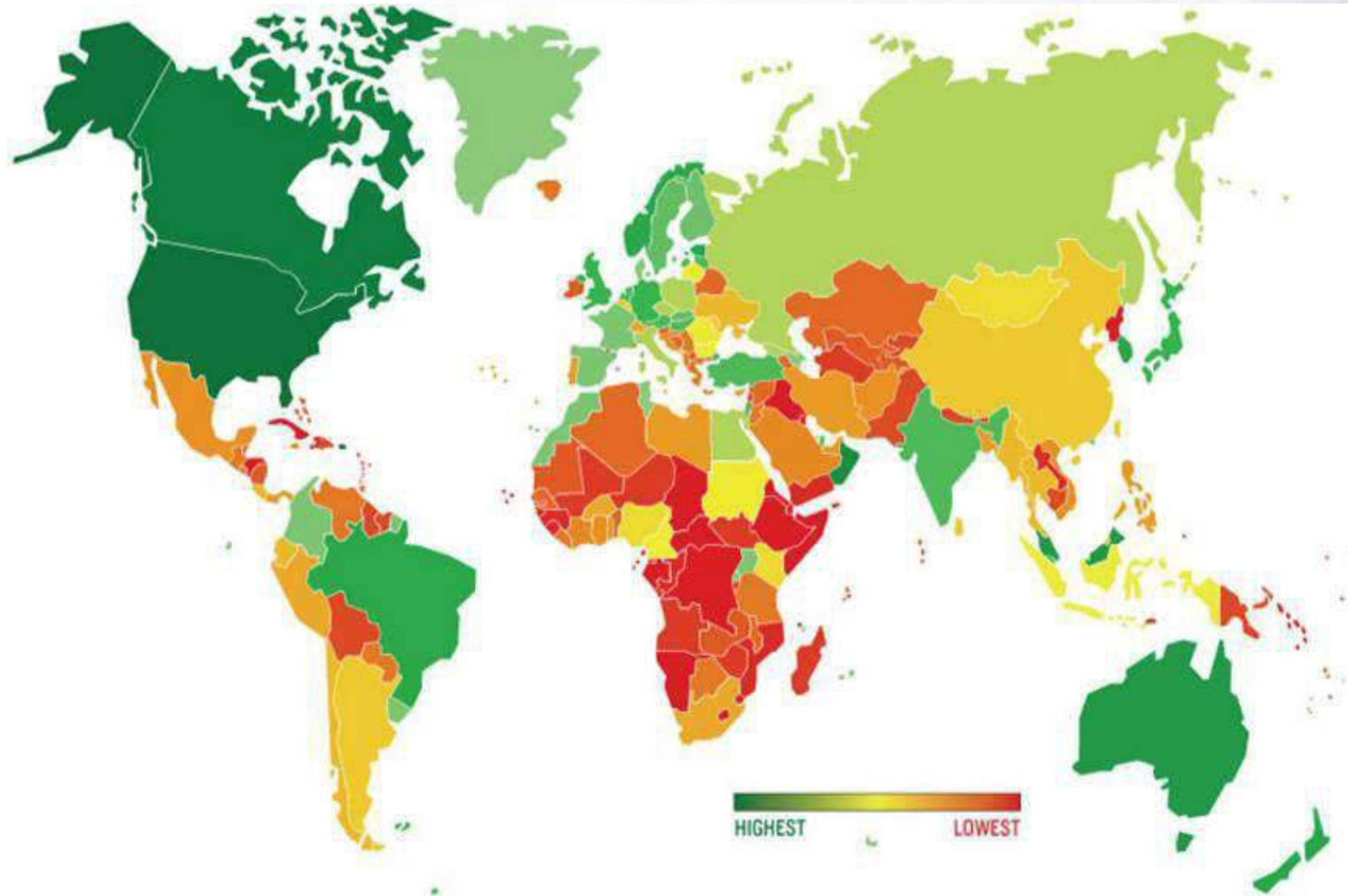
- **Govt and national:**
 - Law enforcement
 - Legal and policy making
 - National database
 - Critical infrastructure
 - Regulation
 - Standards and certification
 - Capacity-building and coordination

Who Is Information Security For ?

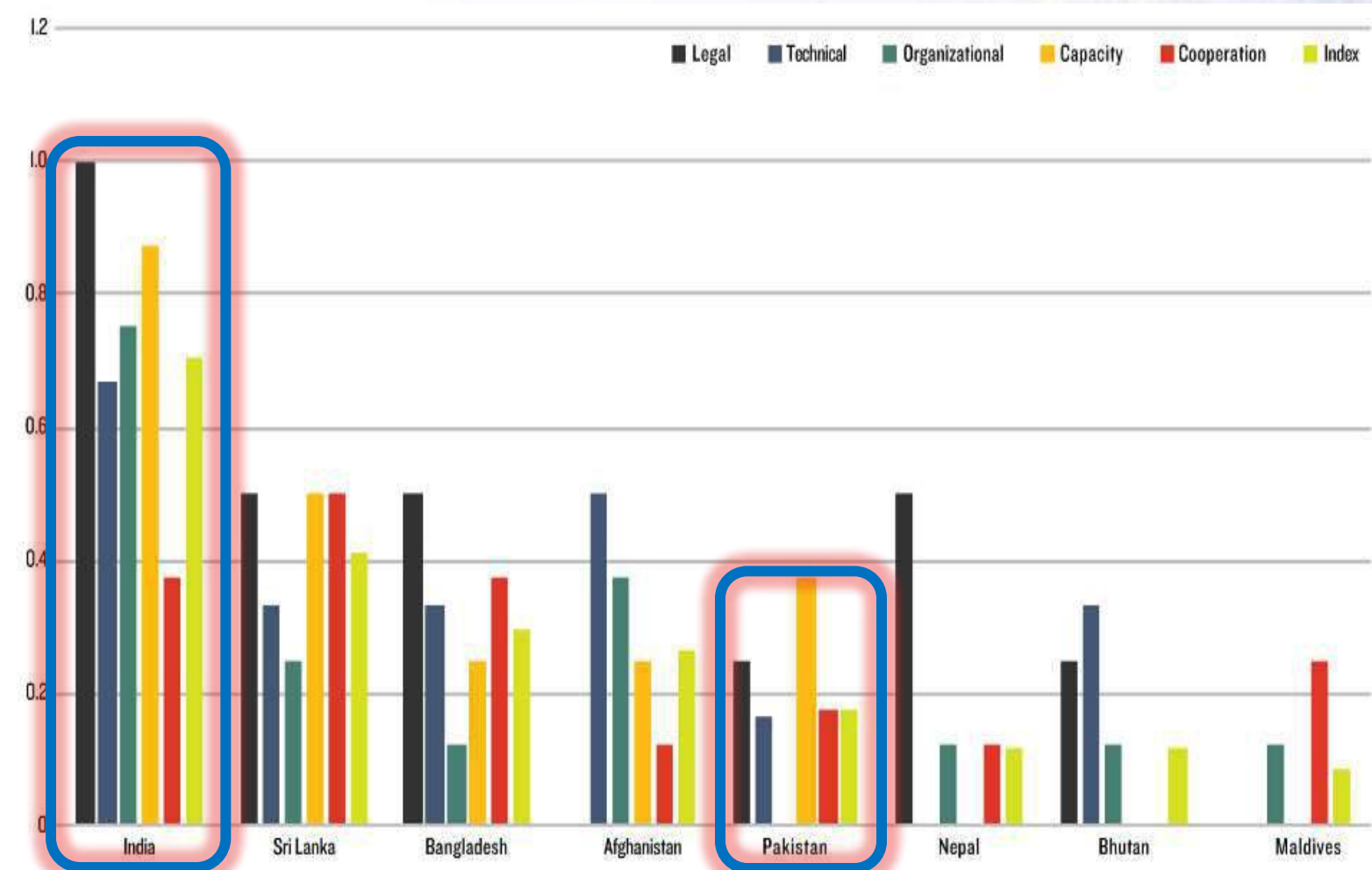


- Legal
- Technical
- Organizational
- Capacity building
- Cooperation

Who Is Information Security For ?



Who Is Information Security For ?



Source: ABI Research, ITU, Global Security Index

Who Is Information Security For ?

International Telecommunication Union

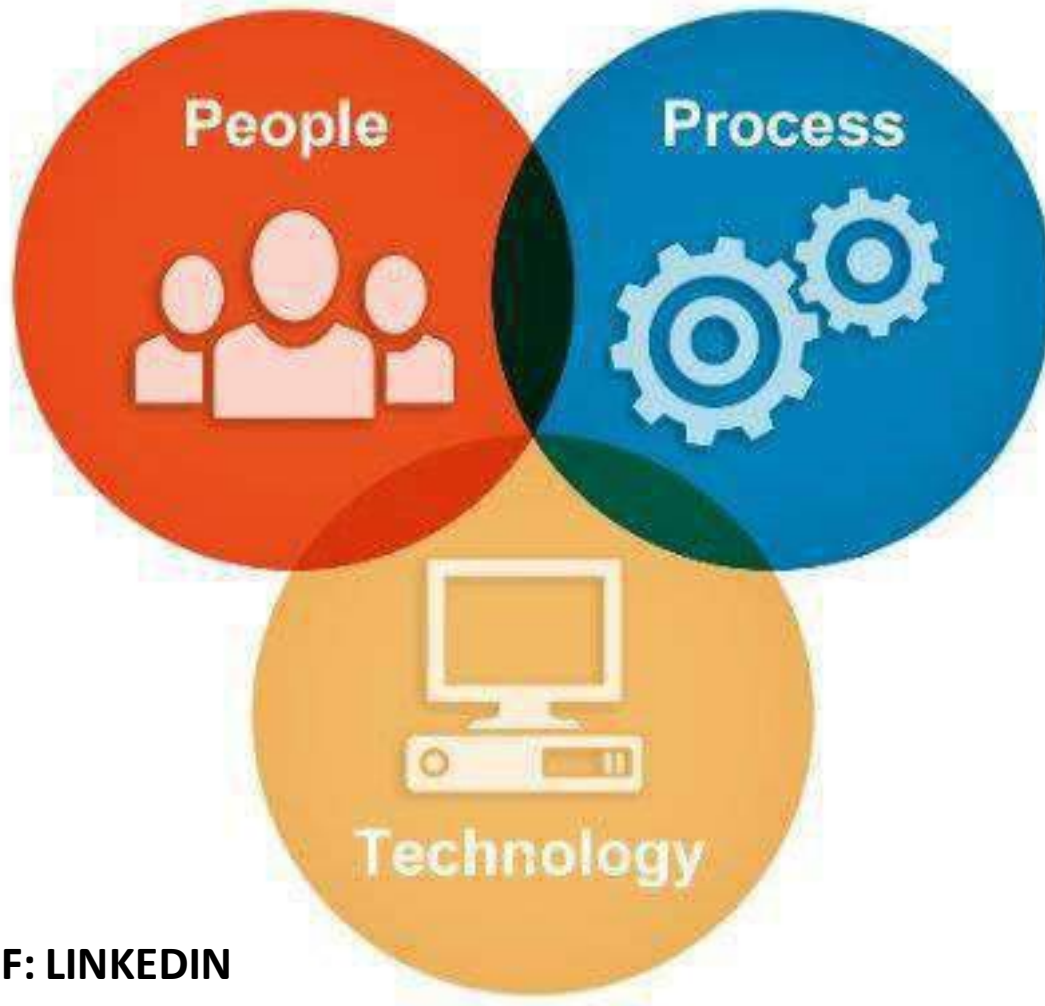
END

- Pakistan ranked almost at the bottom of the table in International ranking by ITU
- Information security is everyone's responsibility
- Pakistan Cyber Security Association (PCSA) formed to address Pakistan's international ranking

How Is Information Security Implemented?

- Three pillars of information security:
 - People
 - Process
 - Technology

How Is Information Security Implemented?



REF: LINKEDIN

How Is Information Security Implemented?

used to define a company's management and board of director's leadership and their commitment to being honest and ethical.

- **Leadership commitment:**
 - “Tone at the top”
 - Information security policy and objectives
 - Assigning responsibility and authority
 - Resource allocation
 - Performance reviews
 - Ensuring accountability

How Is Information Security Implemented?

chief information security officer

- **Information Security Manager or CISO:**
 - Heads department responsible for implementing information security program
 - Directs planning, implementation, measurement, review, and continual improvement of program

How Is Information Security Implemented?

- **IT user:**
 - Understand policies
 - Conduct security/risk assessment
 - Design effective security architecture
 - Develop SOPs and checklists
 - Implement controls
 - Report incidents
 - Conduct effective change management

How Is Information Security Implemented?

- **Business user:**
 - Security awareness and training
 - Follow information security policy
 - Develop and implement secure business processes
 - Role-based access control and periodic reviews
 - Reporting incidents

How Is Information Security Implemented?

- **Information security program**
 - Assessing security risks and gaps
 - Implementing security controls
 - Monitoring, measurement, & analysis
 - Management reviews and internal audit
 - Accreditation/testing

END

Who Are The Players In Information Security ?

- Government
- Industry & sectors
- International organizations
- Professional associations
- Academia and research organizations
- Vendors and suppliers

Who Are The Players In Information Security ?

- **Government:**
 - Policy making
 - Law enforcement
 - Legal system
 - National cyber security strategy and standards
 - International coordination
 - Computer Incident Response Team (CIRT)

Who Are The Players In Information Security ?

- **Industry & sectors:**
 - Financial institutions
 - Telecoms
 - Armed forces
 - Federal and provincial IT boards
 - Enterprises
 - Various other sectors (manufacturing, automotive, health, insurance, etc)

Who Are The Players In Information Security ?

The Asia Pacific Computer Emergency Response Team (APCERT) is a forum for national and non-national Computer Security Incident Response Teams (CSIRTs) and Computer Emergency Response Teams (CERTs) within the Asia Pacific region to foster information sharing and collaboration on cyber security.

ENISA is actively contributing to a high level of network and information security (NIS) within the Union, thus contributing to proper functioning of the internal market. The Agency was established in 2004 and is based in Crete, Greece.

- **International organizations:**
 - APCERT
(www.apcert.org)
 - European Union Agency for Network & Information Security - ENISA
(www.enisa.org)

Who Are The Players In Information Security ?

- **International organizations:**
 - ITU IMPACT
(<http://www.impact-alliance.org>)

<https://www.itic.org/dotAsset/c/c/cc91d83a-e8a9-40ac-8d75-0f544ba41a71.pdf>

Who Are The Players In Information Security ?

Information Systems Audit and Control Association®, ISACA now goes only by its acronym to reflect the broad range of IT governance professionals we serve. Today, ISACA's constituency of more than 165,000 strong worldwide is characterized by its diversity.

International Information Systems Security Certification Consortium, more commonly known as (ISC)2, is a non-profit organization that provides security training and certificates.

- **Professional associations:**
 - ISACA (isaca.org)
 - ISC2 (www.isc2.org)
 - OWASP (www.owasp.org)
 - Cloud Security Alliance
 - Pakistan Cyber Security Association (PCSA)

<http://cybersecurityventures.com/cybersecurity-associations/>

Who Are The Players In Information Security ?

SysAdmin, Audit, Network and Security

- **Academia & research organizations:**
 - Universities and research programs
 - SANS
(www.sans.org)
 - Center for Internet Security
(www.cisecurity.org)

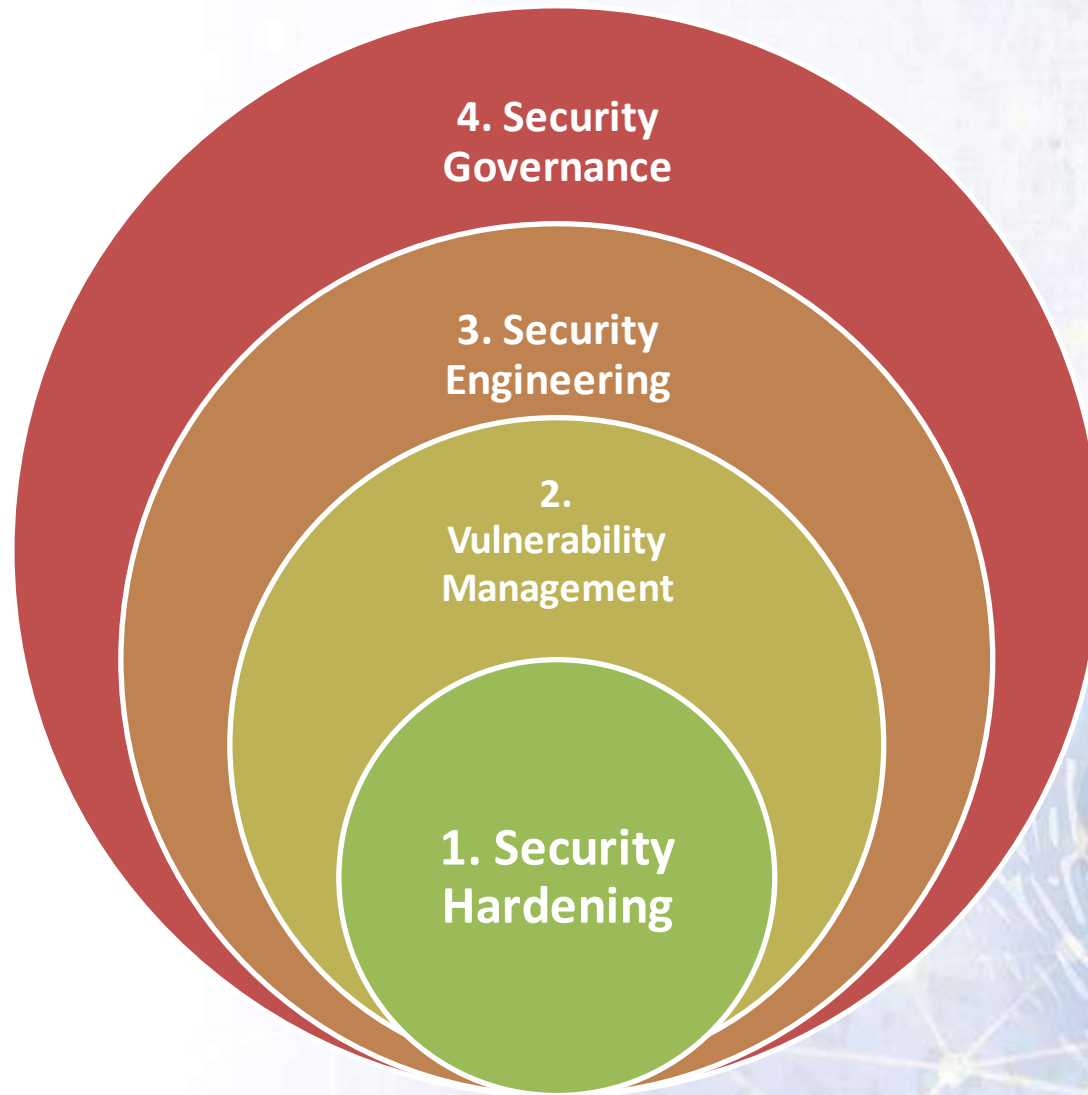
END

<http://cybersecurityventures.com/cybersecurity-associations/>

Infosec Transformation Framework 4 Layers

1. Security hardening
2. Vulnerability management
3. Security engineering
4. Security governance

Infosec Transformation Framework 4 Layers



Infosec Transformation Framework 4 Layers

- **1: Security hardening:**
 - Compile IT assets
 - Establish minimum security baseline (MSB)
 - Research security controls and benchmarks
 - Pilot (test)
 - Implement controls
 - Monitor and update controls

Infosec Transformation Framework 4 Layers

- **2: Vulnerability management:**
 - Purchase internal tool (NESSUS, Qualys, etc)
 - Conduct vulnerability assessment
 - Prioritize and remediate
 - Report
 - Repeat cycle on quarterly/monthly basis

Infosec Transformation Framework 4 Layers

- **3: Security engineering:**
 - Assess risk profile
 - Research security solutions
 - Design security architecture
 - Implement security controls & solutions
 - Test and validate security posture

Infosec Transformation Framework 4 Layers

- **4: Security governance:**
 - Policies and procedures
 - Risk management
 - Core governance activities (change management, incident management, internal audit)
 - Training & awareness
 - Performance reviews

END

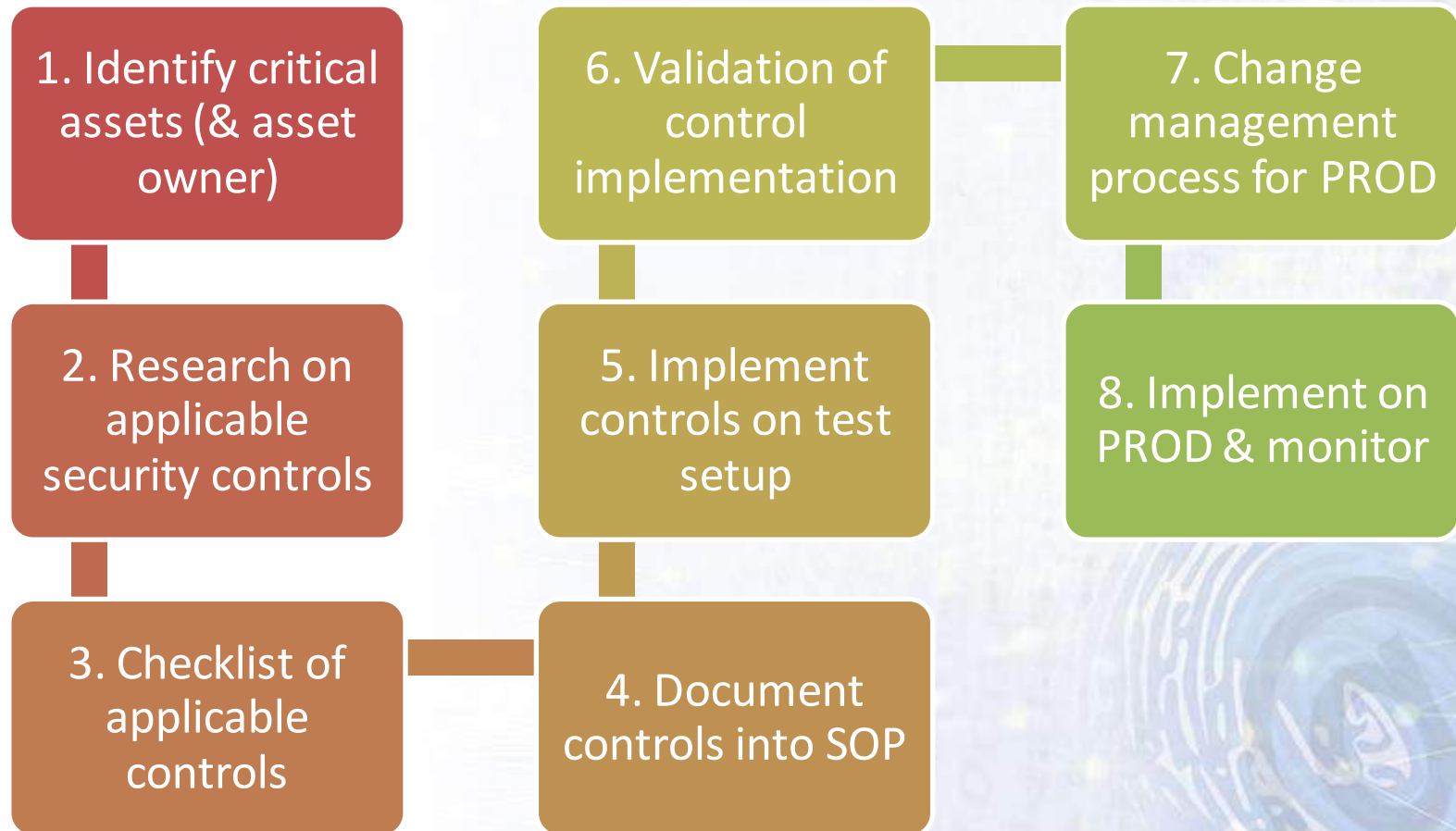
What Is Information Security Hardening?

- **IT assets** (network, systems, application, databases, mobile, physical security) come with default settings which are not suitable for security
- **Security hardening** is the process of configuring IT assets to maximize security of the IT asset and minimize security risks

What Is Information Security Hardening?

- **Security in the “trenches:”**
 - Security at the most fundamental operational layer
 - Security where it matters most
 - Usually (but not always) involves junior staff who need extra guidance, training, and scrutiny

What Is Information Security Hardening?



What Is Information Security Hardening?

- **Why is security hardening at the first step in the security transformation model?**
 - Most basic security settings
 - If not adequately addressed here, rest of the security measures hardly matter

What Is Information Security Hardening?

- **Short example of Cisco router security hardening:**
 - Remote access through SSH and not through telnet
 - Turn of all unused services
 - Session timeout and password retry lockout

<http://www.cisco.com/c/en/us/support/docs/ip/access-lists/13608-21.html>

What Is Information Security Governance ?

- Information security governance in simpler terms just means effective management of the security program
- Responsibility for governance is associated with the Board and senior management

What Is Information Security Governance ?

- **IT Governance Institute Definition:**
 - "Security governance is the set of responsibilities and practices exercised by the board and executive management, with the goal of providing strategic direction,...

What Is Information Security Governance ?

- **IT Governance Institute Definition (contd.):**
 - “... ensuring that objectives are achieved, ascertaining that risks are managed appropriately and verifying that the enterprise's resources are used responsibly.”

What Is Information Security Governance ?

- **ISO27001:2013 – ISMS (Information Security Management System)** is the world's leading and most widely adopted security governance standard



What Is Information Security Governance ?

- **ISO27001** "provides a model for establishing, implementing, operating, monitoring, reviewing, maintaining and improving an information security management system."

What Is Information Security Governance ?

- Ten short clauses and a long Annex with 114 controls in 14 groups
- 27000+ certifications globally in 2015

Difference Between Policy, SOP, & Guideline

- **Policy:**
 - Formal and high level requirement for securing the organization and its IT assets (mandatory)

Difference Between Policy, SOP, & Guideline

GUIDELINE

[provides additional, recommended guidance]

PROCEDURE

[establishes proper steps to take]

STANDARD

[assigns quantifiable measures]

POLICY

[identifies issue & scope]

**How Do
I Do It?**

**What Is
Required?**

**Why Do I
Need To Do This?**

<https://www.linkedin.com/pulse/20140611162901-223517409-difference-between-guideline-procedure-standard-and-policy>

Difference Between Policy, SOP, & Guideline

- **Policy:**
 - Scope is across organization so should be brief and focusing on desired results
 - Signed off by senior management

Difference Between Policy, SOP, & Guideline

- **Procedure / SOP:**
 - More detailed description of the process; who does what, when, and how
 - Scope is predominantly at a department level having specified audience
 - May be signed off by departmental head

<https://www.slu.edu/its/policies>

Difference Between Policy, SOP, & Guideline

- **Guideline:**
 - General recommendation or statement of best practice
 - Not mandatory
 - Further elaborates the related SOP

<https://www.slu.edu/its/policies>

Difference Between Policy, SOP, & Guideline

- **Standard:**
 - Specific and mandatory action or rule
 - Must include one or more specifications for an IT asset or behavior
 - Yardstick to help achieve the policy goals

<https://www.slu.edu/its/policies>

Difference Between Policy, SOP, & Guideline

- **In practice:**
 - Policy recommended to be a single document applicable at the organizational level (wide audience)
 - Sub-policies may be defined at a departmental level
 - Policies and standards are mandatory (exception approval)

Difference Between Policy, SOP, & Guideline

- **Examples:**
 - Information security policy
 - System administrator password sub-policy
 - User ID & Access Management SOP
 - Vulnerability Management standard
 - Social engineering prevention guideline

What Is An Information Security Program ?

- **Project definition:**
 - A project has a defined start and end point and specific objectives that, when attained, signify completion

pmtips.net/blog-new/difference-projects-programmes

What Is An Information Security Program ?

- **Program definition:**
 - A program is defined as a group of related projects managed in a coordinated way to obtain benefits not available from managing the projects individually

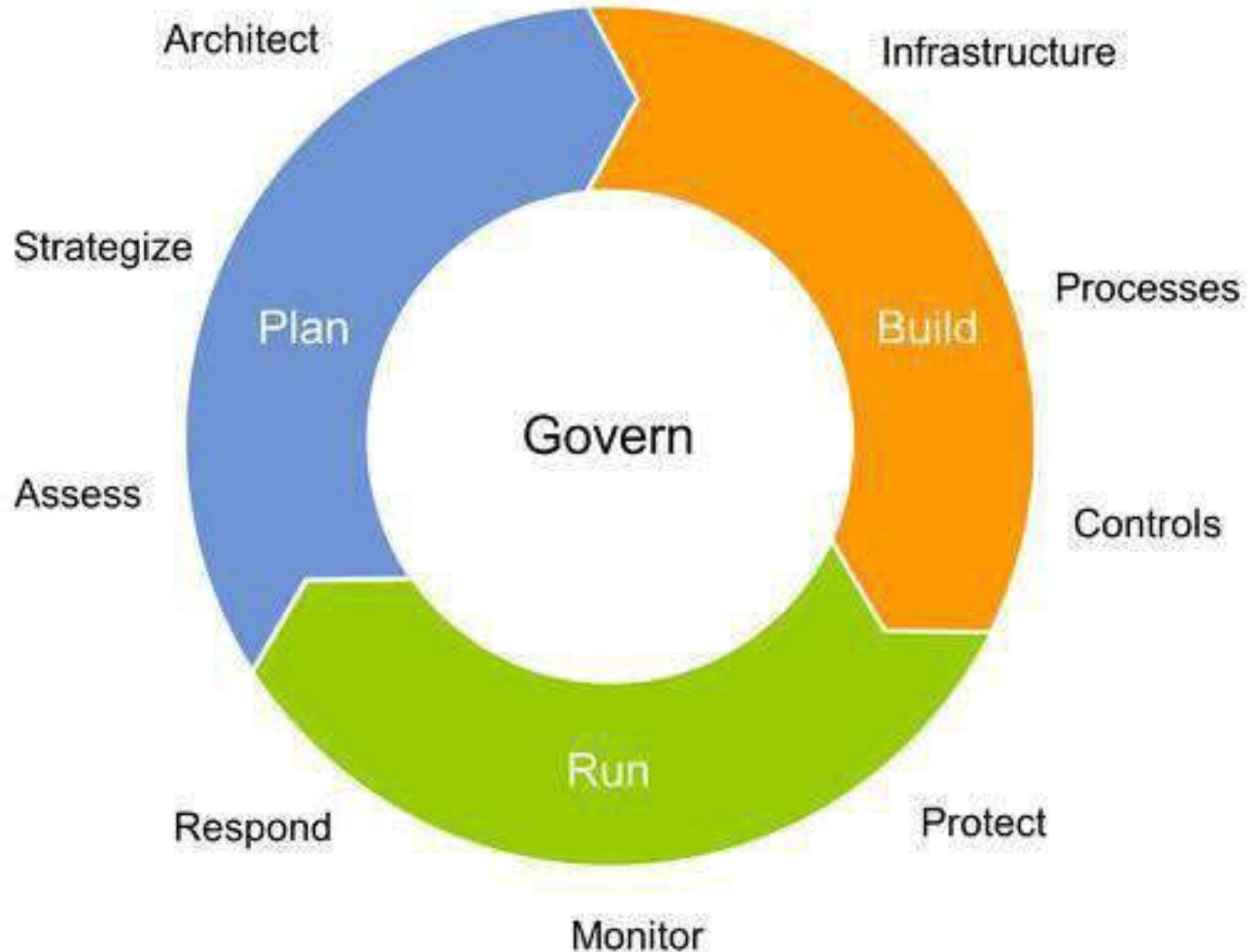
pmtips.net/blog-new/difference-projects-programmes

What Is An Information Security Program ?

- **Security program:**
 - Sum-total of all activities planned and executed by the organization to meet its security objectives

pmtips.net/blog-new/difference-projects-programmes

What Is An Information Security Program?



<https://www.gartner.com/doc/2708617/information-security-program-management-key>

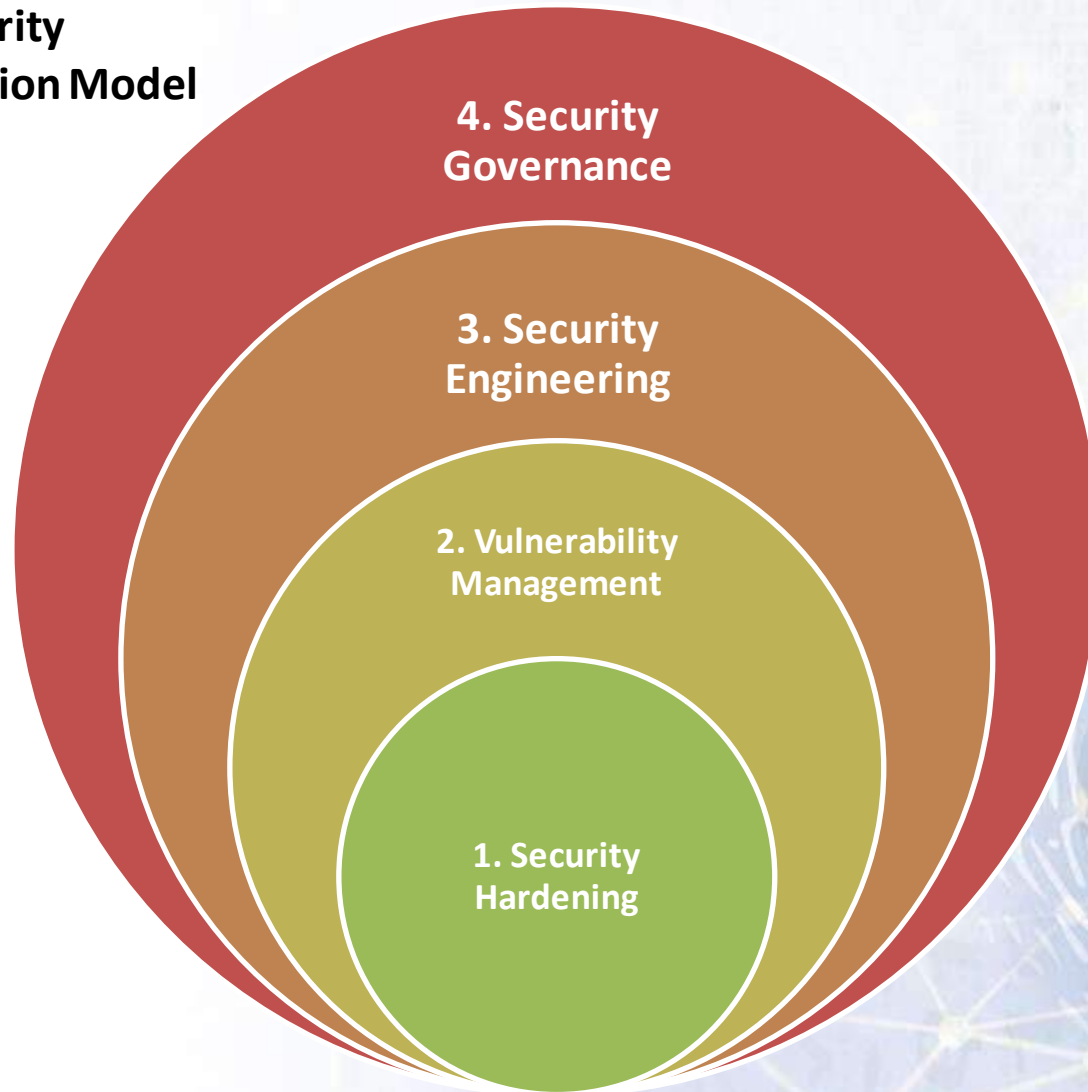
What Is An Information Security Program ?

ISO27001:2013 (ISMS) REQUIREMENTS AND CONTROLS



What Is An Information Security Program ?

4 Layer Security Transformation Model



What Is An Information Security Program ?

- 4-layer security transformation model may be implemented as an ideal security program
- After establishing a basic policy, the sequence of the program (steps 1 through 4) is paramount in order to achieve constructive results

Role of People, Process, and Tech In InfoSec

- People, process, and technology are together referred to as the Information Security Triad
- All three aspects help to form a holistic view of Information Security
- All three are important and cannot be overlooked in an Information Security program or activity

Role of People, Process, and Tech In InfoSec

- **People:**
 - People must be trained to effectively & correctly follow policies, information security processes, and implement technology
 - **Social engineering and phishing** are aspects that people must be trained to handle appropriately

Role of People, Process, and Tech In InfoSec

- **Processes** are fundamental to effective information security
 - User access management
 - Backups devices , router
 - Incident management
 - Change management
 - Vulnerability management
 - Risk management

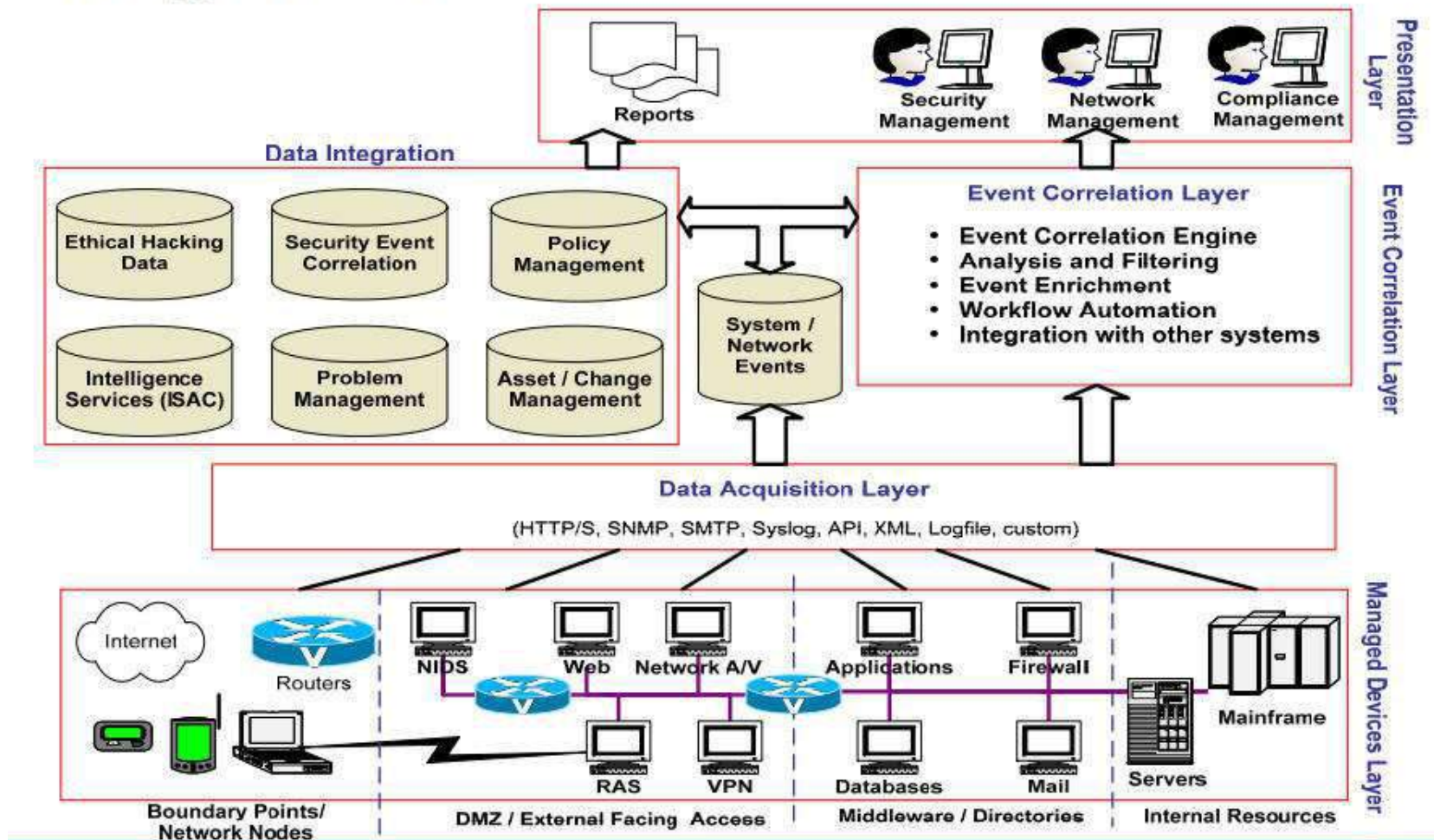
Role of People, Process, and Tech In InfoSec

- **Technology** plays a central role in the Information Security program:

- example
 - Firewalls
 - Antivirus
 - Email anti-spam filtering solution
 - Web filtering solution
 - Data loss prevention (DLP) solution

Role of People, Process, and Tech In InfoSec

Integrated SOC



Role Of An Information Security Manager

- The Information Security Manager (Head Of Information Security or CISO) is delegated and authorized by senior management to run the Information Security program and meet its objectives

Role Of An Information Security Manager

- The Information Security Manager develops a policy to regulate the Information Security program which is signed off by senior management
- Assigned resources and authority to plan, assess, implement, monitor, test, and accredit the Information Security activities

Role Of An Information Security Manager



<http://www.shortinfosec.net/2009/11/role-of-information-security-manager.html>

Role Of An Information Security Manager

- InfoSec Manager Tasks:
 - Develop policy
 - Training & awareness
 - Design security architecture
 - Design security controls
 - Ensure controls are implemented
 - Conduct risk assessment

Role Of An Information Security Manager

- InfoSec Manager Tasks (Contd):
 - Conduct security testing
 - Monitor vulnerability management program
 - Facilitate incident management process
 - Sign-off critical change management activities

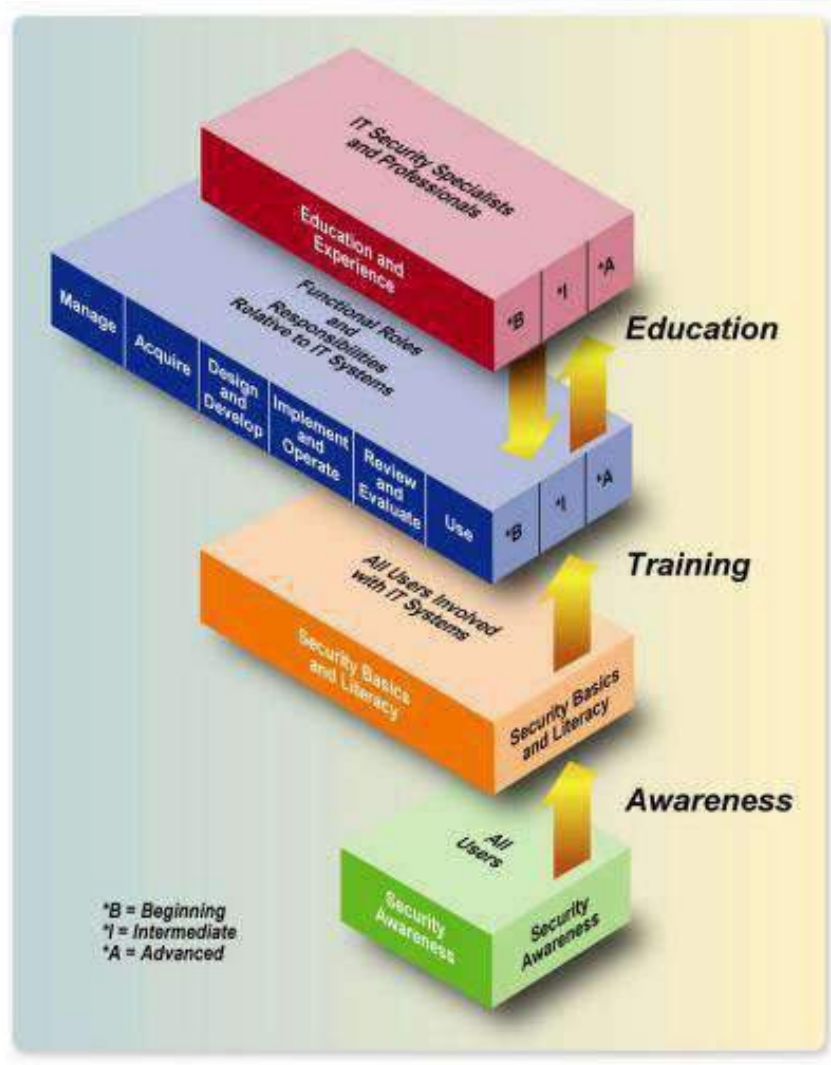
What Is Information Security Awareness ?

aspect of awarence

- Ensure employees are aware of :
 - The importance of protecting sensitive information
 - What they should do to handle information securely
 - Risks of mishandling information

REF: PCI Best Practices For Implementing Security Awareness
<https://www.pcisecuritystandards.org/documents/>

What Is Information Security Awareness ?



What Is Information Security Awareness ?

document

- NIST Special Publication 800-50 (Building An IT Security Awareness & Training Program)
 - Awareness
 - Training
 - Education

What Is Information Security Awareness ?

- Awareness:
 - Awareness is not training
 - Purpose of awareness is simply to focus attention on security
 - Change behavior or reinforce good security practices

REF: NIST SP800-50, PAGE 8

What Is Information Security Awareness ?

- Training:
 - “Strives to produce relevant and needed security skills and competencies”
 - Seeks to teach skills
 - E.g. IT Security course for system administrators covering all security aspects

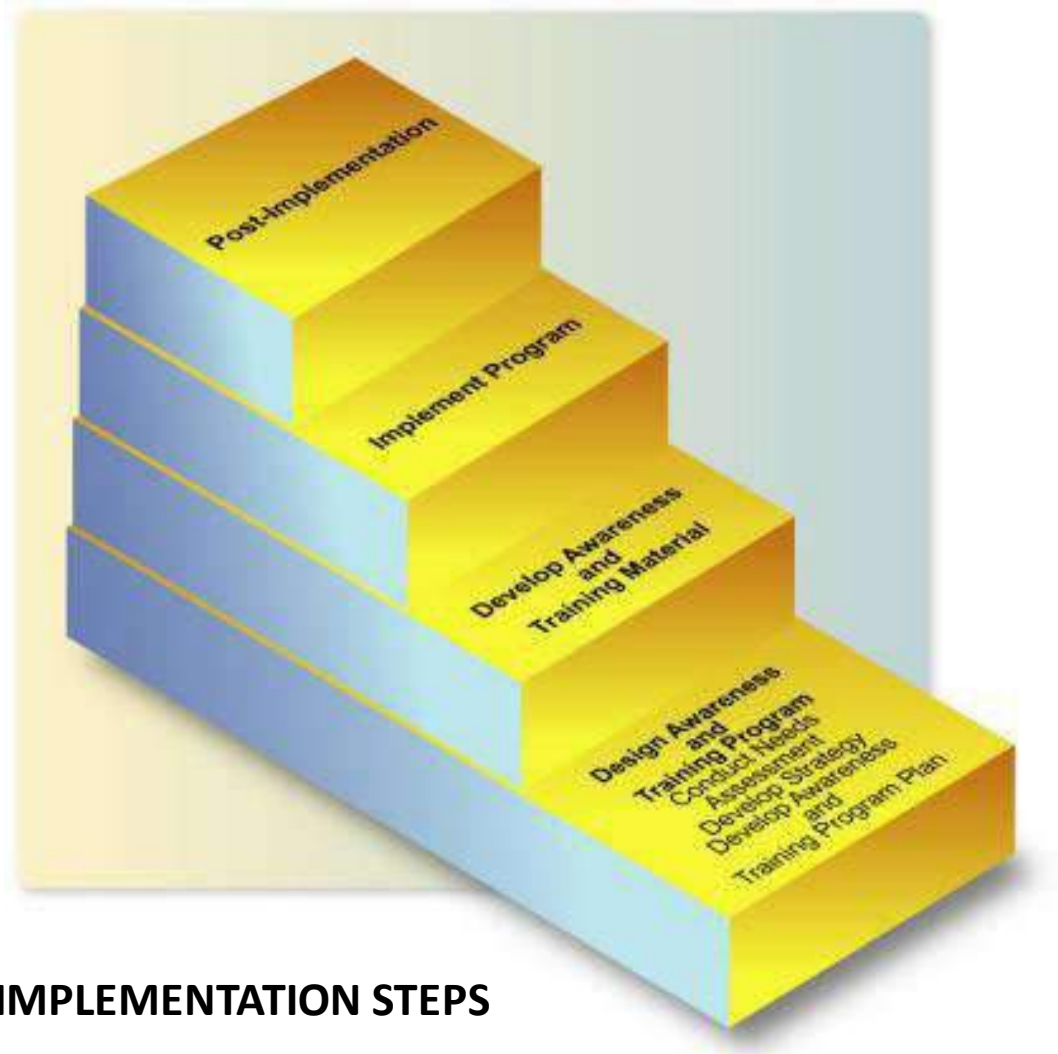
REF: NIST SP800-50, PAGE 9

What Is Information Security Awareness ?

- Education:
 - Integrates all of the skills and competencies into a common body of knowledge
 - E.g. a degree program

What Is Information Security Awareness ?

NIST-SP-800-50



IMPLEMENTATION STEPS

What Is Information Security Awareness ?

- Don'ts:
 - Share your password
 - Click on suspicious email links
 - Install unlicensed software on your PC
- Do's:
 - Logout when getting up from your system
 - Report security incidents

Leading Security Standards & Frameworks

- A standard or framework is a blueprint or roadmap for achieving Information Security objectives
- Examples are ISO27001:2013 (ISMS), PCI DSS, & COBIT

Leading Security Standards & Frameworks

- ISO27001:2013 (ISMS)
 - Specifies the requirements for establishing, implementing, maintaining and continually improving an information security management system
 - Ten short clauses
 - Long annex

Leading Security Standards & Frameworks



ISO27001:2013 MANDATORY CLAUSES

Reference		Description
Mandatory	Clause 4	Context of the organization
	Clause 5	Leadership
	Clause 6	Planning
	Clause 7	Support
	Clause 8	Operation
	Clause 9	Performance evaluation
	Clause 10	Improvement

<https://chapters.theiia.org/bermuda/Events/ChapterDocuments/Information%20Security%20Management%20System%20%28ISMS%29%20Overview.pdf>

Leading Security Standards & Frameworks



ISO27001:2013 DISCRETIONARY CONTROLS

Reference	Description	Control Total
Discretionary	A5 Information security policies	2
	A6 Organization of information security	7
	A7 Human resource security	6
	A8 Asset management	10
	A9 Access control	13
	A10 Cryptography	2
	A11 Physical and environmental security	15
	A12 Operations security	14
	A13 Communications security	7
	A14 System acquisition, development and maintenance	13
	A15 Supplier relationships	5
	A16 Information security incident management	7
	A17 Information security aspects of business continuity management	4
	A18 Compliance	8

TOTAL: 113

<https://chapters.theiia.org/bermuda/Events/ChapterDocuments/Information%20Security%20Management%20System%20%28ISMS%29%20Overview.pdf>

Leading Security Standards & Frameworks

The Payment Card Industry Data Security Standard (PCI DSS) is a widely accepted set of policies and procedures intended to optimize the security of credit, debit and cash card transactions and protect cardholders against misuse of their personal information.

- PCI Data Security Standard (DSS): 
 - Designed to ensure that ALL companies that accept, process, store or transmit credit card information maintain a secure environment
 - Managed by Security Standards Council

<https://www.pcicomplianceguide.org/pci-faqs-2/>

Leading Security Standards & Frameworks

- PCI DSS:
 - SSC is an independent body that was created by the major payment card brands (Visa, MasterCard, American Express, Discover and JCB)
 - 6 Broad goals and 12 requirements



REF: PCI Best Practices For Implementing Security Awareness
<https://www.pcisecuritystandards.org/documents/>

Leading Security Standards & Frameworks



PAYMENT CARD INDUSTRY SECURITY STANDARDS

Protection of Cardholder Payment Data



<https://www.pcisecuritystandards.org/documents/PCI%20SSC%20Quick%20Reference%20Guide.pdf>

Leading Security Standards & Frameworks

Goals	PCI DSS Requirements	
Build and Maintain a Secure Network and Systems	1. Install and maintain a firewall configuration to protect cardholder data 2. Do not use vendor-supplied defaults for system passwords and other security parameters	
Protect Cardholder Data	3. Protect stored cardholder data 4. Encrypt transmission of cardholder data across open, public networks	
Maintain a Vulnerability Management Program	5. Protect all systems against malware and regularly update anti-virus software or programs 6. Develop and maintain secure systems and applications	
Implement Strong Access Control Measures	7. Restrict access to cardholder data by business need to know 8. Identify and authenticate access to system components 9. Restrict physical access to cardholder data	
Regularly Monitor and Test Networks	10. Track and monitor all access to network resources and cardholder data 11. Regularly test security systems and processes	
Maintain an Information Security Policy	12. Maintain a policy that addresses information security for all personnel	

<https://www.pcisecuritystandards.org/documents/PCI%20SSC%20Quick%20Reference%20Guide.pdf>

Leading Security Standards & Frameworks

- COBIT:
 - ISACA framework for IT Governance
 - COBIT 5 helps enterprises to create optimal value from IT by maintaining a balance between realising benefits and optimising risk levels and resource use (ISACA)



Leading Security Standards & Frameworks

- COBIT 5 brings together **five principles** that allow the enterprise to build an effective governance and management framework (ISACA)
- Based on a holistic set of **seven enablers** that optimises IT investment and use for the benefit of stakeholders (ISACA)

Leading Security Standards & Frameworks



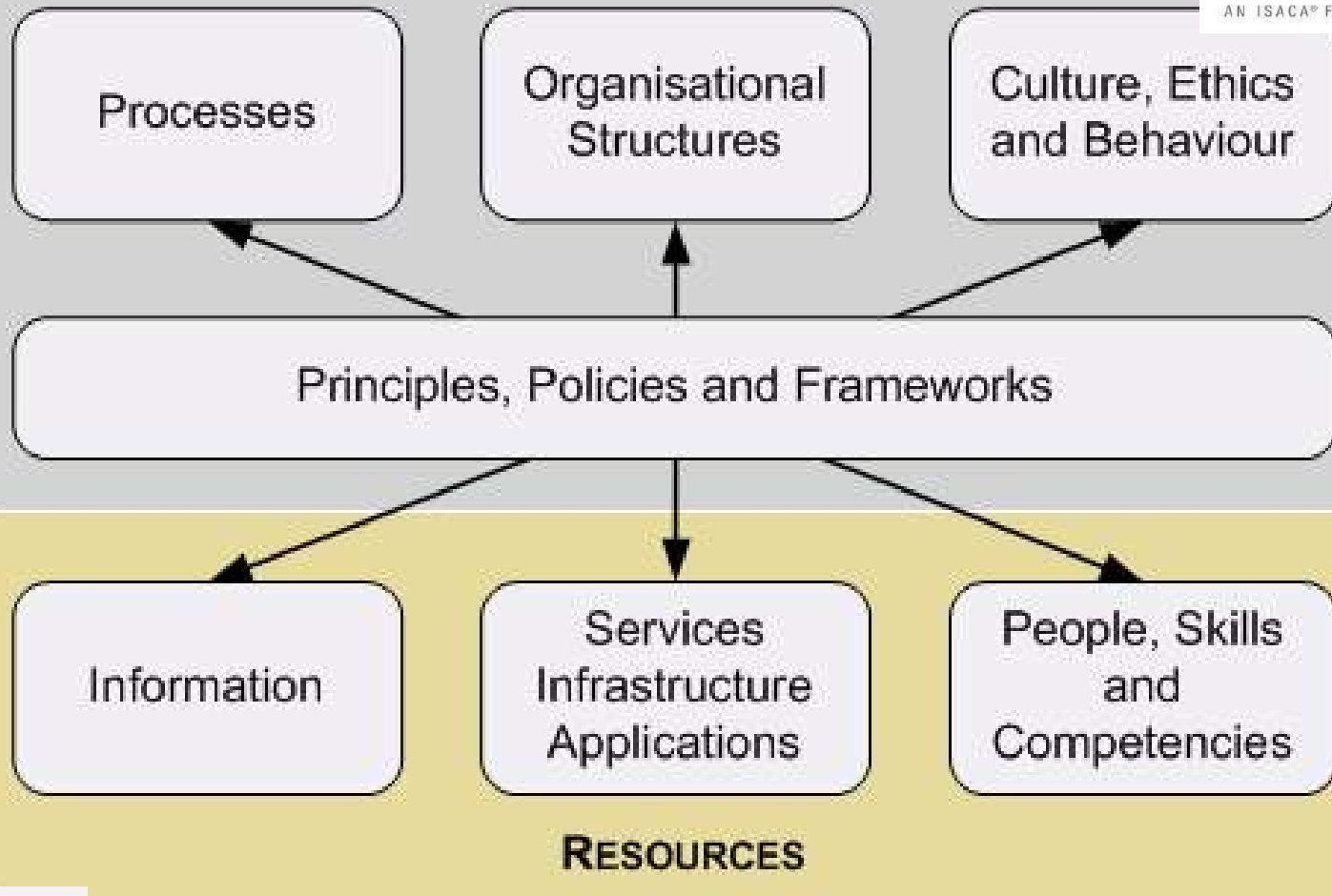
COBIT®
AN ISACA® FRAMEWORK



Leading Security Standards & Frameworks



COBIT 5 ENTERPRISE ENABLERS



Leading Security Standards & Frameworks

- A standard or framework is a blueprint or roadmap for achieving Information Security objectives
- Examples are ISO27001:2013 (ISMS), PCI DSS, & COBIT

What Is Information Security Risk ?

- Risk is a fundamental concept that drives all security standards, frameworks, and activities
- In simple terms, Information Security Risk refers to the potential damage or loss that may be caused to an organization in the absence of appropriate controls

What Is Information Security Risk ?

- A process aimed at achieving an optimal balance between realizing opportunities for gain and minimizing vulnerabilities and loss
- Usually accomplished by ensuring that impact of threats exploiting vulnerabilities is within acceptable limits at an acceptable cost

REF: ISACA CISM MANUAL

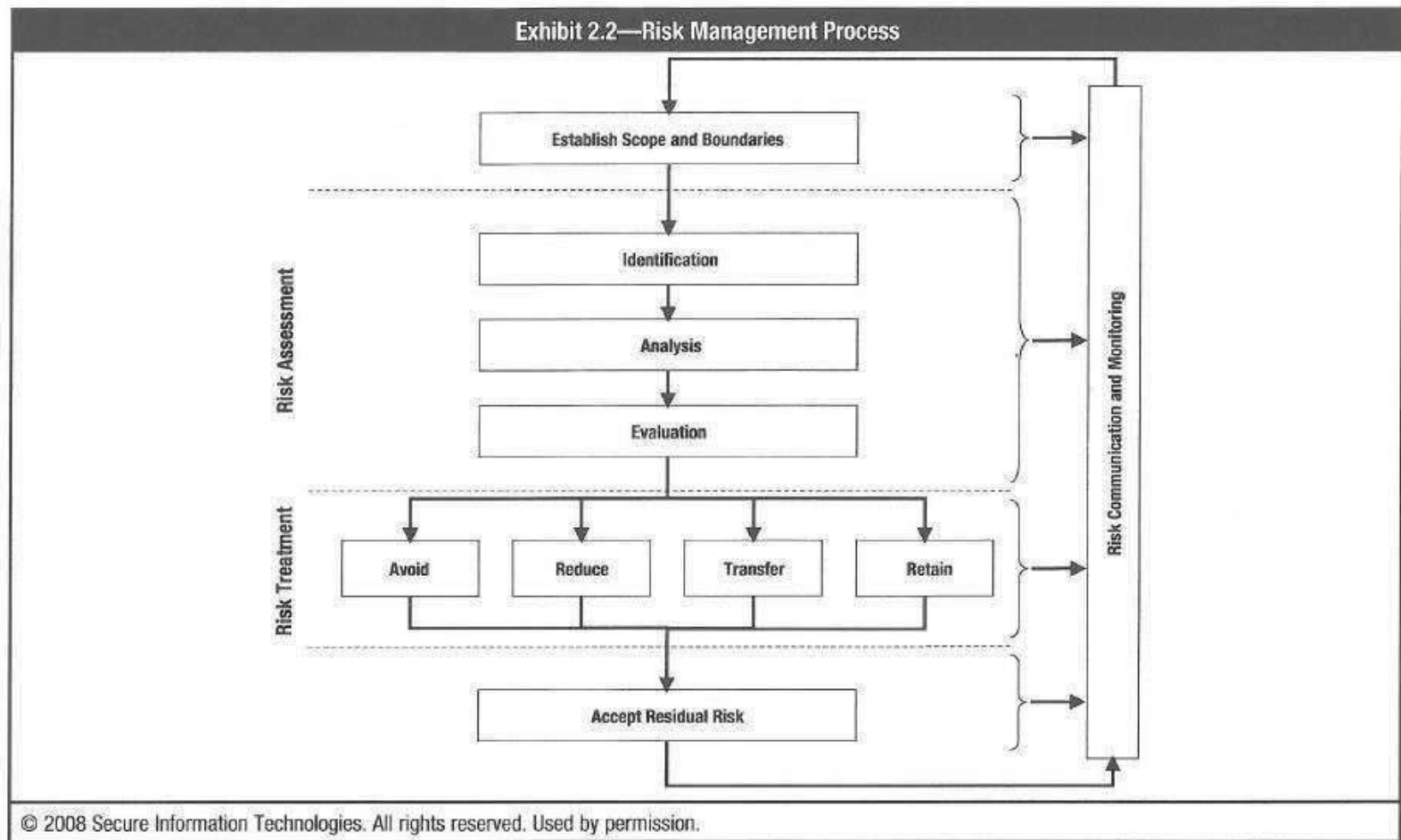
What Is Information Security Risk ?

- Risk is managed so that:
 - It does not materially impact the business process in an adverse way
 - Acceptable level of assurance and predictability to the desired outcomes of any organizational activity

REF: ISACA CISM MANUAL



What Is Information Security Risk ?



REF: ISACA CISM MANUAL

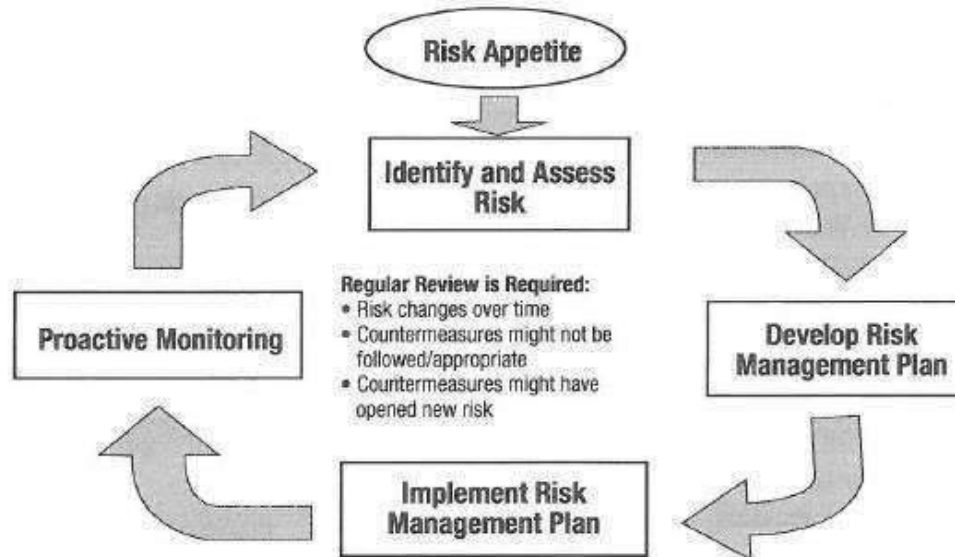
What Is Information Security Risk ?

- Risk Assessment:
 - Foundation for effective risk management
 - Solid understanding of the risk universe
 - Nature and extent of risk to IT resources and potential impact on organizations activities

REF: ISACA CISM MANUAL

What Is Information Security Risk ?

Exhibit 2.3—Continuous Risk Management Steps



REF: ISACA CISM MANUAL

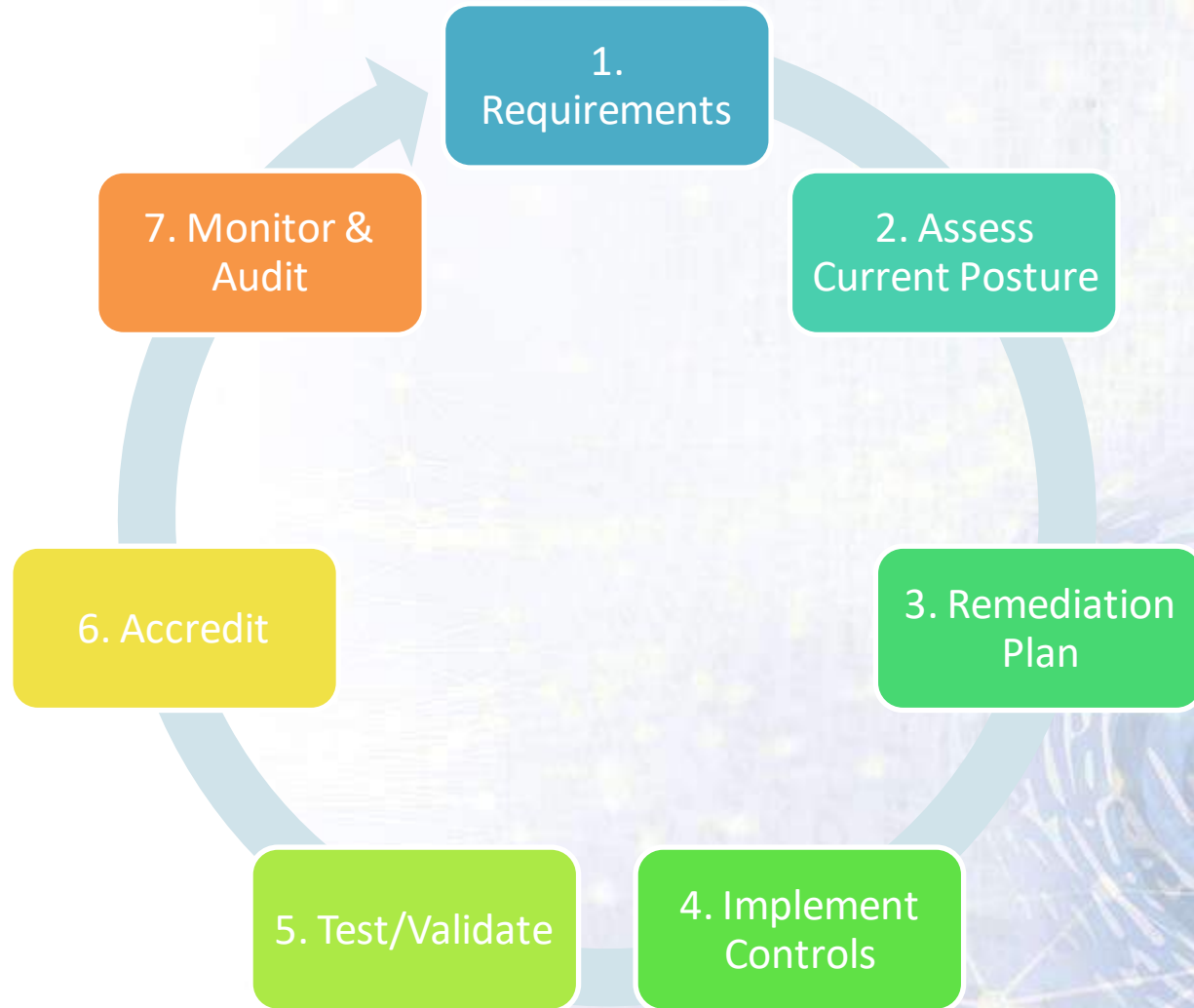
What Is Information Security Risk ?

- Challenges with risk focused approach:
 - In an environment where controls are absent, a risk based approach may become too academic
 - Effort should focus on 4-Step Security Transformation Framework

Information Security Lifecycle

- An Information Security lifecycle represents the recommended sequence to adequately address security during any project or activity
- It is a process to ensure that all security projects and activities consistently follow the same sequence and steps

Information Security Lifecycle



Information Security Lifecycle

- Step 1: Requirements
 - Established by policy, or security program
 - Could also be driven by security transformation program
 - Establish security exposure, determine risk and priority

Information Security Lifecycle

- Step 2: Assess Current Security Posture
 - Conduct gap analysis
 - Could also be a risk assessment and evaluation

Information Security Lifecycle

- Step 3: Remediation Plan
 - Methodology & framework
 - Controls
 - Resources
 - Approvals and communication
 - Timeline
 - Project monitoring and review
 - Develop SOP

Information Security Lifecycle

- Step 4: Implement Controls
 - Pilot
 - Test/validate in pilot
 - Change management
 - Implement in production/live environment
 - Roll-back if unexpected response
 - Maintain SOP

Information Security Lifecycle

- Step 5: Test/Validate
 - Security team or independent review of correctness and coverage of security control implementation
 - Ensure SOP/checklist developed and followed

Information Security Lifecycle

- Step 6: Security Accreditation
 - Review process has been followed (change management, SOP, sign-offs)
 - Establish monitoring mechanism
 - Awareness training
 - Issue formal accreditation

Information Security Lifecycle

- Step 7: Monitor & Audit
 - Monitoring mechanism (KPIs, reporting, review)
 - Incident management
 - Internal audit

Management Commitment

A Management Commitment implies the direct participation by the highest level management (top management) in all specific and critically important aspects such as safety, quality, environment, security, etc. or programmes of an organisation

Management's commitment to quality is very important because they provide the resources for implementation and maintenance of the management system which contains all the processes related to quality.

- What is management commitment?
 - Management commitment is the expression of the intent, relevant actions, and allocation of sufficient resources to ensure the InfoSec program is properly implemented

Management Commitment

- ISO2700:2013 (ISMS)
Clause 5.1:
 - a) Policy and objectives are established (compatible with strategic direction)
 - b) Integration of ISMS reqmts into processes
 - c) Resources
 - d) Communicating importance



Management Commitment

- ISO2700:2013 (ISMS)
Clause 5.1:
 - e) Intended outcomes are achieved
 - f) Directing and supporting persons
 - g) Promoting continual improvement
 - h) Supporting other management roles



Management Commitment

- “Tone at the top”
 - Management closely watches the actions of executive leadership (culture)
 - The importance given to InfoSec by the executive leadership becomes the minimum threshold for rest of the organization

Management Commitment

- In practice:
 - Security policy
 - Security responsibility delegated to head (CISO) or dept
 - Security steering committee (board level)
 - Quarterly or frequent management reviews of information security program

Information Security Responsibility

- Default organizational perception:
 - Security is responsibility of one person or one department
 - Can get away with “security as an after-thought”
 - Reactive

Information Security Responsibility

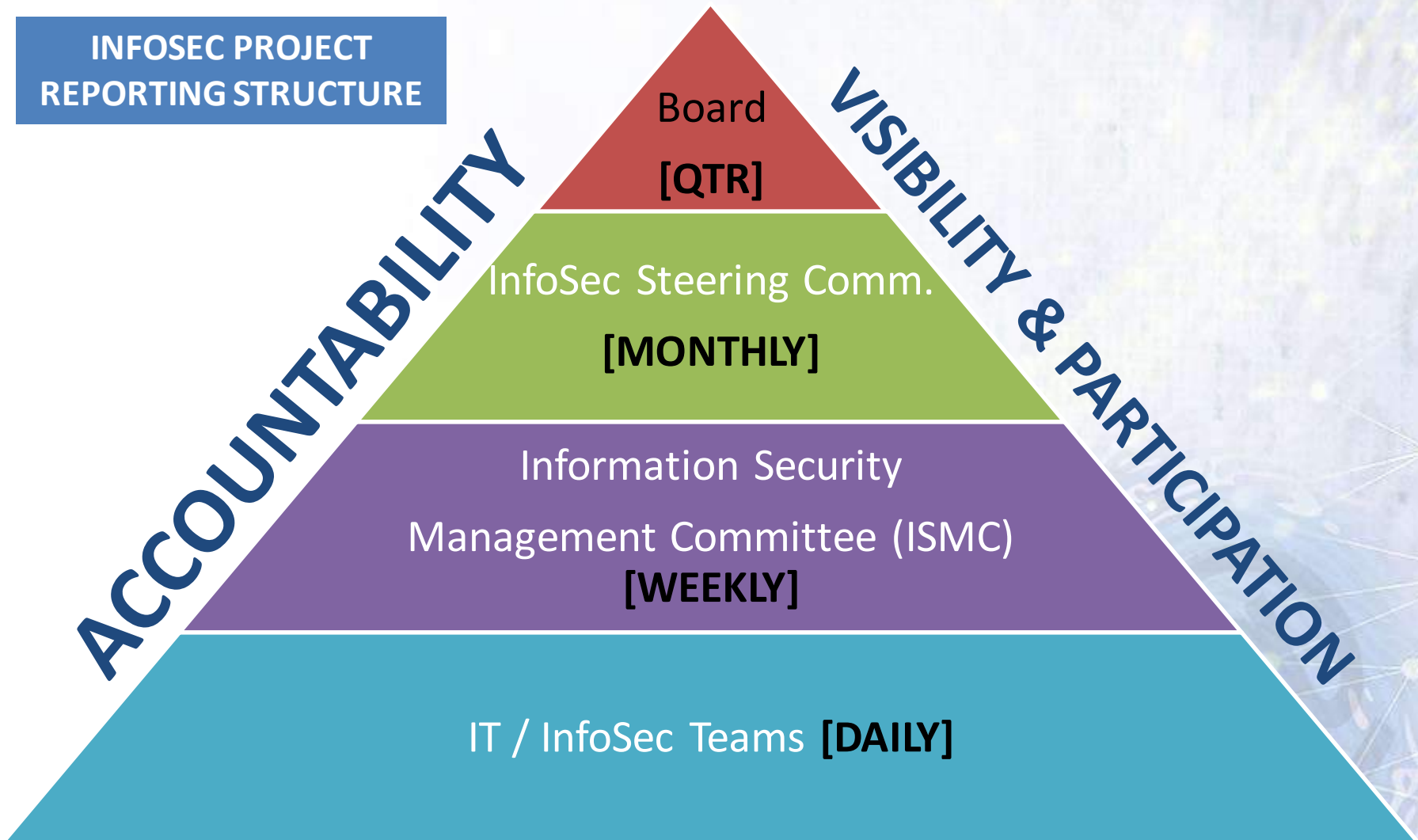
- Security is everyone's responsibility:
 - Management commitment & tone at the top
 - Security awareness campaigns/program
 - A strong and effective security program
 - Allocation of sufficient resources

Information Security Responsibility

- Security involvement & accountability:
 - Effective security implementation should be built into the performance KPIs of key team members (management, technical, business)
 - Annual appraisals, security awards and recognition

Information Security Responsibility

INFOSEC PROJECT REPORTING STRUCTURE



Information Security Responsibility

- Security is everyone's responsibility and has to gradually take its place in org culture

Cyber Security Breaches

WannaCry ransomware attack on 12 May 2017 affecting hundreds of thousands of computers in more than 150 countries.

AIDS_Trojan. 1989 also marked a grim day in history, with Joseph Popp creating the first ransomware attack. Joseph Popp created a Malware called the AIDS Trojan, which was distributed through his postal mailing lists using a floppy disk.

According to data breach statistics, the largest data breach in history is the one that Yahoo! suffered for several years

- Fox News Video:
“World’s Biggest Cyber Attacks”
 - <http://video.foxnews.com/v/5435057924001/?#sp=show-clips>
- World’s Biggest Data Breaches:
 - <http://www.informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/>

Cyber Security Breaches

- Leading Global Reports:
 - Verizon 2017 Data Breach Investigations Report (DBIR)
 - Symantec 2017 Internet Security Threat Report (ISTR)

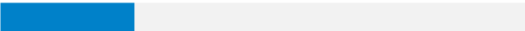
Cyber Security Breaches



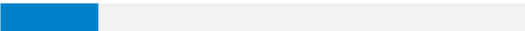
Who's behind the breaches?

75% 

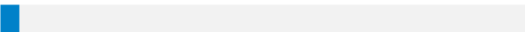
perpetrated by outsiders.

25% 

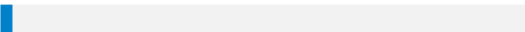
involved internal actors.

18% 

conducted by state-affiliated actors.

3% 

featured multiple parties.

2% 

involved partners.

51% 

involved organized criminal groups.



What tactics do they use?

62% 

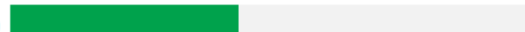
of breaches featured hacking.

51% 

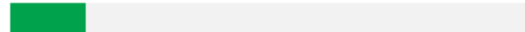
over half of breaches included malware.

81% 

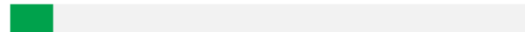
of hacking-related breaches leveraged either stolen and/or weak passwords.

43% 

were social attacks.

14% 

Errors were causal events in 14% of breaches. The same proportion involved privilege misuse.

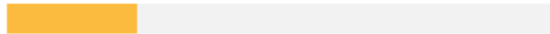
8% 

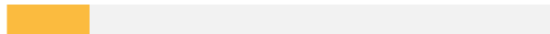
Physical actions were present in 8% of breaches.

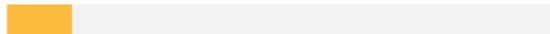
Cyber Security Breaches



Who are the victims?

24% 
of breaches affected financial organizations.

15% 
of breaches involved healthcare organizations.

12% 
Public sector entities were the third most prevalent breach victim at 12%.

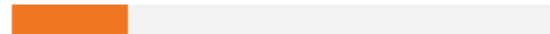
15% 
Retail and Accommodation combined to account for 15% of breaches.



What else is common?

66% 
of malware was installed via malicious email attachments.

73% 
of breaches were financially motivated.

21% 
of breaches were related to espionage.

27% 
of breaches were discovered by third parties.

Cyber Security Breaches



Breaches

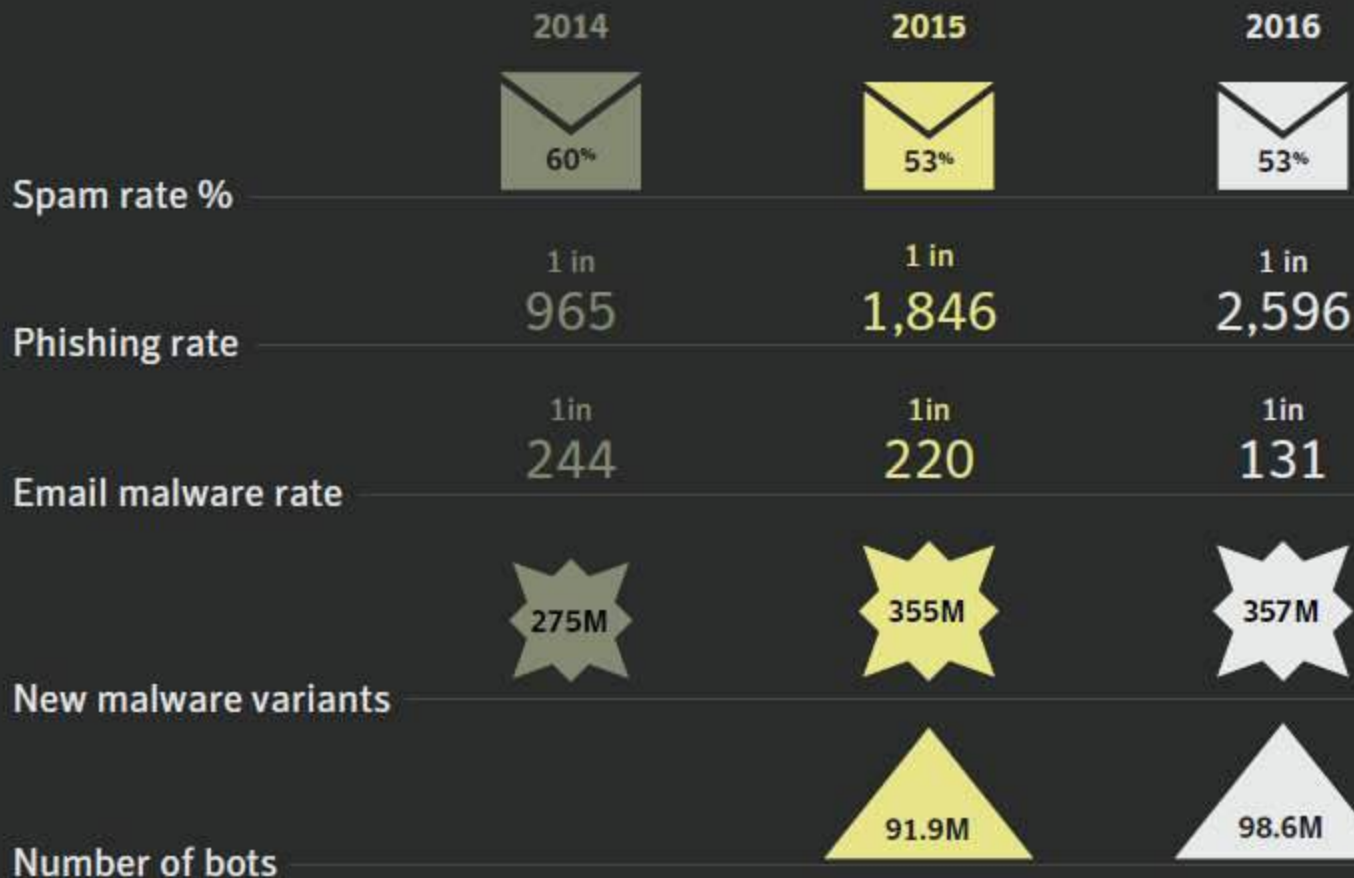


In the last **8** years more than **7.1 billion** identities have been exposed in data breaches

Cyber Security Breaches



Email threats, malware, and bots

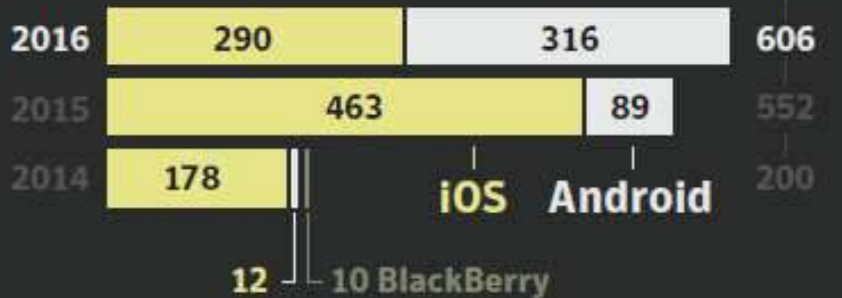


Cyber Security Breaches

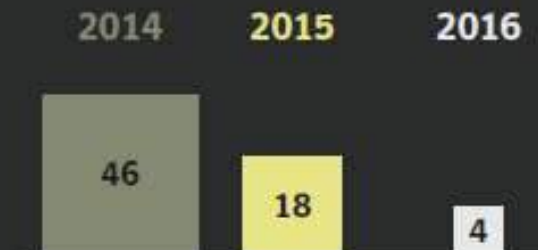


Mobile

New mobile vulnerabilities



New Android mobile malware families



New Android mobile malware variants



Cyber Security Breaches



Web

Percentage of scanned websites with vulnerabilities

2014

76%

2015

78%

2016

76%

Percentage of which were critical

20%

15%

9%

Average number of web attacks blocked per day

2015

340K

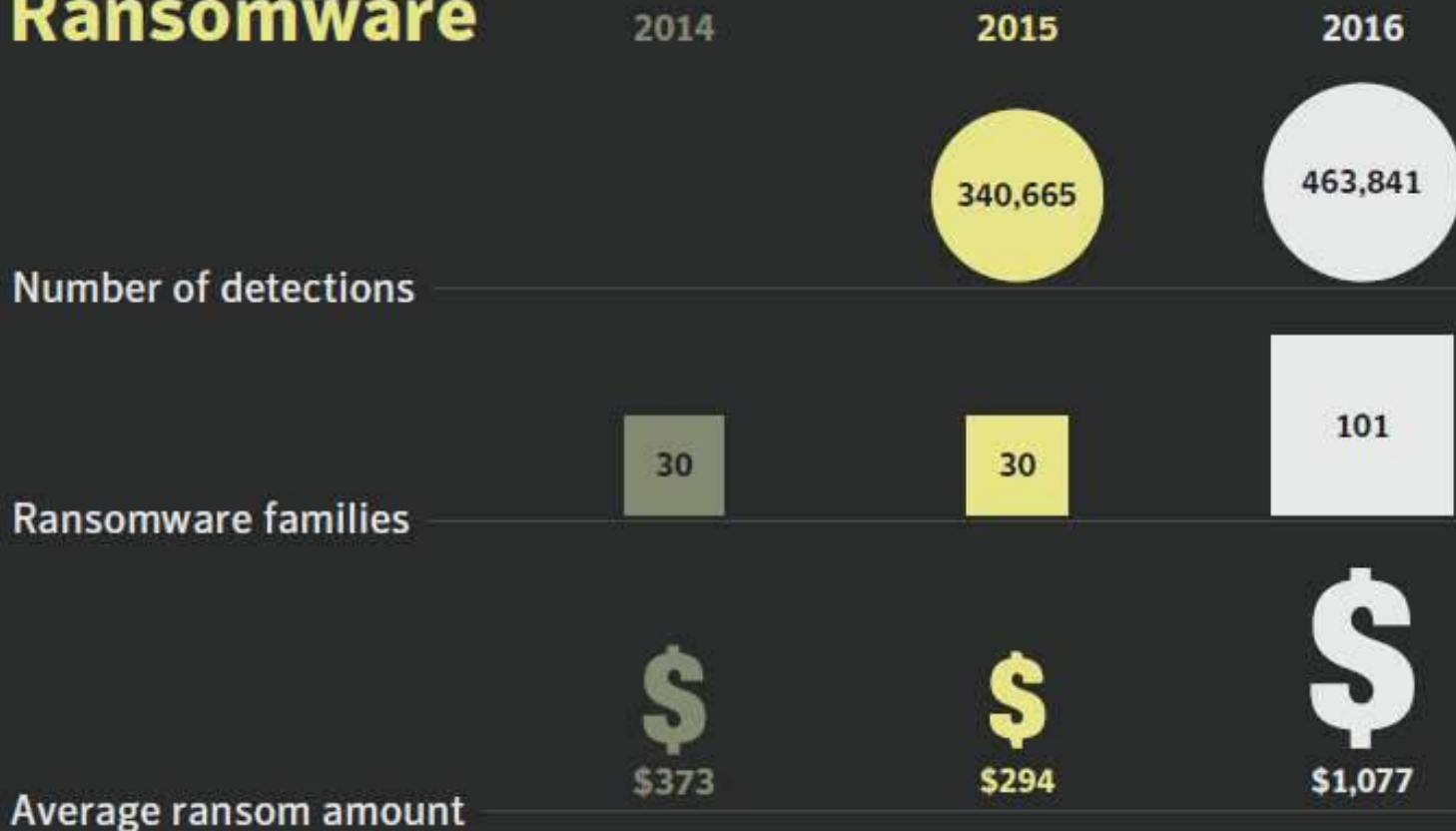
2016

229K

Cyber Security Breaches



Ransomware



Internet of Things



Speed of attack

2 minutes:
time it takes for
an IoT device to
be attacked



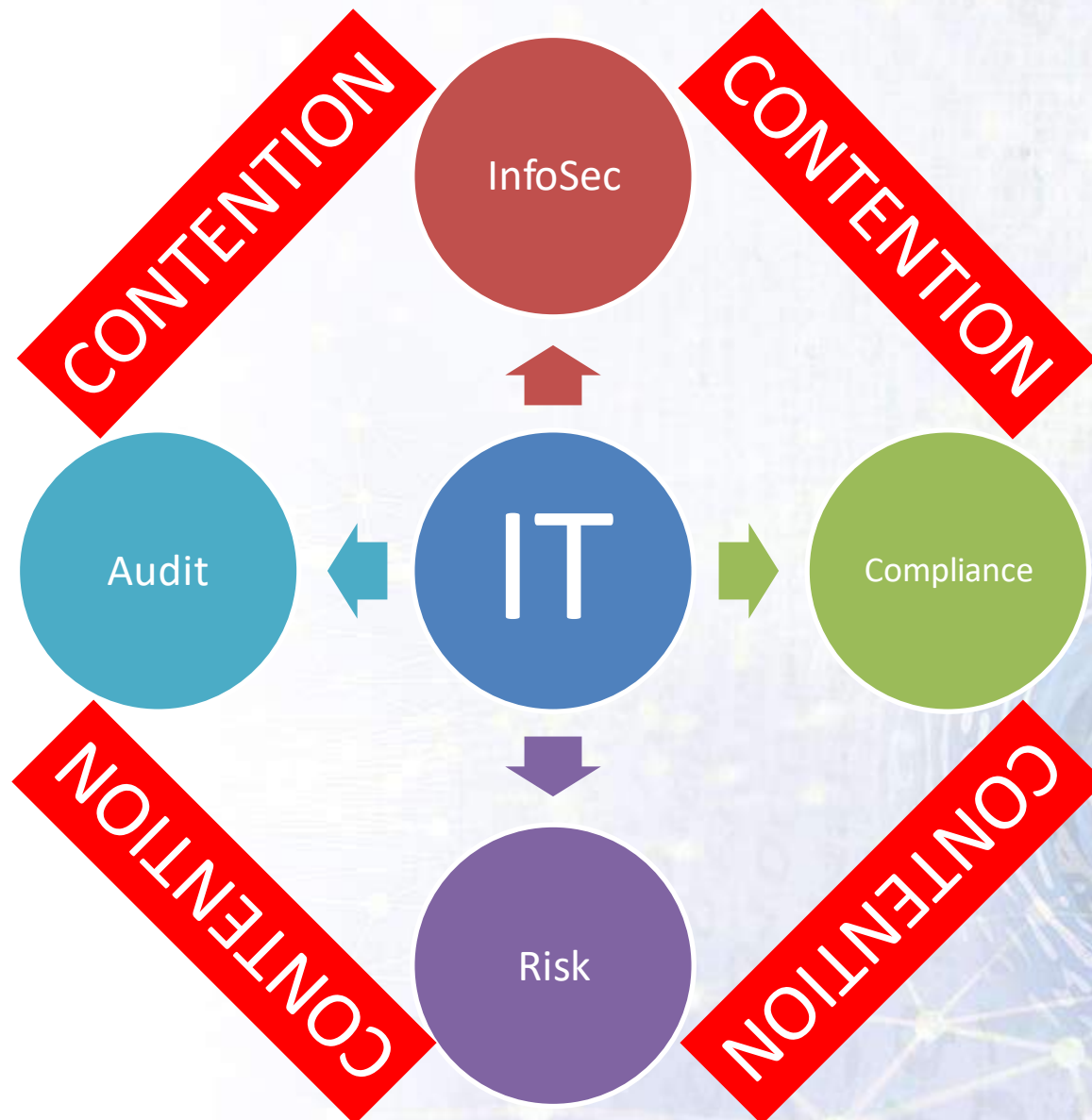
Cyber Security Breaches

- Leading Global Reports:
 - Verizon 2017 Data Breach Investigations Report (DBIR)
 - Symantec 2017 Internet Security Threat Report (ISTR)

Challenges Of InfoSec Implementation

- Challenges Of IT:
 - Complex and difficult to manage
 - Under pressure from business groups
 - Lack of sufficient competent resources
 - Lack of process culture
 - IT not aligned to perform diligent security work

Challenges Of InfoSec Implementation



Challenges Of InfoSec Implementation

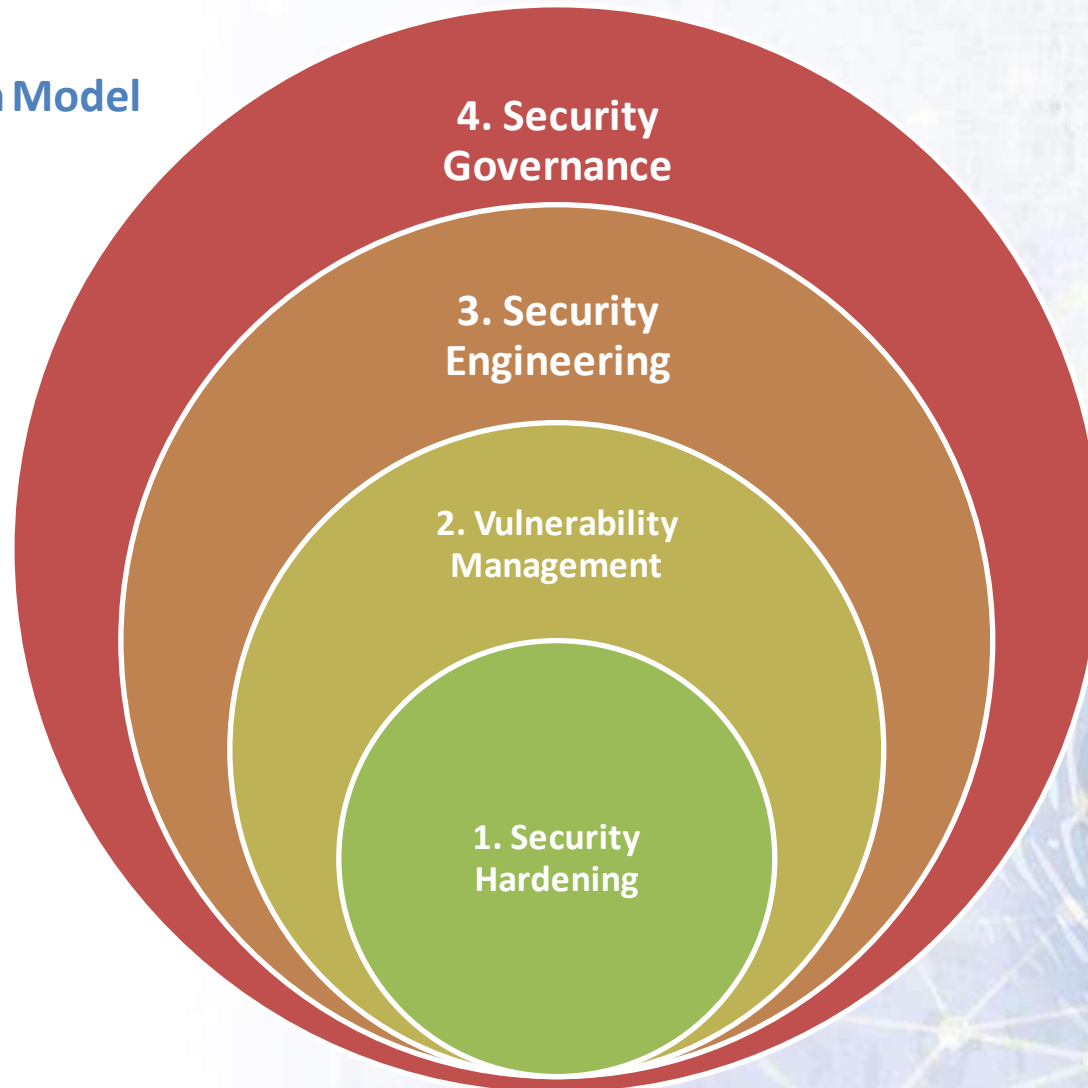
- Challenges Of InfoSec:
 - Silos & lack of coherent ownership
 - Lot of time & energy wasted in traversing dept boundaries
 - Enabling environment for tough security work missing
 - Security hardening glaringly absent

Challenges Of InfoSec Implementation

- Pakistan Industry Security Characteristics:
 - Wavering management commitment
 - Superficial “dressing” security
 - Reactive to regulator audit/compliance mandate
 - Industry in denial

Challenges Of InfoSec Implementation

InfoSec Transformation Model



Challenges Of InfoSec Implementation

- Challenges Of InfoSec

Role Of A Regulator

- Cyber attack can have devastating consequences causing financial loss and disruption of critical infrastructure
- Cyber security has become a key risk factor putting under threat not only consumer rights protection, but also viability and health of the industry itself

Role Of A Regulator

- A cybersecurity regulation comprises directives that safeguard information technology and computer systems with the purpose of forcing companies and organizations to protect their systems and information from cyber-attacks (Wikipedia)

Role Of A Regulator

- Industry regulators including [banking regulators](#) have taken notice of the risk from cybersecurity and have either begun or are planning to begin to include cybersecurity as an aspect of regulatory examinations (Wikipedia)

Role Of A Regulator

- Role Of Regulator In Cyber Security:
 - Regulations, guidelines, and audit
 - Engagement of key stakeholders
 - Technical and industry expertise
 - Regional and international cooperation

Role Of A Regulator

- Regionally, the most well developed cyber security strategy and framework developed by Singapore (ITU rank # 1), Malaysia (ITU rank # 3), and Oman (ITU rank # 4)

Role Of A Regulator

- Singapore:
 - Cyber Security Agency (2015); strategy, education, outreach, eco-system development
 - National Cyber Security Master Plan 2018 (created 2013)
 - Cyber Security Strategy (created 2016)

Role Of A Regulator

- Pakistan; Ministry of IT (MOIT):
 - National IT Policy 2016 (draft)
 - Digital Pakistan Policy 2017

Role Of A Regulator

- Pakistan; State Bank Of Pakistan (SBP):
 - Enterprise Technology Governance & Risk Management Framework for Financial Institutions (30 May 2017)

Role Of A Regulator

- Pakistan lacks:
 - National cyber security strategy
 - National cyber security master plan
 - National cyber security agency
 - National certification & accreditation body
 - National Computer Emergency Response Team (CERT)

Status Of InfoSec in Pakistan

- Pakistan Electronic Crimes Act (PECA) enacted as late as 2016
- Cyber security strategy, eco-system still missing
- Research program, capacity building, standardization, & certification bodies absent
- Condition of InfoSec in industry largely dismal

Abstract

Pakistan																															

Global Cyber Security Index 2017 (ITU):

Pakistan ranked 67th with a score of 0.44/1

Bangladesh ranked 53rd with a score of 0.524/1

India ranked 23rd with a score of 0.683/1

https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2017-PDF-E.pdf

Status Of InfoSec in Pakistan

- Pakistan cyber security posture (industry):
 - Superficial security
 - Reactive
 - Emphasis on governance
 - Security hardening of IT assets largely absent
 - Industry has been in denial for last decade

Status Of InfoSec in Pakistan

- Reasons for poor security posture:
 - Archaic digitalization and commerce
 - Perception that Pakistan is immune
 - Lack of awareness and management commitment
 - Lack of effective regulations

very old

Status Of InfoSec in Pakistan

- Changing dynamics (PK):
 - Pakistan financial industry rocked by Bangladesh SWIFT hack 2016
 - Wannacry (May 2017) badly hit several dozen organizations in Pakistan
 - Increasing e-commerce, electronic banking

Status Of InfoSec in Pakistan

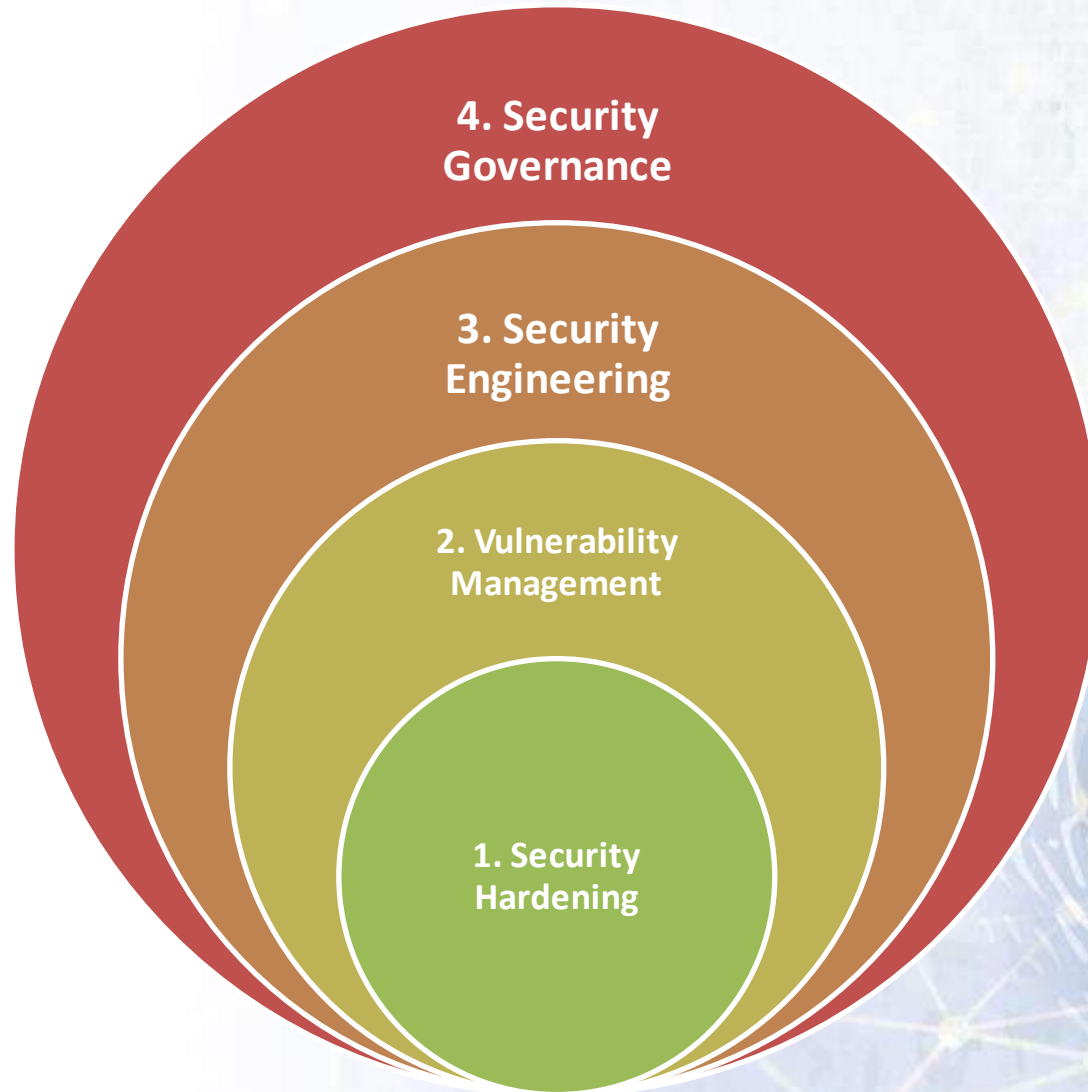
- Pakistan needs:
 - Necessary measures by the Government in line with what Malaysia, Oman have done for cyber security
 - Development of the security eco-system as an enabler in order to drive strong security posture

we need to build security like oman and malaysia

Solution For InfoSec Improvement (PK)

- Generally, Pakistan Information Security is one generation behind IT deployment
- Four-layer security transformation model provides the correct sequence and focus in order to address organizational security gaps

Solution For InfoSec Improvement (PK)



Solution For InfoSec Improvement (PK)

1. Security Hardening;
Security controls on IT
assets & process
2. Vulnerability
Management; patching finding
3. Security Engineering;
More complex security
design & solutions
4. Security Governance;
Managing the
information security
program

Solution For InfoSec Improvement (PK)

- Solution for strong security posture:
 - Management commitment (Board)
 - 4 layer transformation model as security program
 - Allocation of resources
 - Periodic reviews for assessing progress

Solution For InfoSec Improvement (PK)

dont focus on one step of transformation model

- Don't repeat the same mistakes:
 - Too much governance without the underlying security hardening
 - Reactive rather than intrinsic
 - Lack of resources (10% of what allocated for IT)
 - Management interest

Typical Enterprise IT Network

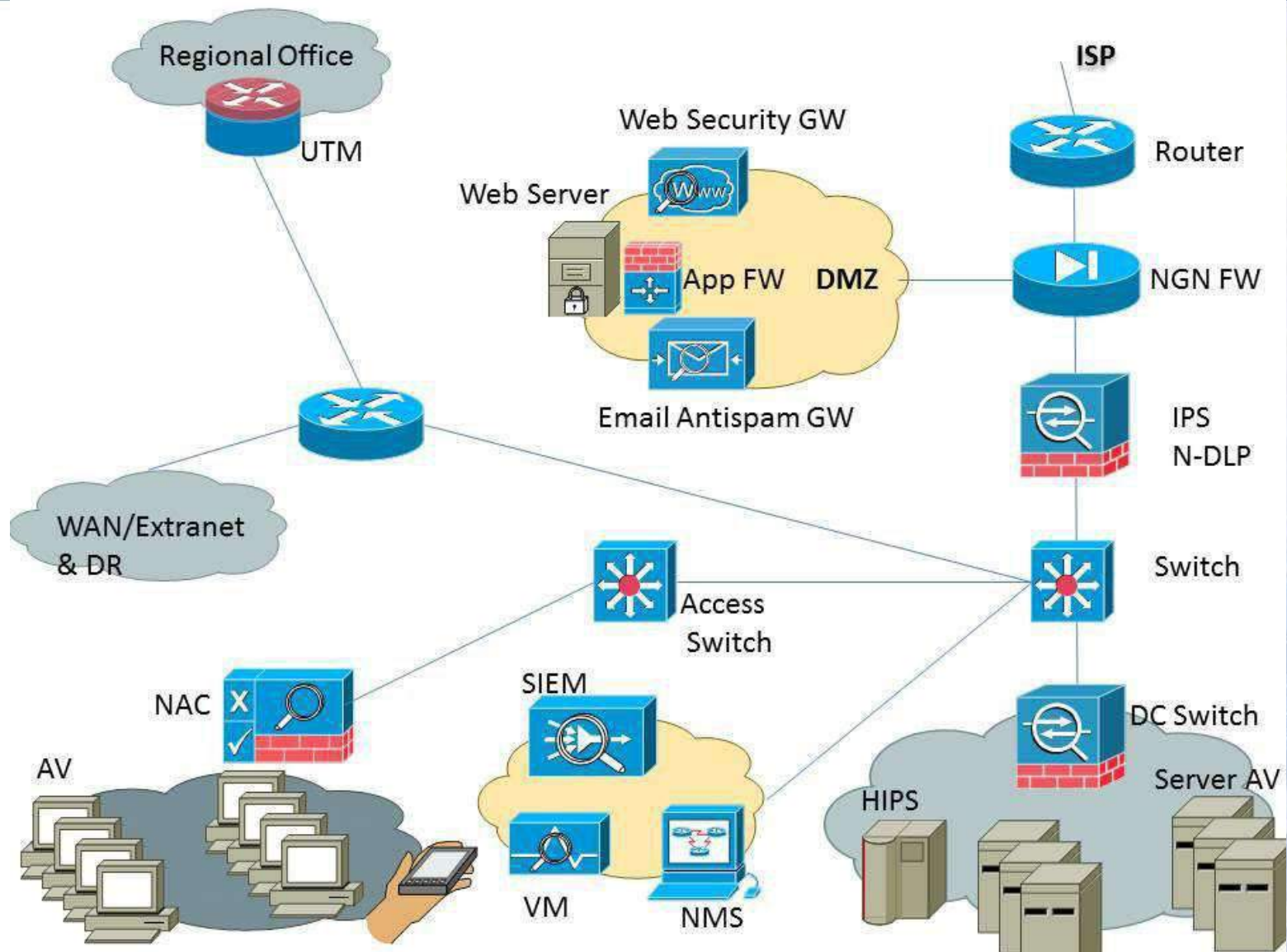
- Chapter 2:
 - **Typical Enterprise IT Architecture & Security Overlay**

what the architect of the organization on lay
and how do we play as a top of the it architect

Typical Enterprise IT Network

- What does a typical enterprise IT network look like ?

Typical Enterprise IT Network



Typical Enterprise IT Network

A router is a device that connects two or more packet-switched networks or subnetworks.

- Edge router
- NGN FW
- DMZ:
 - Web security GW/Proxy
 - Application security FW
 - Web server
 - Email antispam GW
- IPS & N-DLP
- Distribution switch

Typical Enterprise IT Network

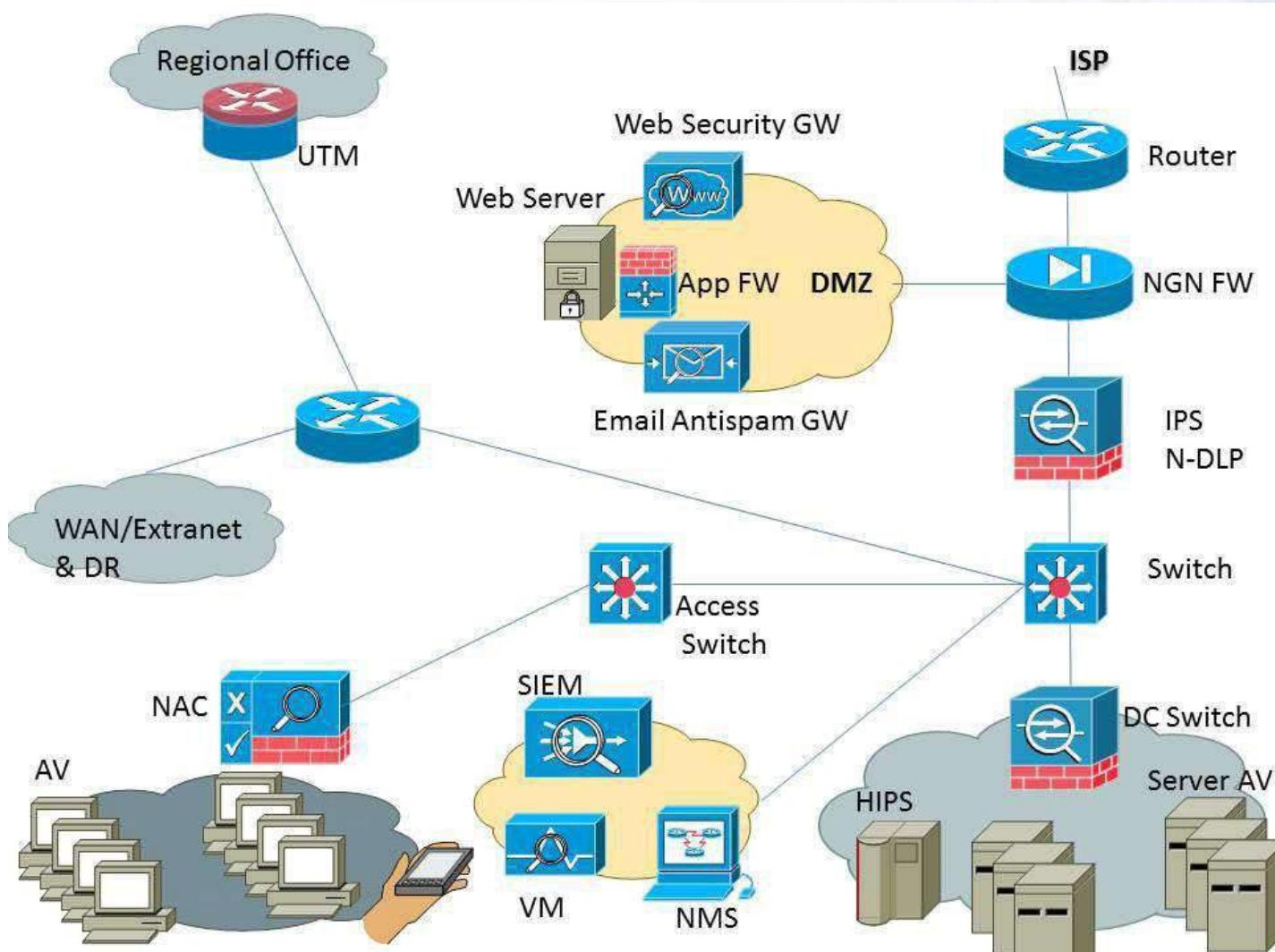
- Data center switch & FW
- Access switch
- NAC
- SOC:
 - SIEM
 - VM
 - Other SOC tools
- System AV
- Server HIPS
- UTM
- Mobile device - MDM

Major Components: Enterprise IT Network

Distributed Denial-of-Service

- Edge router
 - WAN interfaces
 - Edge filtering (access lists)
 - DDOS protection
- NGN FW
 - Capable of APT attack prevention, malware filtering, web security, email security, application bandwidth filtering

Major Components: Enterprise IT Network



Major Components: Enterprise IT Network

- DMZ:
 - Security zone with placement of published web server, web & email security GWs, app security GW
- IPS:
 - Intrusion prevention (signature based)
 - May be feature in NGN-FW

Major Components: Enterprise IT Network

- Distribution switch
 - Connectivity to access switches, external exit point (WAN), and DC switch
- Data center switch & FW
 - Data center filtering (malware & access-lists)

Major Components: Enterprise IT Network

- Access switch
 - User connectivity
 - Switchport security & access switch security
- NAC
 - Network admission control (IEEE802.1X)
- SIEM
 - Logging & dashboard for events, root cause analysis, event correlation

Major Components: Enterprise IT Network

- Vulnerability Manager
 - Vulnerability scanning and asset tracking
- System AV
 - Signature based malware prevention
- Server HIPS
 - IPS features for servers, also file integrity checking

Major Components: Enterprise IT Network

- UTM
 - Multi-featured NGN FW device
- Mobile device – MDM
 - Security features for mobile devices

OSI Security Architecture

old

- ITU-T X.800, Security Architecture For OSI ('91)
- Defines a technique for defining security requirements, and characterizes the approaches to satisfy those requirements
- Defines security attack, mechanism, and service

http://www.cse.wustl.edu/~jain/cse571-11/ftp/I_01ov.pdf

https://cgi.csc.liv.ac.uk/~alexei/COMP522_10/COMP522-SecurityArchitecture_07.pdf

OSI Security Architecture

- Security attack: action that compromises the security of information owned by an organization (or person)
 - Passive: aims to learn or make use of system information only
 - Active: attempts to alter system resources/operation

OSI Security Architecture

sufficient

- Security service is a service that ensures adequate security of the system or data transfer
 - Authentication
 - Access control
 - Data confidentiality
 - Data integrity
 - Non-repudiation
 - Availability

security services

OSI Security Architecture

Security Services (X.800)

- ❑ **Authentication** - assurance that communicating entity is the one claimed
 - have both peer-entity & data origin authentication
- ❑ **Access Control** - prevention of the unauthorized use of a resource
- ❑ **Data Confidentiality** – protection of data from unauthorized disclosure
- ❑ **Data Integrity** - assurance that data received is as sent by an authorized entity
- ❑ **Non-Repudiation** - protection against denial by one of the parties in a communication
- ❑ **Availability** – resource accessible/usable

http://www.cse.wustl.edu/~jain/cse571-11/ftp/I_01ov.pdf

OSI Security Architecture

- Security mechanism:
 - Feature designed to detect, prevent, or recover from a security attack
 - Cryptography underlies many of the mechanisms

http://www.cse.wustl.edu/~jain/cse571-11/ftp/l_01ov.pdf

OSI Security Architecture

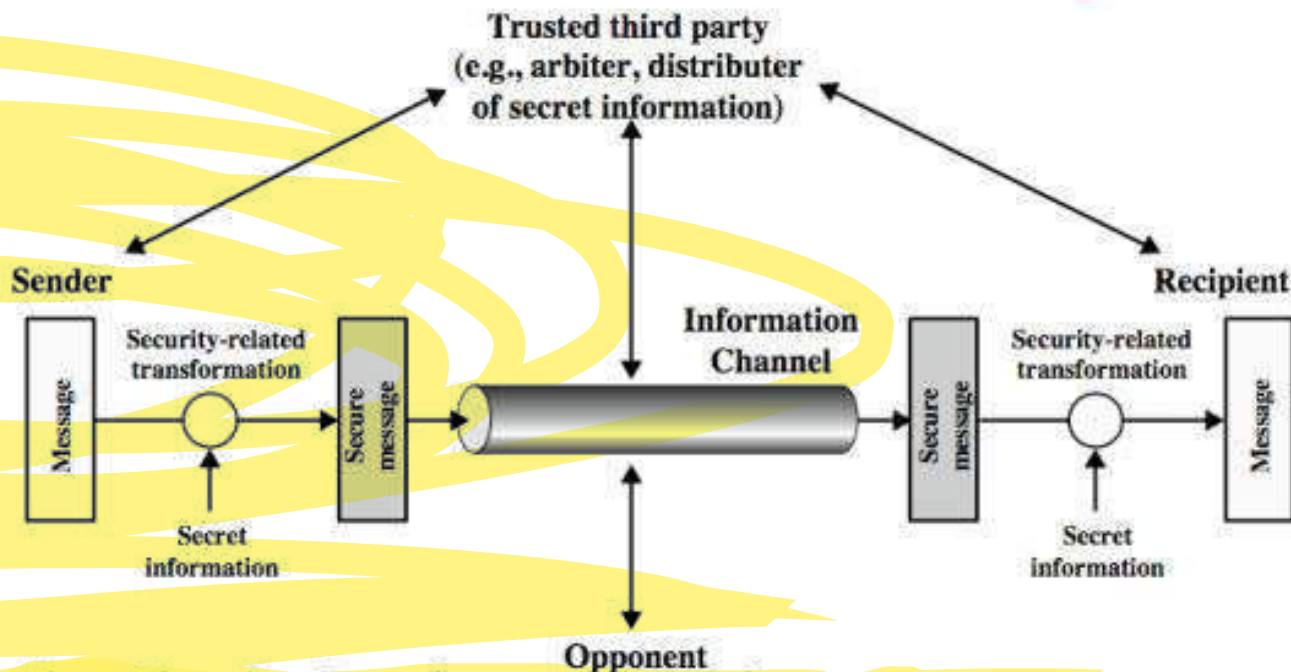
Services and Mechanisms Relationship

Service	Mechanism							
	Enciph- erment	Digital signature	Access control	Data integrity	Authenti- cation exchange	Traffic padding	Routing control	Notari- zation
Peer entity authentication	Y	Y			Y			
Data origin authentication	Y	Y						
Access control			Y					
Confidentiality	Y						Y	
Traffic flow confidentiality	Y					Y	Y	
Data integrity	Y	Y		Y				
Nonrepudiation		Y		Y				Y
Availability				Y	Y			

http://www.cse.wustl.edu/~jain/cse571-11/ftp/l_01ov.pdf

OSI Security Architecture

Model for Network Security



1. Algorithm for Security transformation
2. Secret key generation
3. Distributed and share secret information
4. Protocol for sharing secret information

http://www.cse.wustl.edu/~jain/cse571-11/ftp/I_01ov.pdf

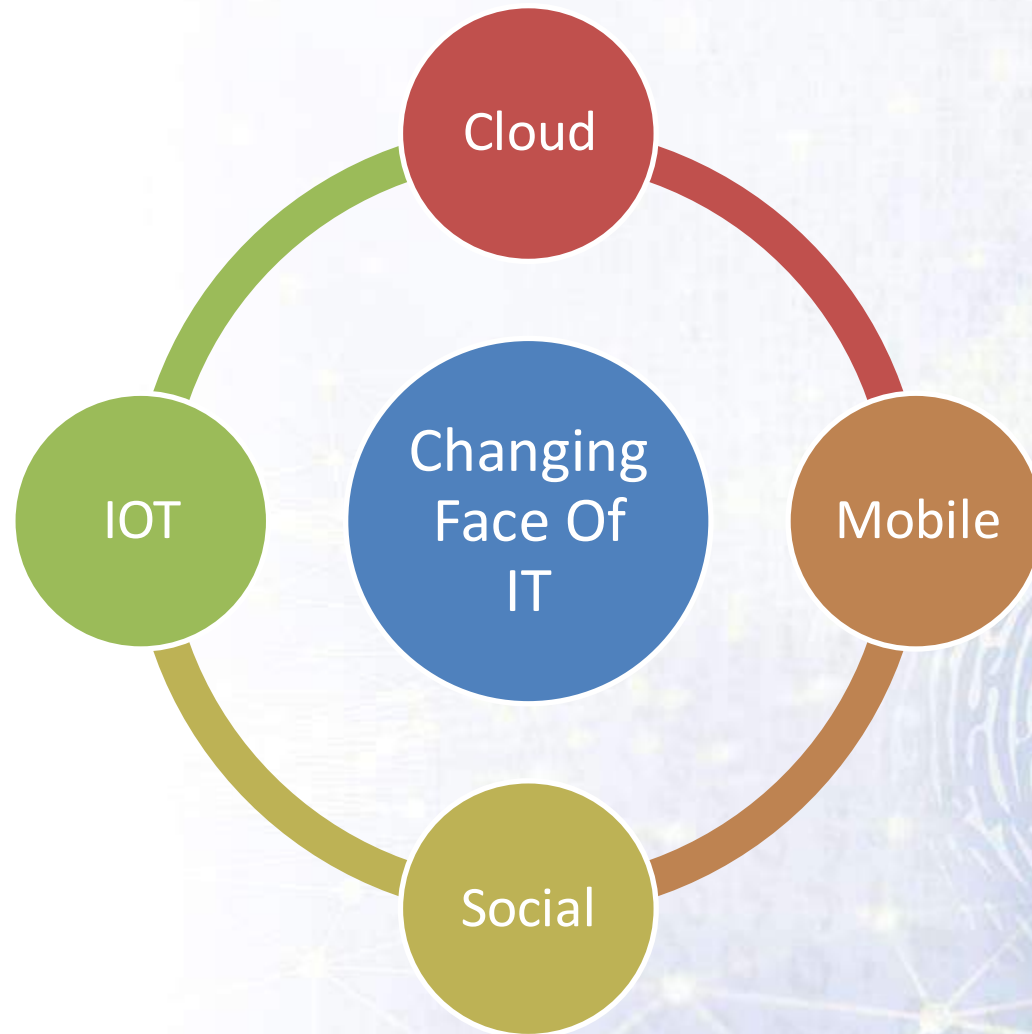
OSI Security Architecture

- ITU-T X.800, Security Architecture For OSI is dated from 1991

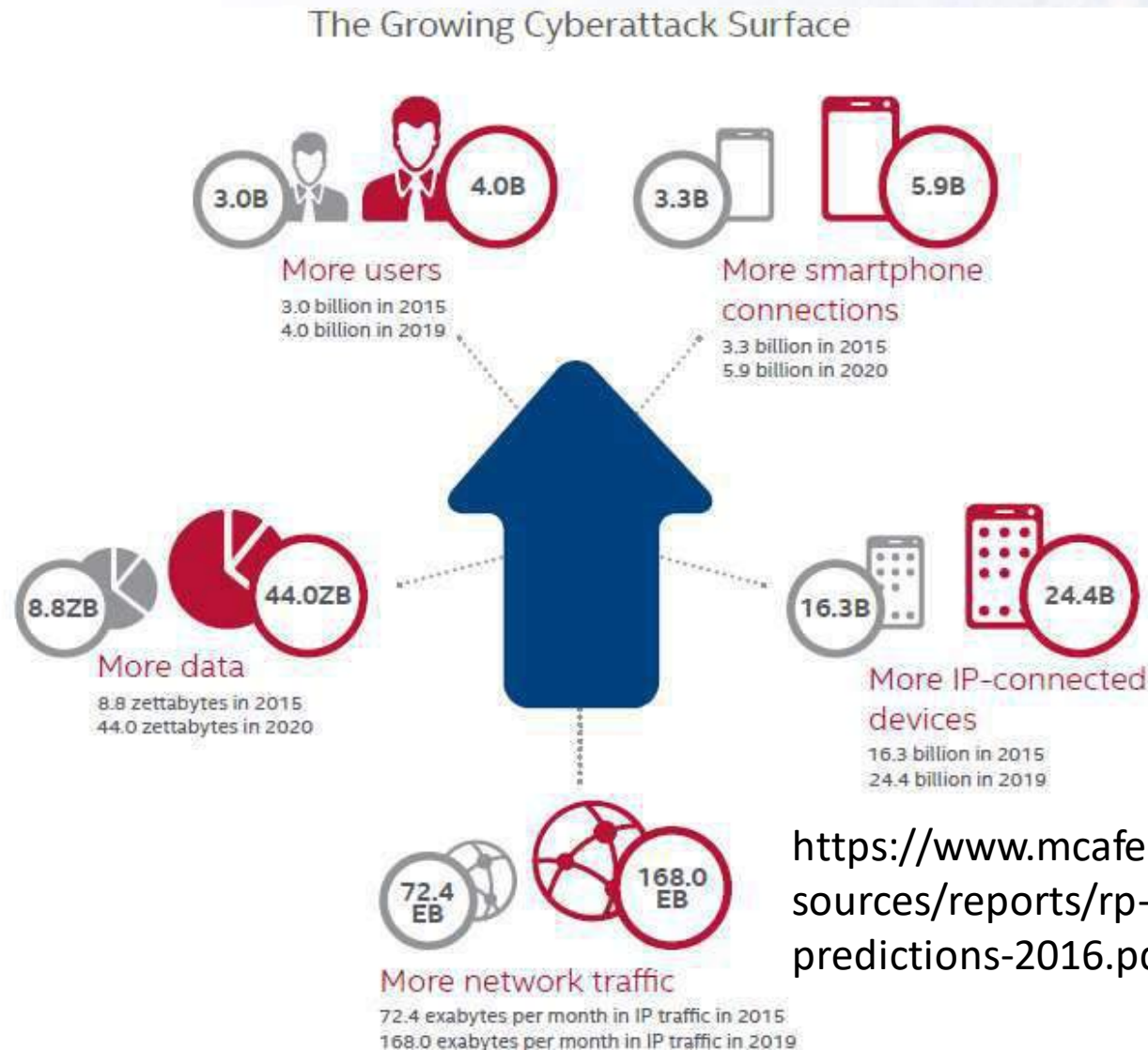
New IT Frontiers: Cloud, Mobile, Social, IOT

- IT dynamics are changing the way we communicate, work, and live
- These disruptive new IT frontiers have significant security consequences

New IT Frontiers: Cloud, Mobile, Social, IOT

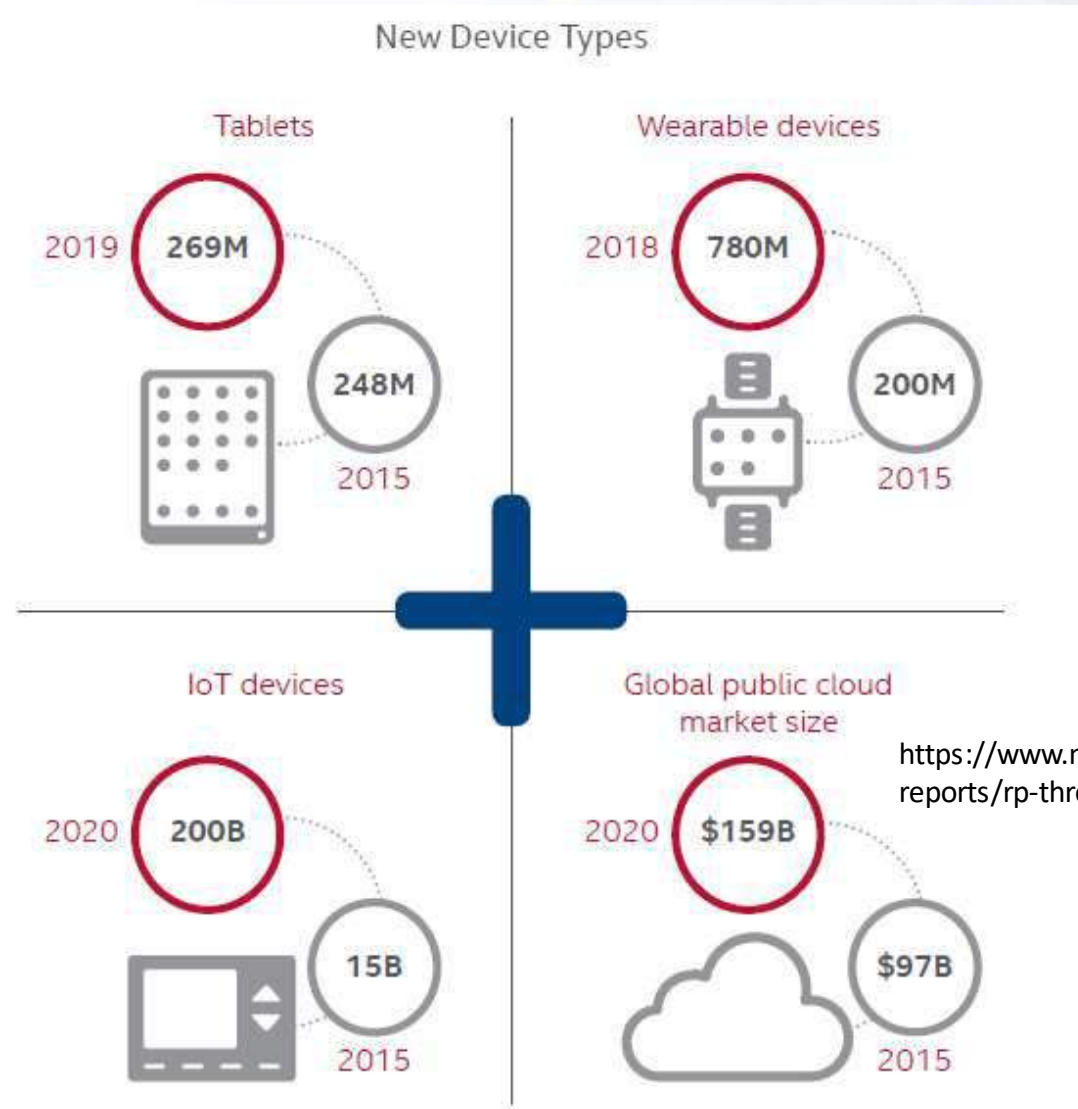


New IT Frontiers: Cloud, Mobile, Social, IOT



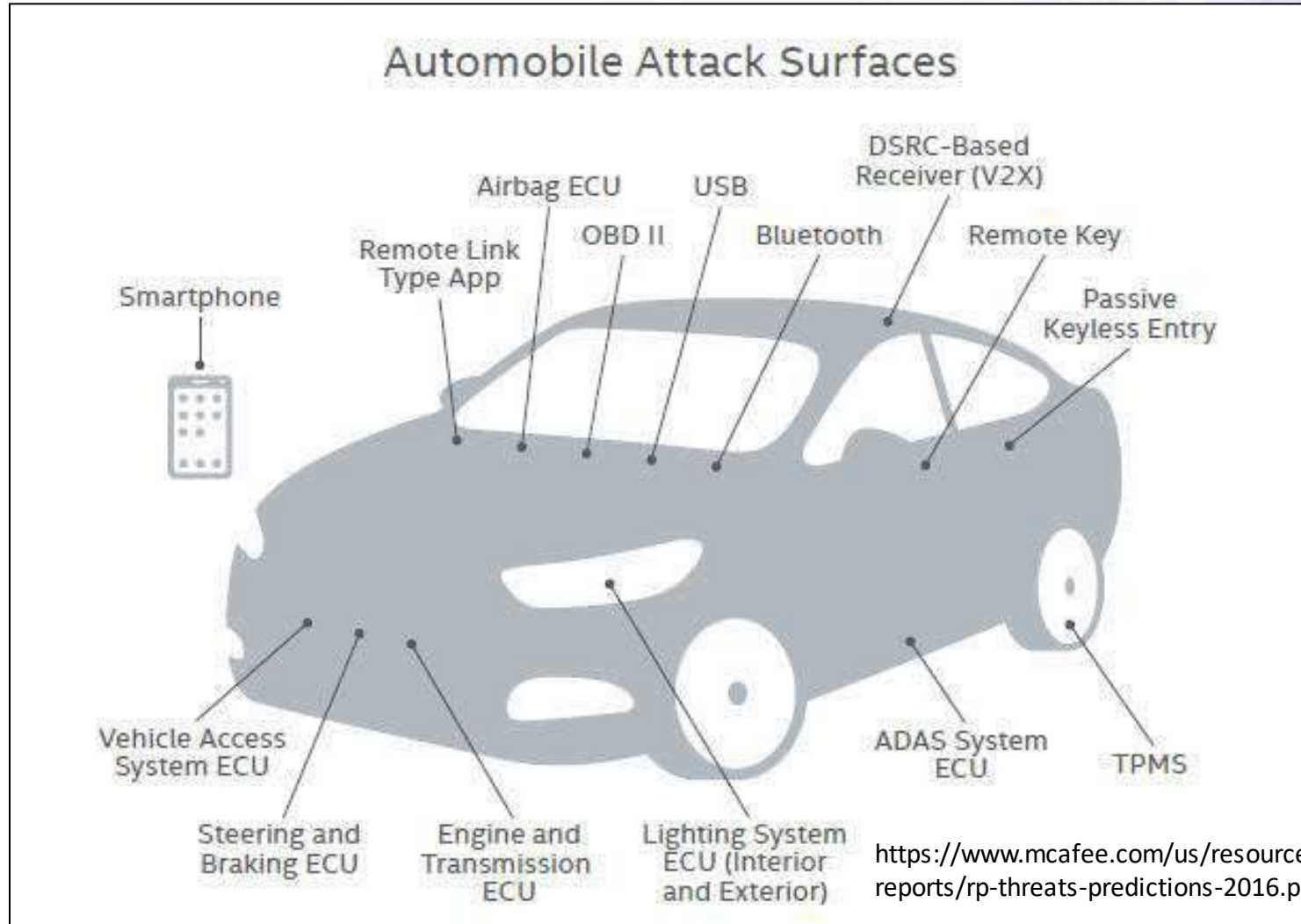
<https://www.mcafee.com/us/resources/reports/rp-threats-predictions-2016.pdf>

New IT Frontiers: Cloud, Mobile, Social, IOT



<https://www.mcafee.com/us/resources/reports/rp-threats-predictions-2016.pdf>

New IT Frontiers: Cloud, Mobile, Social, IOT

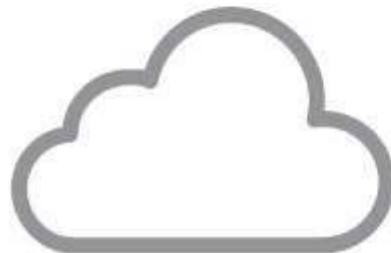


New IT Frontiers: Cloud, Mobile, Social, IOT

Wearables Attack Surfaces



- Operating system kernel
- Networking software/WiFi
- User interface
- Memory
- Local files and storage system
- Access control/security software



- Cloud virtual machine and control apps
- Web app
- Memory
- Local files and storage system
- Access control/security software

<https://www.mcafee.com/us/resources/reports/rp-threats-predictions-2016.pdf>

New IT Frontiers: Cloud, Mobile, Social, IOT

- For cloud, mobile, and IOT security guidance, checklists, and other details visit:
 - www.cloudsecurityalliance.org
 - www.owasp.org

New IT Frontiers: Cloud, Mobile, Social, IOT

- Useful URLs:
 - [https://www.owasp.org/index.php/OWASP Mobile Security Project](https://www.owasp.org/index.php/OWASP_Mobile_Security_Project)
 - [https://www.owasp.org/index.php/OWASP Internet of Things Project](https://www.owasp.org/index.php/OWASP_Internet_of_Things_Project)
 - <https://downloads.cloudsecurityalliance.org/assets/research/security-guidance/csaguide.v3.0.pdf>
 - [https://downloads.cloudsecurityalliance.org/initiatives/mobile/Mobile Guidance v1.pdf](https://downloads.cloudsecurityalliance.org/initiatives/mobile/Mobile_Guidance_v1.pdf)
 - [https://downloads.cloudsecurityalliance.org/assets/research/mobile/MAST White Paper.pdf](https://downloads.cloudsecurityalliance.org/assets/research/mobile/MAST_White_Paper.pdf)
 - [https://downloads.cloudsecurityalliance.org/whitepapers/Security Guidance for Early Adopters of the Internet of Things.pdf](https://downloads.cloudsecurityalliance.org/whitepapers/Security_Guidance_for_Early_Adopters_of_the_Internet_of_Things.pdf)
 - <https://downloads.cloudsecurityalliance.org/assets/research/internet-of-things/connected-vehicle-security.pdf>

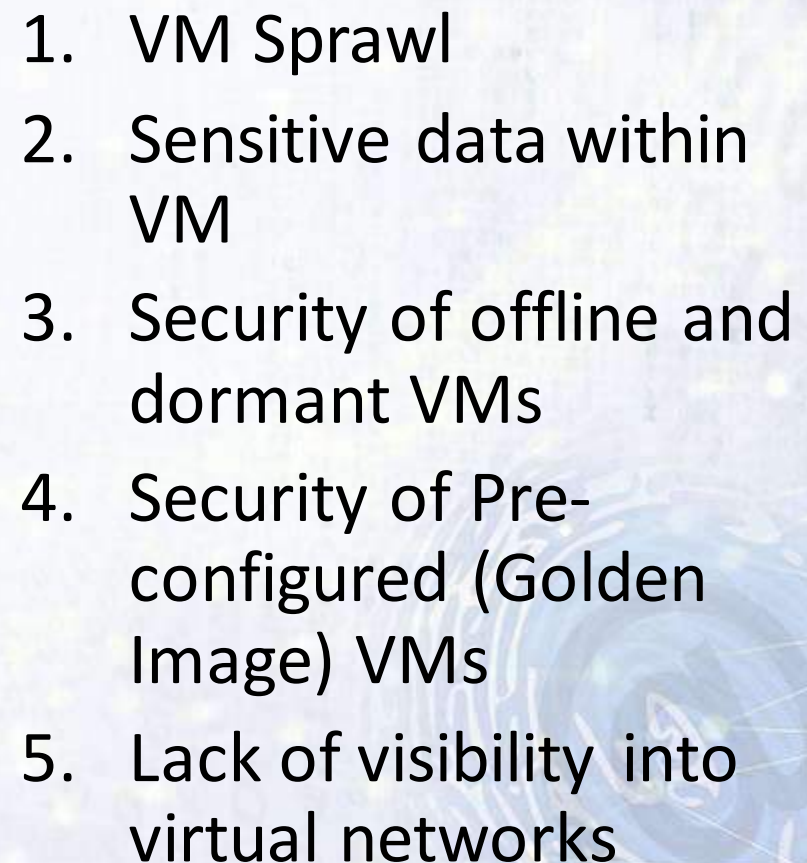
Virtualization Environment Security

- Cloud Security Alliance:
“Best Practices For
Mitigating Risks In
Virtual Environments”
(PDF)
- Virtualization security
classified into three
areas:
 - Architectural
 - Hypervisor software
 - Configuration

5.0 2.5 2.5 5.0 5.0 5.0

1000 2000 3000 4000 5000 6000 7000 8000 9000 10000



- 
- The background of the slide features a stylized globe with a network of white lines connecting various points, suggesting a global or networked environment. The globe is rendered in shades of blue and green, with the network lines in white. The overall aesthetic is modern and technological.
1. VM Sprawl
 2. Sensitive data within VM
 3. Security of offline and dormant VMs
 4. Security of Pre-configured (Golden Image) VMs
 5. Lack of visibility into virtual networks

Virtualization Environment Security

- Risk # 1 (VM Sprawl)
 - Impact: VMs can be created quickly, self-provisioned, or moved between physical servers, avoiding conventional change management process
 - Proliferation of VMs causing performance and security risks

Virtualization sprawl is a phenomenon that occurs when the number of virtual machines (VMs) on a network reaches a point where administrators can no longer manage them effectively. Virtualization sprawl is also referred to as virtual machine sprawl, VM sprawl or virtual server sprawl.

Virtualization Environment Security

- Risk # 1 (VM Sprawl)
 - Controls: Policies, procedures and governance of VM lifecycle management
 - Control creation, storage and use of VM images with a formal change management process
 - Discover VMs & apply security controls

Virtualization Environment Security

- Risk # 1 (VM Sprawl)
 - Controls: keep a small number of identified, good and patched images of a guest operating system separately for fast recovery & restoration of systems

Virtualization Environment Security

- Risk # 2 (Sensitive Data Within a VM)
 - Impact: VM images and snapshots can be copied easily via USB or console of hypervisor installed elsewhere

Virtualization Environment Security

- Risk # 2 (Sensitive Data Within a VM)
 - Controls: Encrypt data stored on virtual and cloud servers
 - Policies to restrict storage of VM images and snapshots
 - Image change management process with approvals
 - Logging & monitoring

Case Study – Enterprise Network (Small Org)

- Organizational characteristics:
 - Location: Karachi
 - 70 total staff
 - 10 IT staff
 - 8 servers
 - 1 main DC, no DR site
 - IT service oriented business delivered to banks, telcos, enterprises

Case Study – Enterprise Network (Small Org)

- Organizational culture:
 - Small IT oriented profitable business
 - Mostly chaotic culture with no defined or documented processes
 - Organization lacks discipline (execution)
 - Quality of resources: average

Case Study – Enterprise Network (Small Org)

- IT setup:
 - Windows 2010/2012, Linux server OS
 - ASP.net 4.x, PHP applications (total 10)
 - Windows 8/10 desktops (50+)
 - 1 Cisco ASA FW in DC
 - No DR site or offsite backup
 - Free AV, no AD, no licenses

Case Study – Enterprise Network (Small Org)

- Security posture:
 - Completely absent
 - No hardening done
 - No vulnerability management
 - No security management or governance
 - No policy or staff dedicated for
 - No management commitment (prior)

Case Study – Enterprise Network (Small Org)

- Security requirement:
 - Customers are banks and telcos
 - Desired ISO27001:2013 (ISMS) certification for customer RFPs

Case Study – Enterprise Network (Small Org)

- Driving change ?
 - Executive management facing security questions from top clients
 - COO approaches security consulting company for pen-testing
 - Consultant advises project for security transformation

Case Study – Enterprise Network (Small Org)

- Security transformation project:
 - Project initiation: 2 Mths
 - Layer 1: security hardening of IT assets (6 Mths)
 - Layer 2: VM (1 Mth)
 - Layer 3: security engineering (1 Mth)
 - Layer 4: Governance & ISO cert.(3 Mths)

Case Study – Enterprise Network (Small Org)

- Conclusion:
 - Absence of a process oriented, organized culture makes it difficult for security implementation
 - Adhoc culture is difficult to transform
 - Executive management support and commitment was the success factor

Case Study – Enterprise (Medium Org)

- Organizational characteristics:
 - Location: Lahore
 - 350 total staff (group)
 - 15+ IT staff
 - 25 servers
 - 1 main DC, 1 DR site, 1 backup site
 - IT service business in media industry

Case Study – Enterprise (Medium Org)

- Organizational culture:
 - Medium sized, profitable IT business
 - Good internal culture (several employees with org since 10 yrs)
 - Organization lacks processes
 - Teams have execution discipline
 - Senior resources are experienced

Case Study – Enterprise (Medium Org)

- IT setup:
 - Windows 2010/2012, Linux server OS
 - Oracle & MS-SQL databases
 - ASP.net 4.x applications (total 15)
 - Windows 8/10 desktops (300+)
 - 1 Cisco ASA FW in DC; MicroTik routers as edge routers

Case Study – Enterprise (Medium Org)

- IT setup (contd):
 - Asterisk voice server for call center (10 seats, 6-8 lines)
 - 1 DR site (offshore) and 1 backup site (PK)
 - Panda AV, AD, unlicensed windows
 - Mdaemon for email server, migrating to MS Exchange

Case Study – Enterprise (Medium Org)

- Security posture:
 - Completely absent
 - No hardening done
 - No vulnerability management
 - No security management or governance
 - No policy or staff dedicated for security
 - No management commitment (prior)

Case Study – Enterprise (Medium Org)

- Security requirement:
 - Security incident; competitive data leakage to third-party by internal employee
 - License renewal due by regulator; demonstration of security commitment imperative

Case Study – Enterprise (Medium Org)

- Driving change ?
 - Executive management concerned about information security & security culture
 - CEO approaches security consulting company
 - Consultant advises project for security transformation

Case Study – Enterprise (Medium Org)

- Security transformation project:
 - Project initiation: 15 days
 - Layer 1: security hardening of IT assets (3 Mths)
 - Layer 2: VM (1 Mth)
 - Layer 3: security engineering (4 Mths)
 - Layer 4: Governance & ISO cert.(3 Mths)

Case Study – Enterprise (Medium Org)

- Conclusion:
 - Senior resources in the organization were committed
 - Demonstration of security commitment was essential for organizations survival
 - ISO27001:2013 (ISMS) serves as credible credential for customers/regulator

Case Study – Enterprise (Large Org)

- Organizational characteristics:
 - Location: Karachi
 - 10,000+ total staff
 - 150 IT staff
 - 200 servers
 - 1 main DC, 1 DR site
 - Energy & distribution sector

Case Study – Enterprise (Large Org)

- Organizational culture:
 - Large sized privatized org
 - Strong internal culture
 - Organization lacks process culture
 - Teams have high execution discipline
 - Good quality & qualification of IT resources

Case Study – Enterprise (Large Org)

- IT setup:
 - Windows 2010/2012, Linux, AIX OS
 - Oracle & MS-SQL databases
 - Over 100 internal applications (Sharepoint, GIS, ASP.net)
 - Windows 7/8/10 desktops (5500+)

Case Study – Enterprise (Large Org)

- IT setup (contd):
 - Asterisk voice server for voice communication
 - 1 DR site (hosted)
 - Licensed AV, AD, & windows
 - Complete SAP ERP suite & internal development

Case Study – Enterprise (Large Org)

- Security posture:
 - Superficial
 - No hardening done
 - Weak vulnerability management
 - Poor security management/governance
 - Security team exists
 - No management commitment (prior)

Case Study – Enterprise (Large Org)

- Security requirement:
 - Security incident;
servers hacked
causing financial loss

Case Study – Enterprise (Large Org)

- Driving change ?
 - Executive management concerned about information security & security culture
 - Board drives IT to hire consultant
 - Consultant convinces IT to go for security transformation

Case Study – Enterprise (Large Org)

- Security transformation project:
 - Project initiation: 15 days
 - Layer 1: security hardening of IT assets (6 Mths)
 - Layer 2: VM (1 Mth)
 - Layer 3: security engineering (1 Mths)
 - Layer 4: Governance & ISO cert.(5 Mths)

Case Study – Enterprise (Large Org)

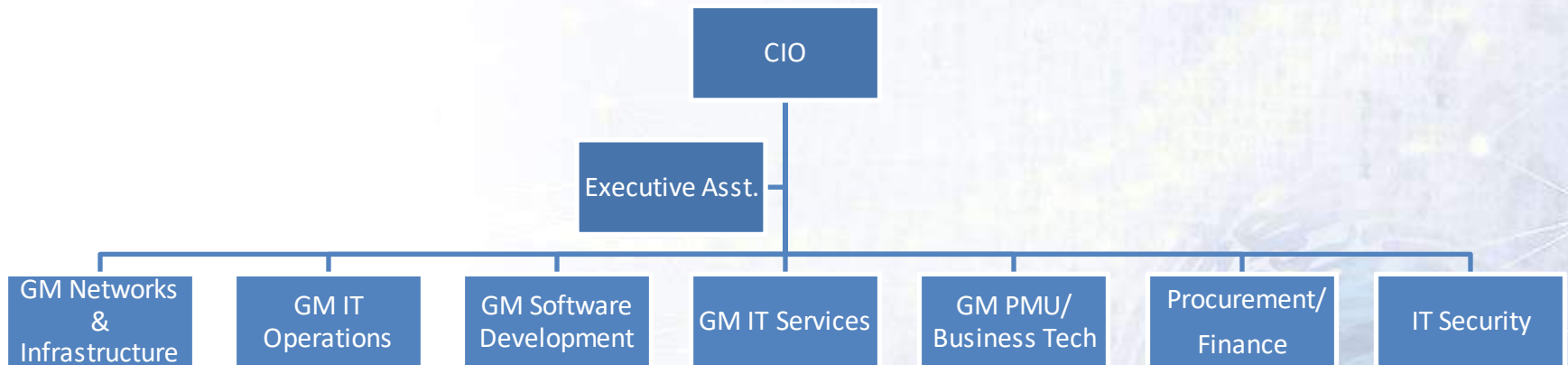
- Conclusion:
 - Strong commitment of the Board & IT Director drove the implementation of the security transformation project
 - ISO27001:2013 (ISMS) achieved as a security credential

Structure Of An IT Team

- Typical organogram of an IT team
- Job functions
- Additional tasks
- Large sized org
- Medium sized org
- Small sized org

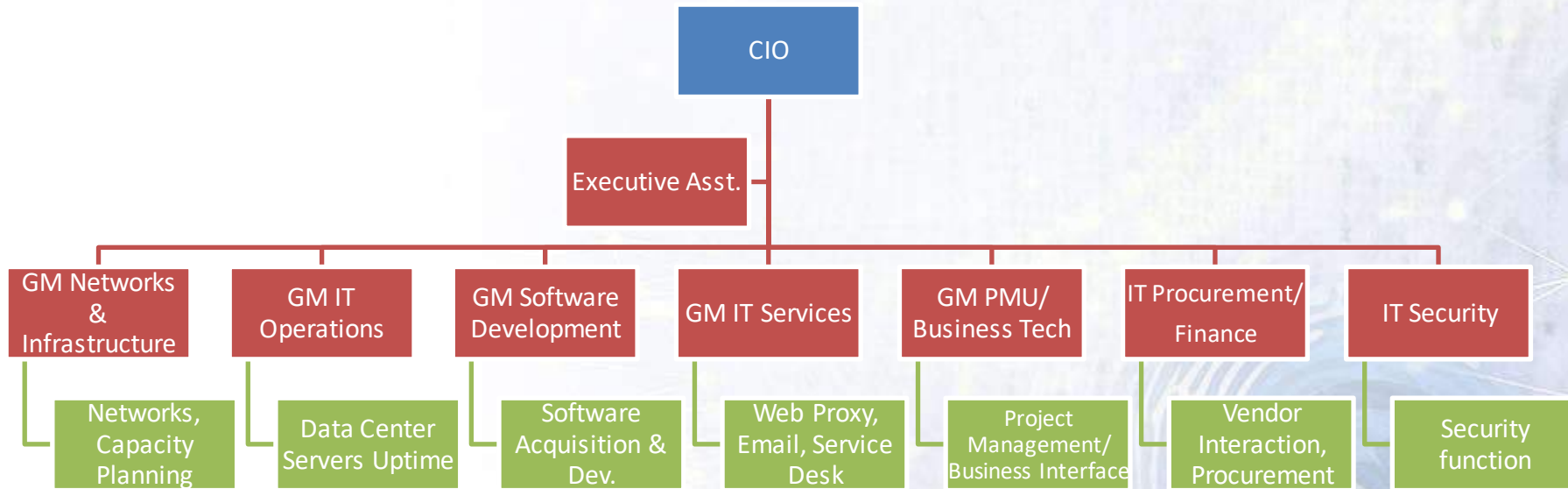
Structure Of An IT Team

GENERAL STRUCTURE



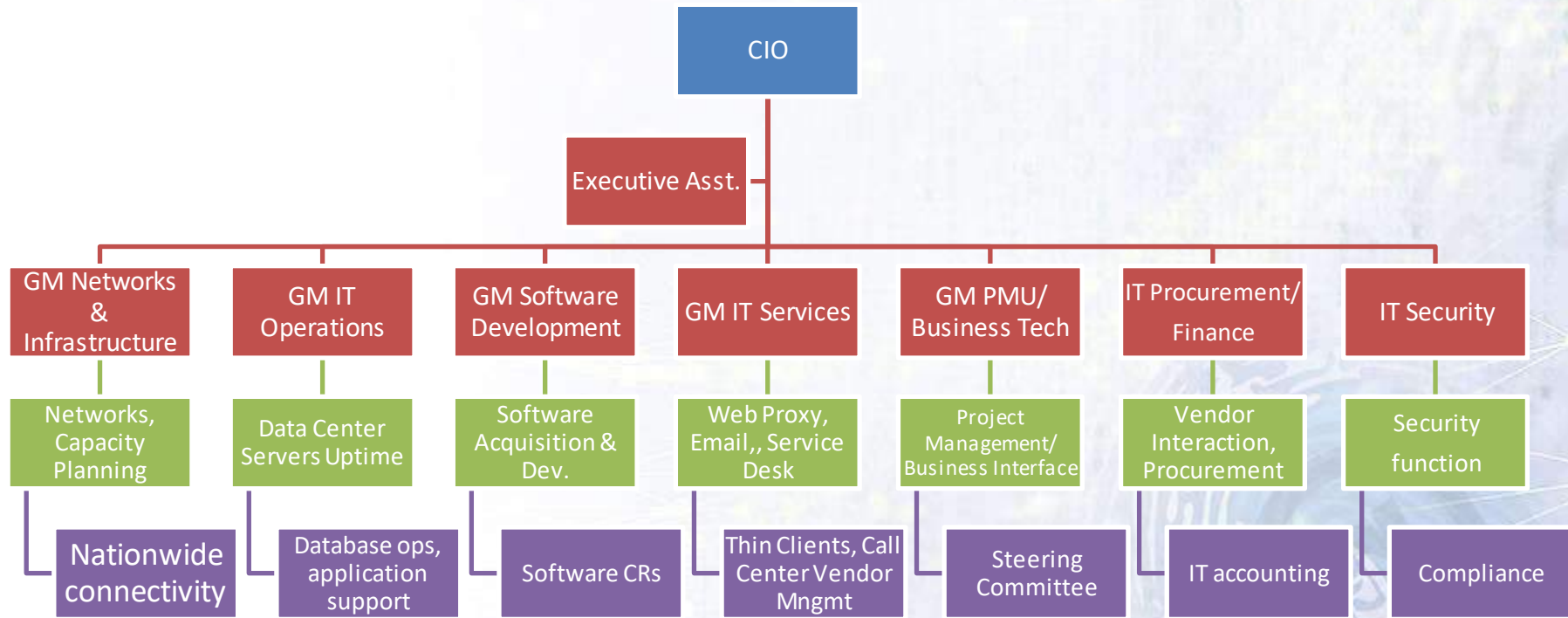
Structure Of An IT Team

JOB FUNCTIONS



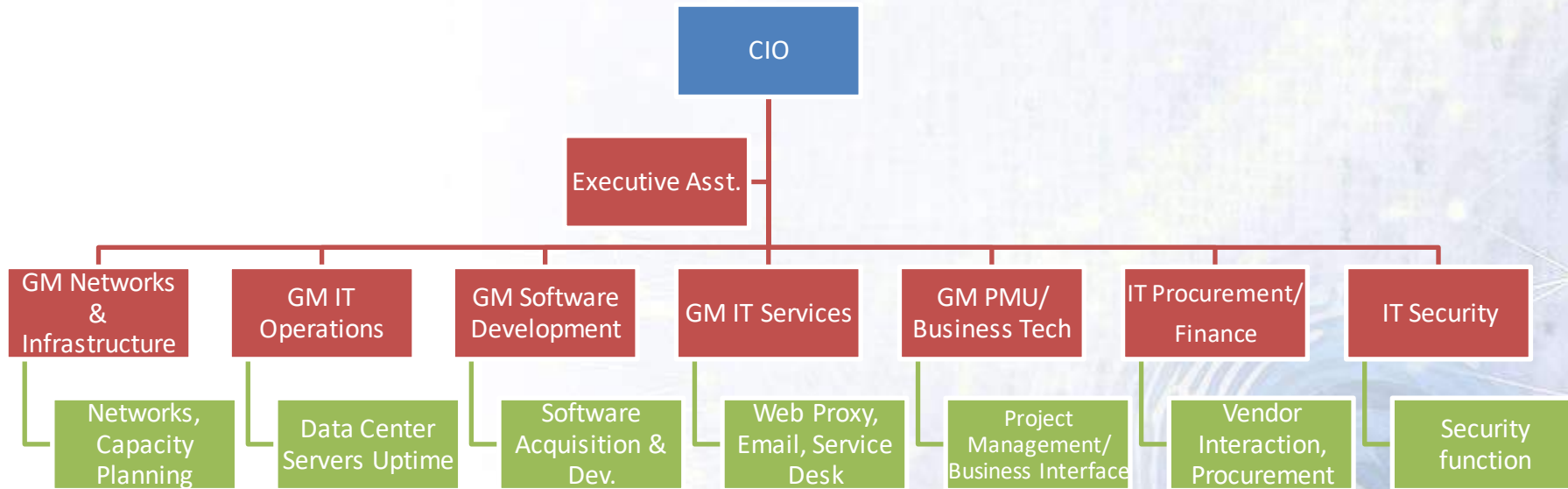
Structure Of An IT Team

ADDITIONAL TASKS



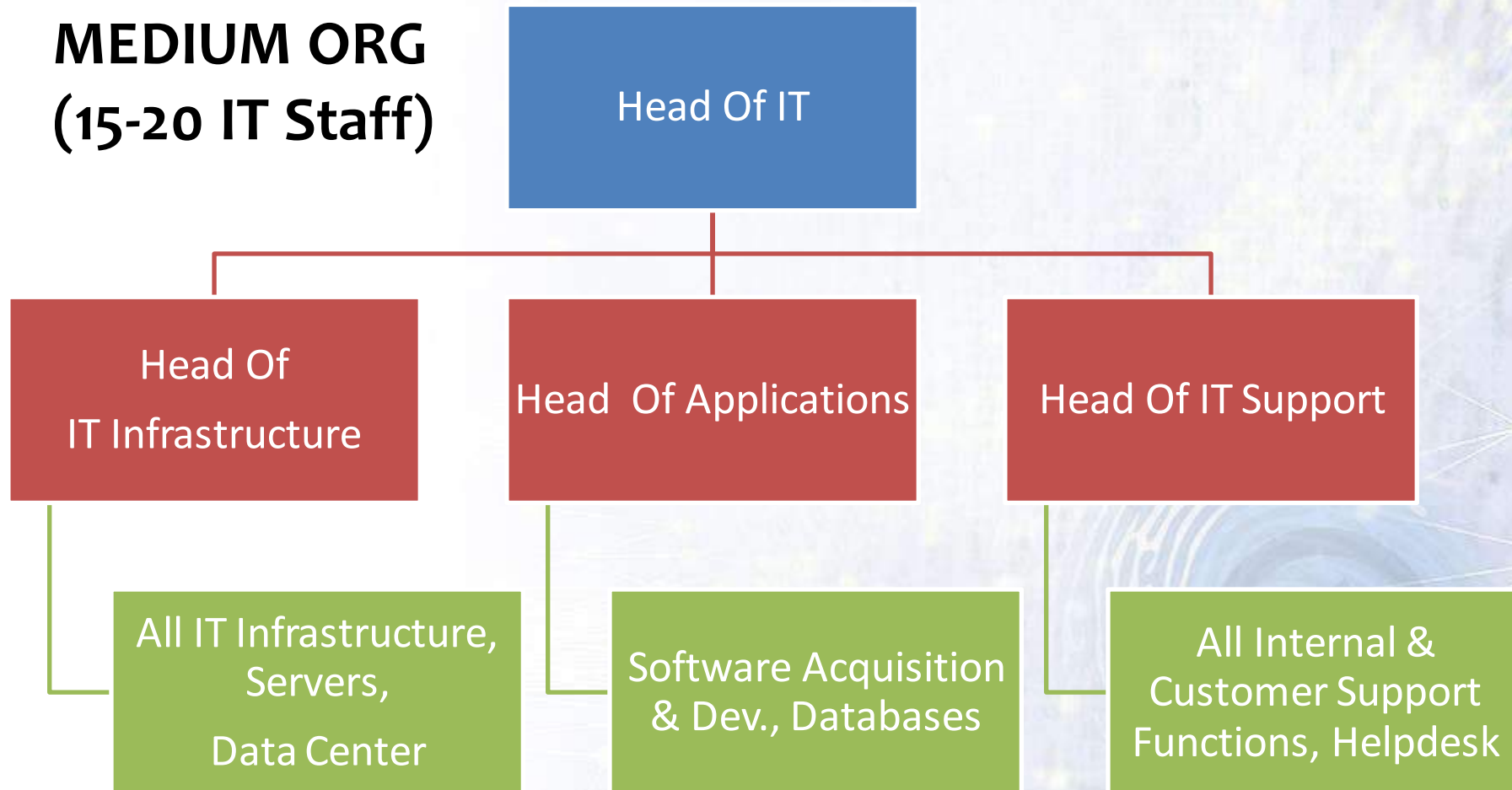
Structure Of An IT Team

LARGE ORG (150 IT Staff)



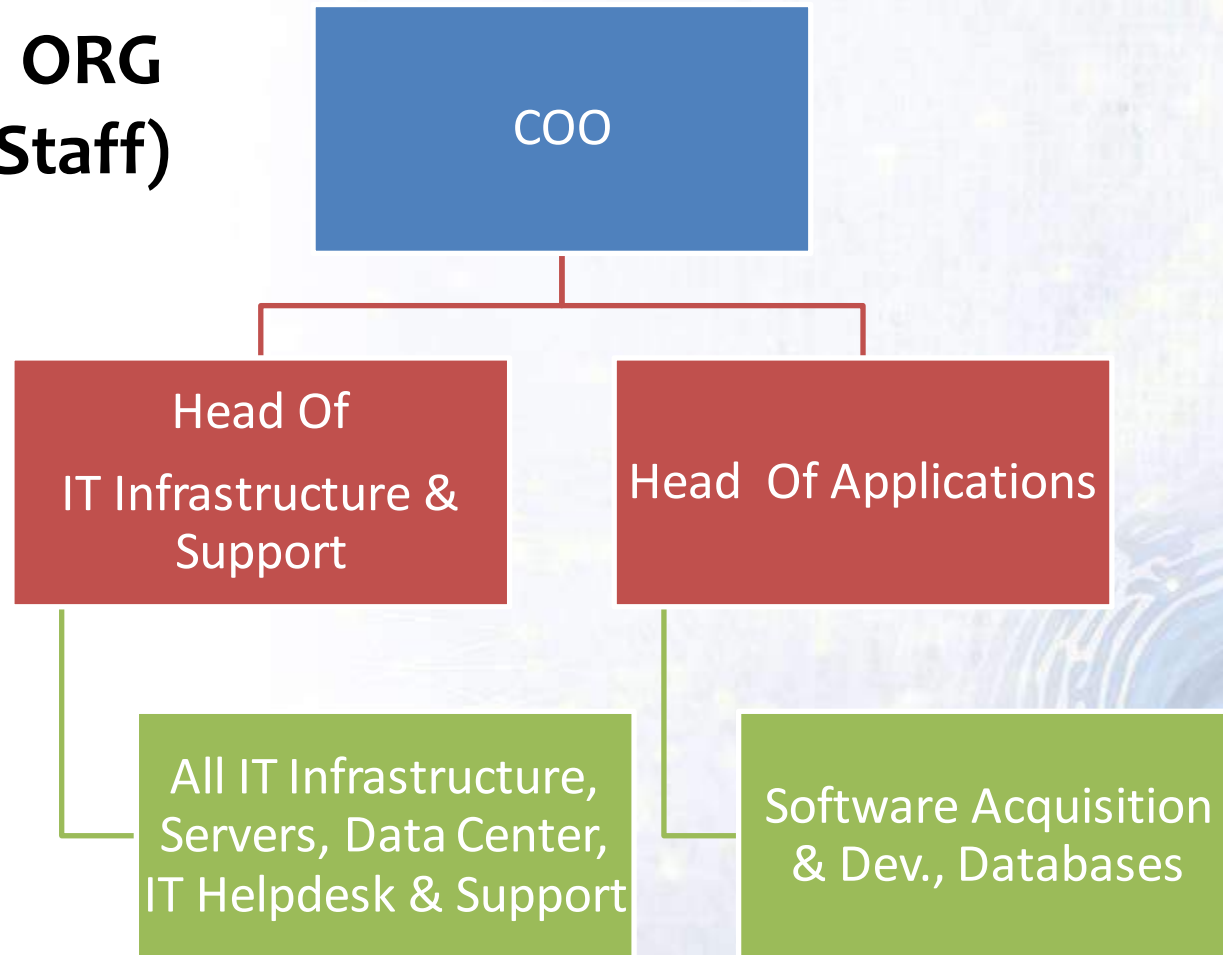
Structure Of An IT Team

**MEDIUM ORG
(15-20 IT Staff)**



Structure Of An IT Team

**SMALL ORG
(7-8 IT Staff)**



Structure Of An IT Team

- IT teams come in various structures, however there are set industry best-practices and organizations should follow tried & tested best-practices
- IT is today an enabler forming the engine for business automation, but also carries with it security hazards

Objectives, Performance KPIs, Priorities Of IT

- IT is a challenging domain which requires skill, experience, structure, and spending to run efficiently
- Business is making steep demands on IT for agile delivery of applications in order to keep up with competition
- Running IT requires a diverse skillset

Objectives, Performance KPIs, Priorities Of IT

- Primary objective set for IT by management is to:
 - Setup the infrastructure with least cost in the minimum time
 - To maintain the network with minimum disruption and maximum performance requiring the least resources

Objectives, Performance KPIs, Priorities Of IT

- Performance KPIs:
 - Minimal network disruption
 - Timely completion of new projects
 - Quick and efficient changes to existing applications (change-requests) to meet business requirements

Objectives, Performance KPIs, Priorities Of IT

- Priorities of IT:
 - To meet the performance KPIs
 - To meet adhoc and unplanned business requirements
- Note that security figures nowhere in the objectives, performance KPIs, or priorities of IT teams

Objectives, Performance KPIs, Priorities Of IT

- General IT teams performance in Banking:
 - Extremely large number of applications (hundreds) & legacy
 - Heavy-weight business teams and IT seen as a cost-center
 - Technologists generally poor at banking (business)

Objectives, Performance KPIs, Priorities Of IT

- General IT teams performance in Telcos:
 - More professional and qualified workforce
 - Most telco have been setup in the last 10 years so have clean greenfield networks (no legacy)
 - Fewer applications; IT supports business

Objectives, Performance KPIs, Priorities Of IT

- General IT teams performance in Enterprise:
 - Competence and professionalism of IT teams matches culture of organization
 - IT efficiency driven by top management commitment and interest

Objectives, Performance KPIs, Priorities Of IT

- Security posture:
 - Surprisingly in 95% of all orgs in Pakistan (all types and sizes), security posture has been found to be deficient
 - Lack of awareness in the country has contributed to this deficient and poor security posture

IT Team Interaction With Other Stakeholders

- IT budget/projects approved by IT Steering Committee (annual)
- Business requirements & new projects
- Audit & compliance requirements
- Expansion (branches) & maintenance
- IT support for computing (helpdesk)
- Business continuity & DR

IT Team Interaction With Other Stakeholders

- IT budget/projects approved by IT Steering Committee (annual):
 - Capex and opex layout
 - Includes new projects & licensing/maintenance of operations
 - New hirings

IT Team Interaction With Other Stakeholders

- Business requirements & new projects:
 - New upcoming business projects
 - Change requests (CRs) and expansion of existing business projects
 - Vendor management for business solutions
 - UAT (testing) of business applications

IT Team Interaction With Other Stakeholders

- Audit & compliance requirements:
 - External audit
 - Internal audit
 - Compliance
 - Information security & risk depts

IT Team Interaction With Other Stakeholders

- Expansion (branches) & maintenance:
 - IT requirements for business expansion (new branches, new locations, new territories)
 - Maintenance of existing IT infrastructure (UPS, networking, bandwidth circuits)

IT Team Interaction With Other Stakeholders

- IT support for computing (helpdesk):
 - New software and versions rollout (e.g. migration of AV or email program)
 - IT support for business functions (application not working, speed slow, etc)
 - Software bugs

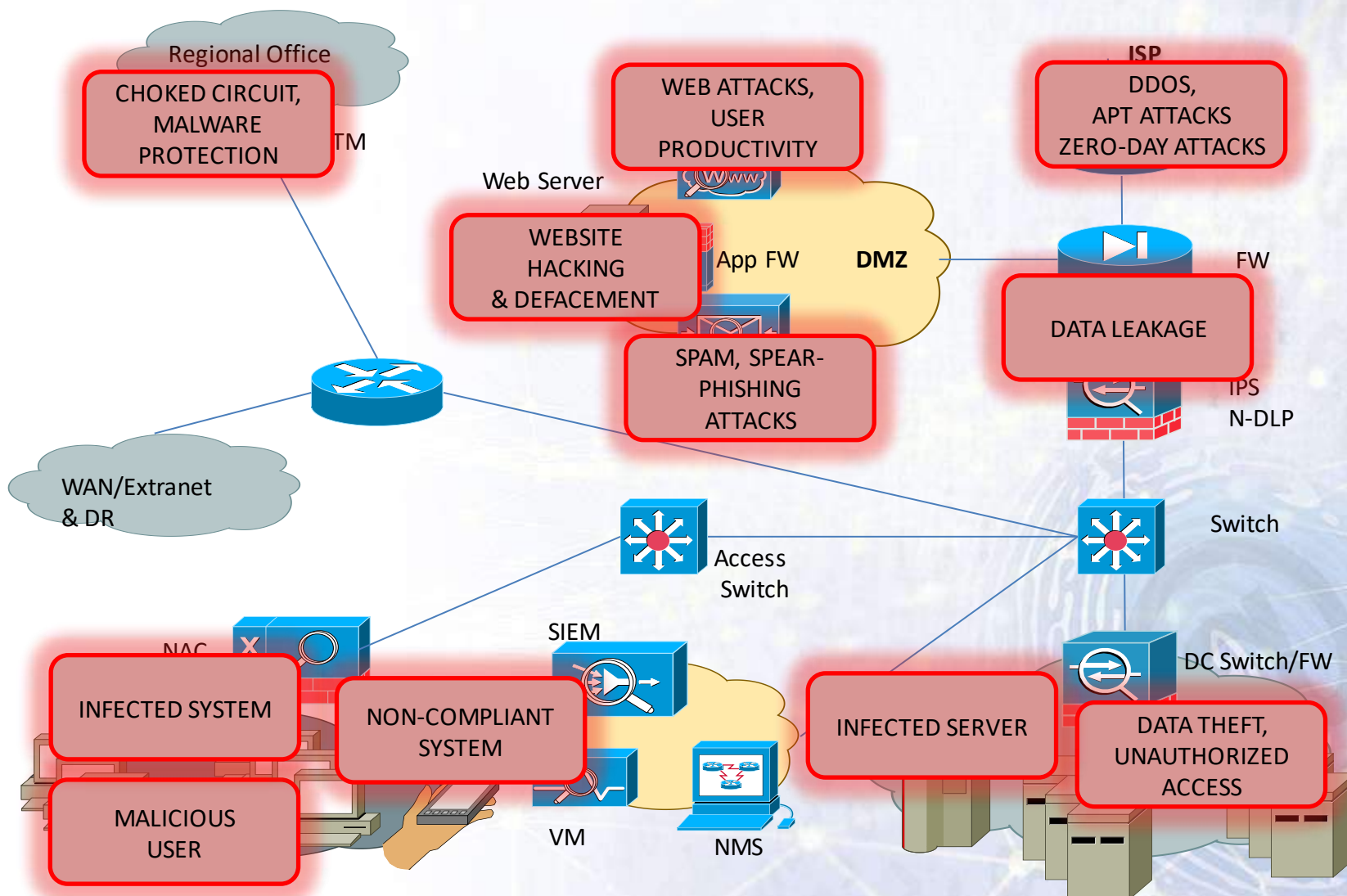
IT Team Interaction With Other Stakeholders

- Business continuity & DR:
 - DR is a technology function for which interaction with business functions is required (testing)
 - Business continuity is handled under business operations for which IT also participates

Security Overlay Of Enterprise (Part 1)

- How is the enterprise secured with the help of various components and security design ?

Security Overlay Of Enterprise (Part 1)



Security Overlay Of Enterprise (Part 1)

Security Challenge	Location/Device	Security Solution
Perimeter Filtering	Edge Router	Access Lists & Various RFCs
DDOS Attack	Edge Router/DDOS Protection Solution	DDOS Protection
Zero-Day Attack / APT Attack	Edge Device / Edge NGN FW	Zero-Day/APT Attack Prevention
Web Server Attacks	DMZ / Web Application FW	Web Application Attack Prevention
Email SPAM & Malware/Phishing	DMZ / Email Security GW	Email Security

Security Overlay Of Enterprise (Part 1)

Security Challenge	Location/Device	Security Solution
Web-based User Attacks	DMZ / Web Security GW	Web Filtering & Malware Protection
System Malware	System	AV
User Network Access Control	At Aggregation Point Of User Access	Network Admission Control (NAC)
User Controls For USB/Media, HDD Encrypt	System	Data Loss Prevention (DPL) – System Level
Remote Branch Connectivity/ Malware	Intranet-Extranet Edge / UTM	Unified Threat Management (UTM) Solution

Security Overlay Of Enterprise (Part 1)

Security Challenge	Location/Device	Security Solution
Data Center Unauthorized Access / Malware	Data Center FW	Data Center FW Filtering & Malware Protection
Data Exfiltration	Edge / Network DLP	Network DLP Solution
Event Monitoring & Detection	Data Center / SIEM	Security Info. & Event Management
Unpatched Systems	Data Center / VM	Vulnerability Scanner
Server Integrity Monitoring & IPS Filtering	Data Center / HIPS	Host Intrusion Prevention System (HIPS)

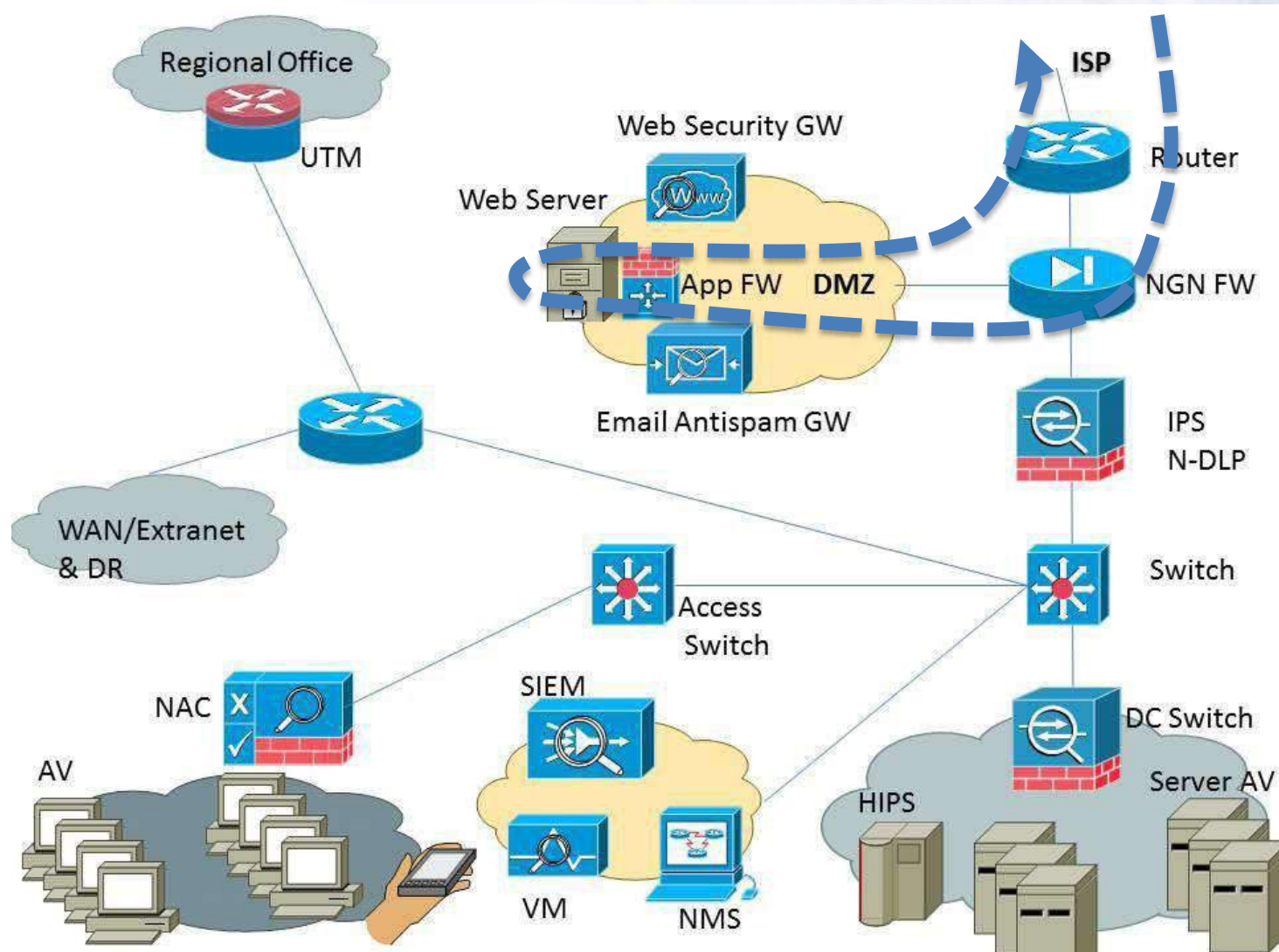
Security Overlay Of Enterprise (Part 1)

- How is the enterprise secured with the help of various components and security design ?

Security Overlay Of Enterprise (Part 2)

- What are the traffic flows specific to good security design ?

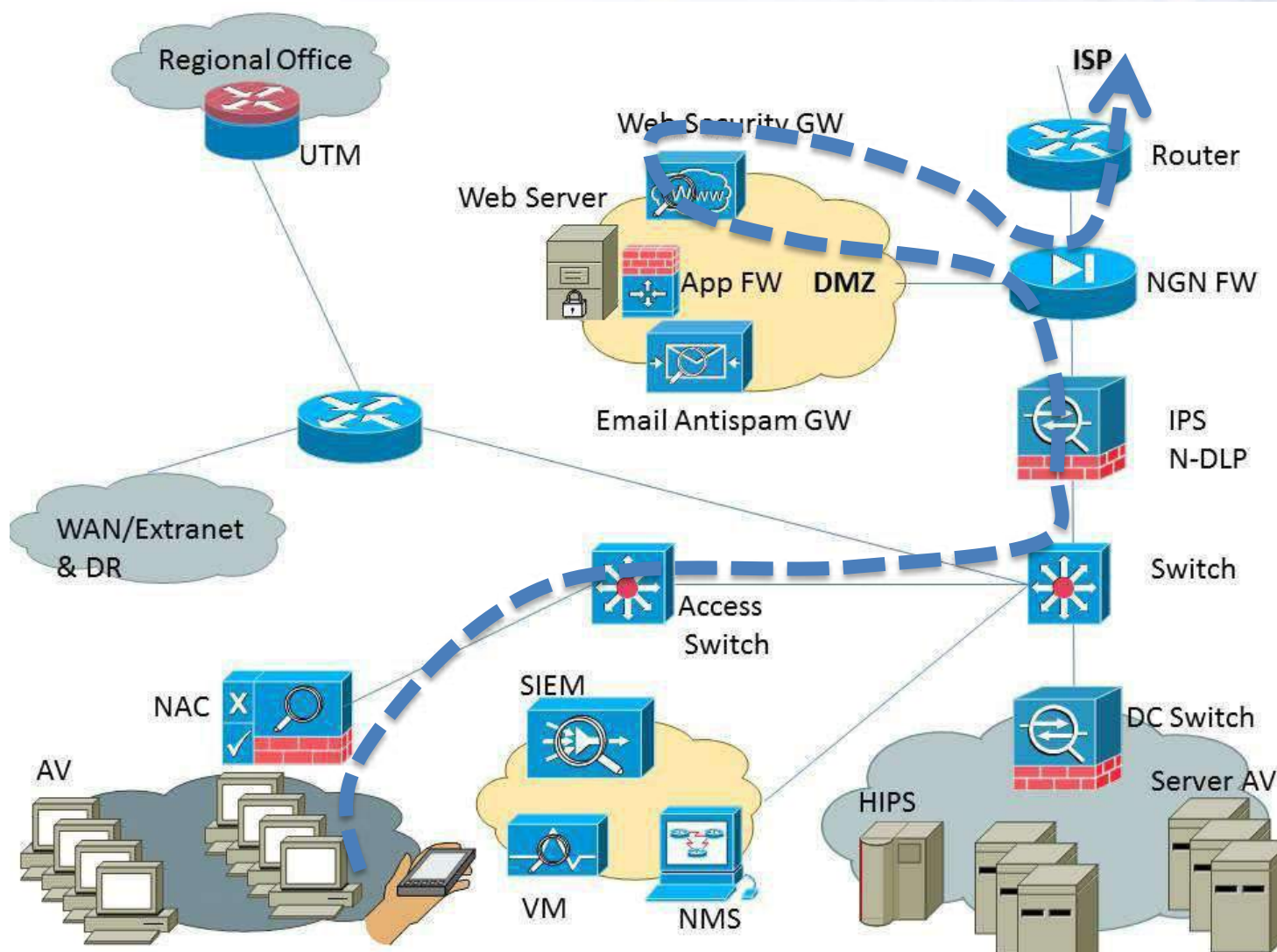
Security Overlay Of Enterprise (Part 2)



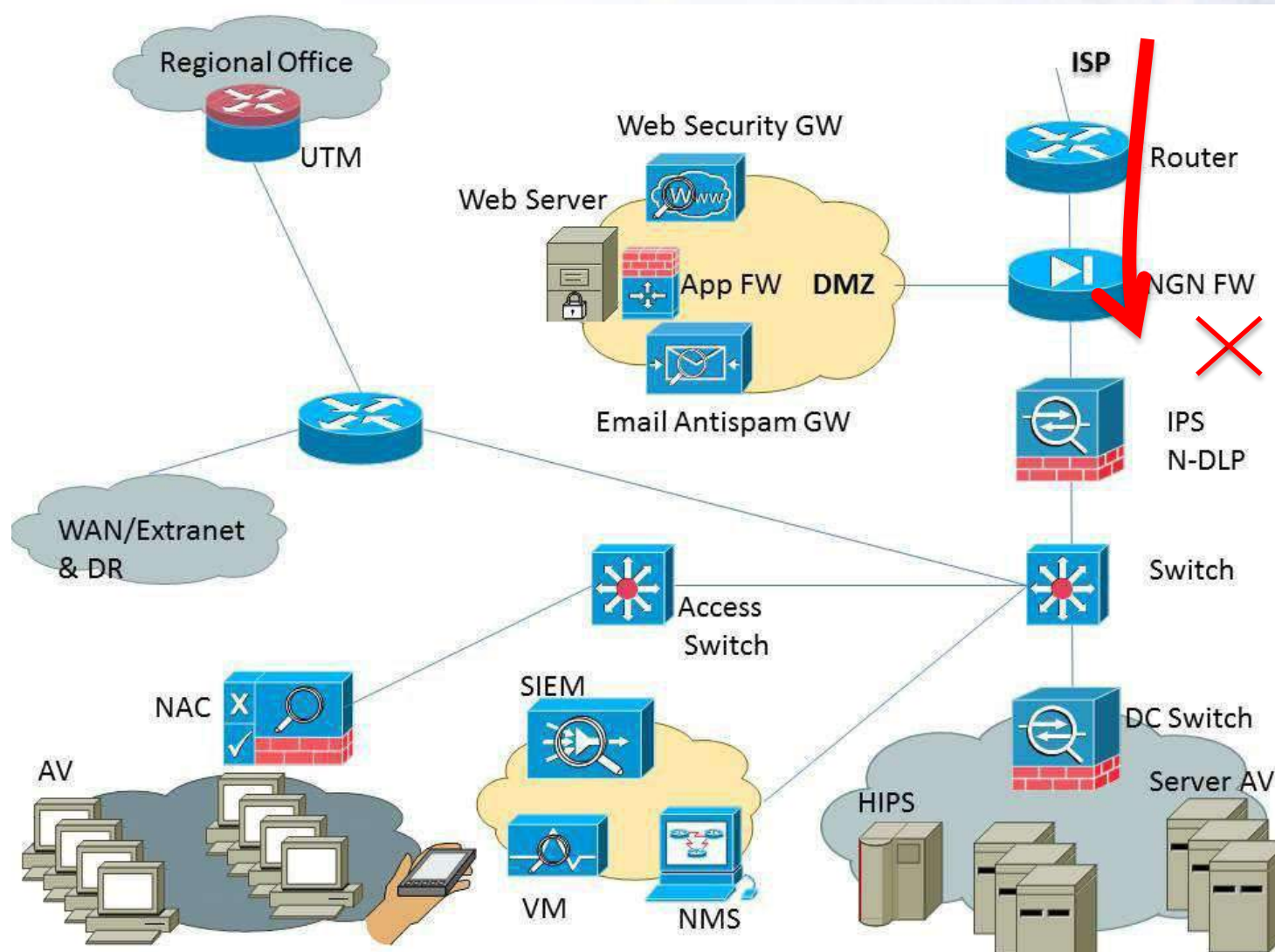
1	2	3	4	5	6	7	8



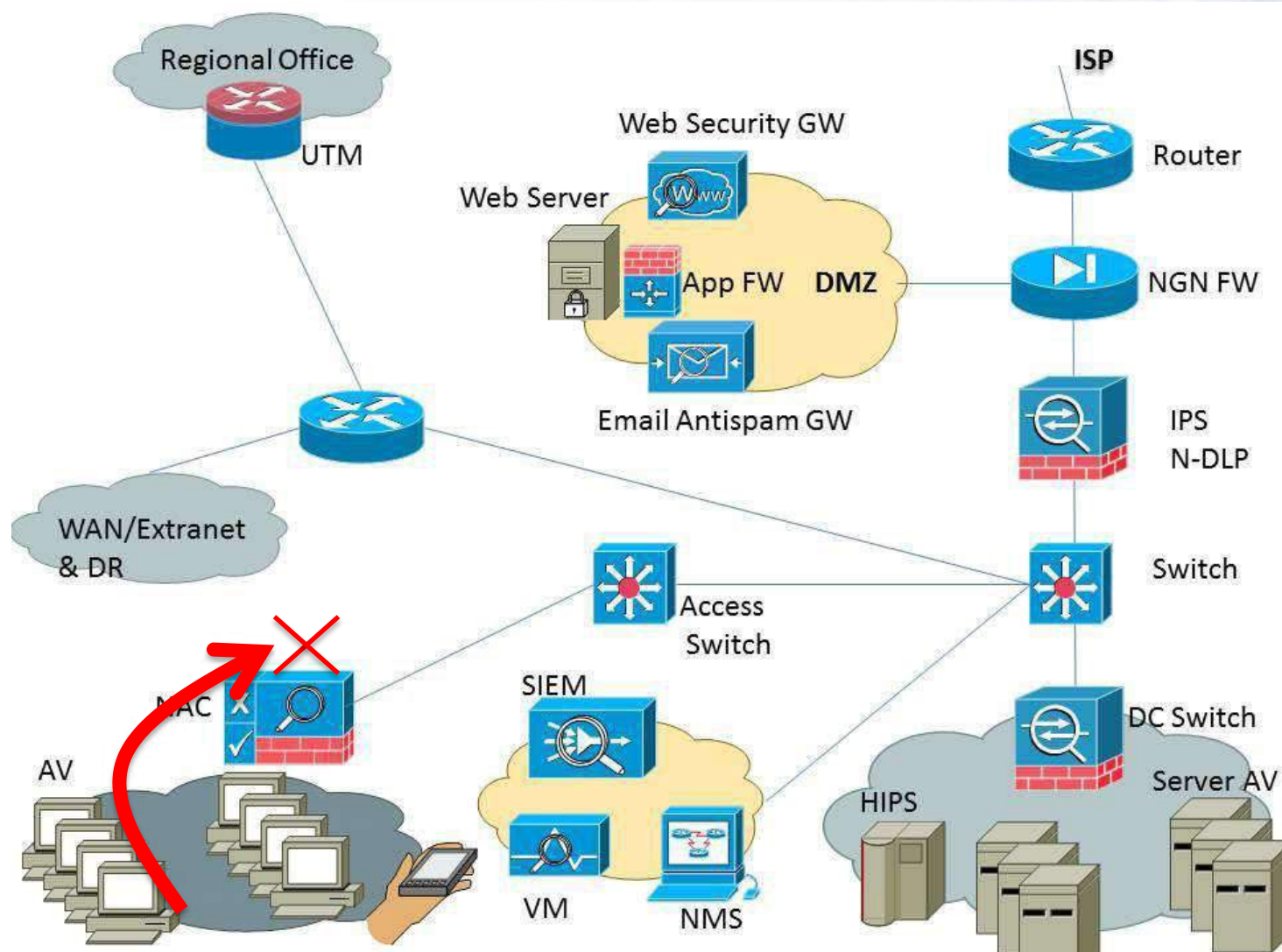
Security Overlay Of Enterprise (Part 2)



Security Overlay Of Enterprise (Part 2)



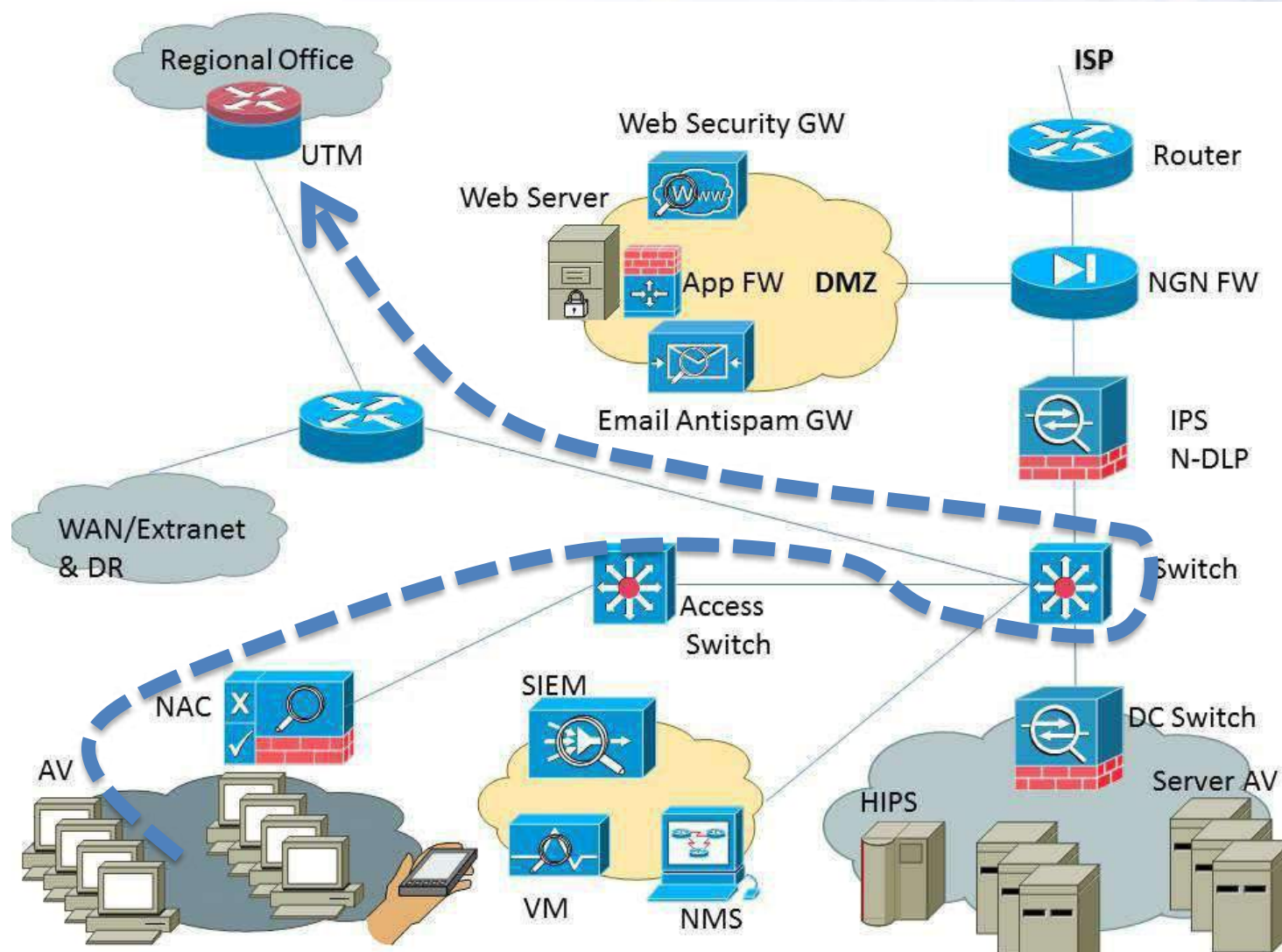
Security Overlay Of Enterprise (Part 2)



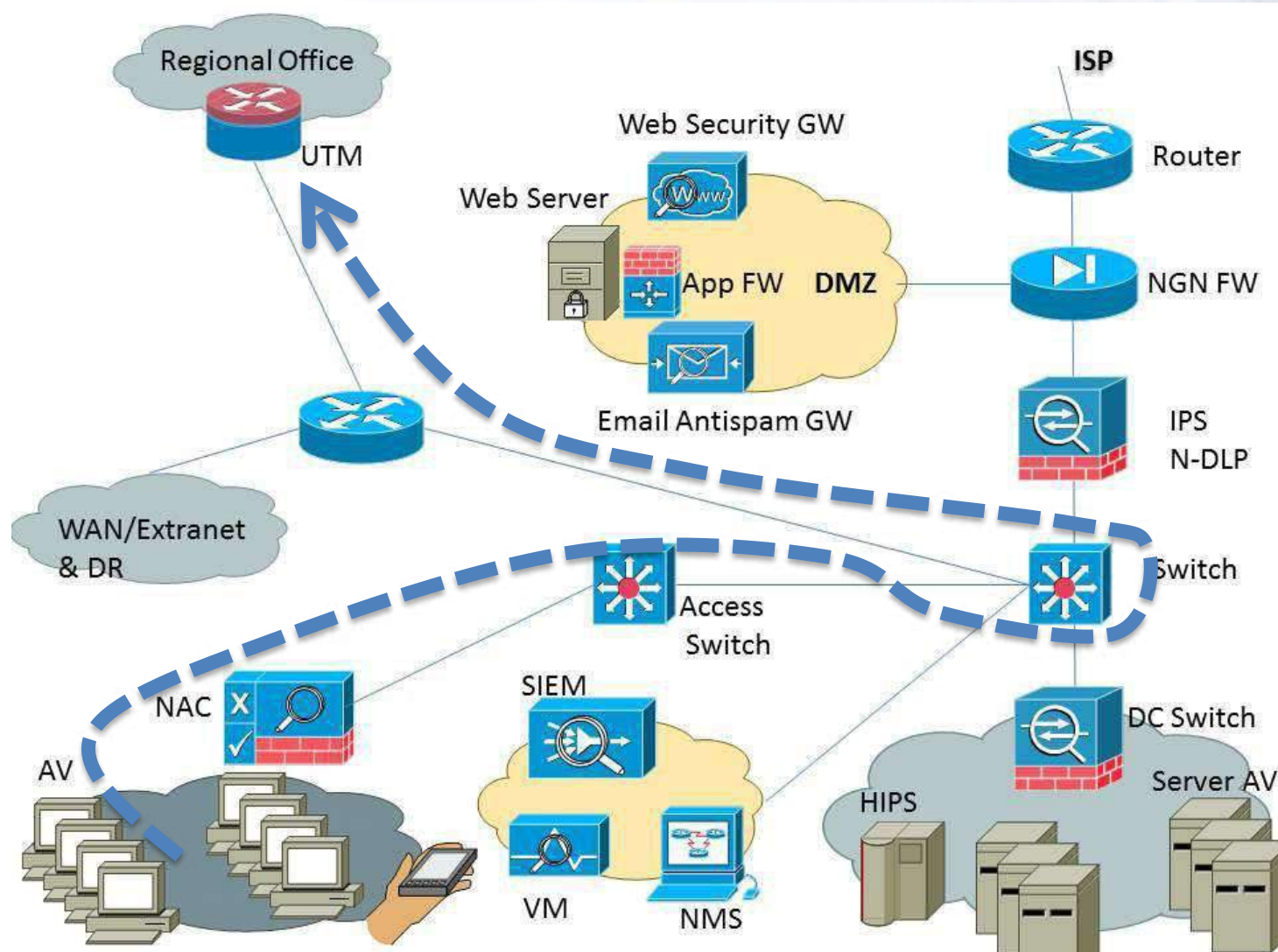
1	2	3	4	5	6	7	8



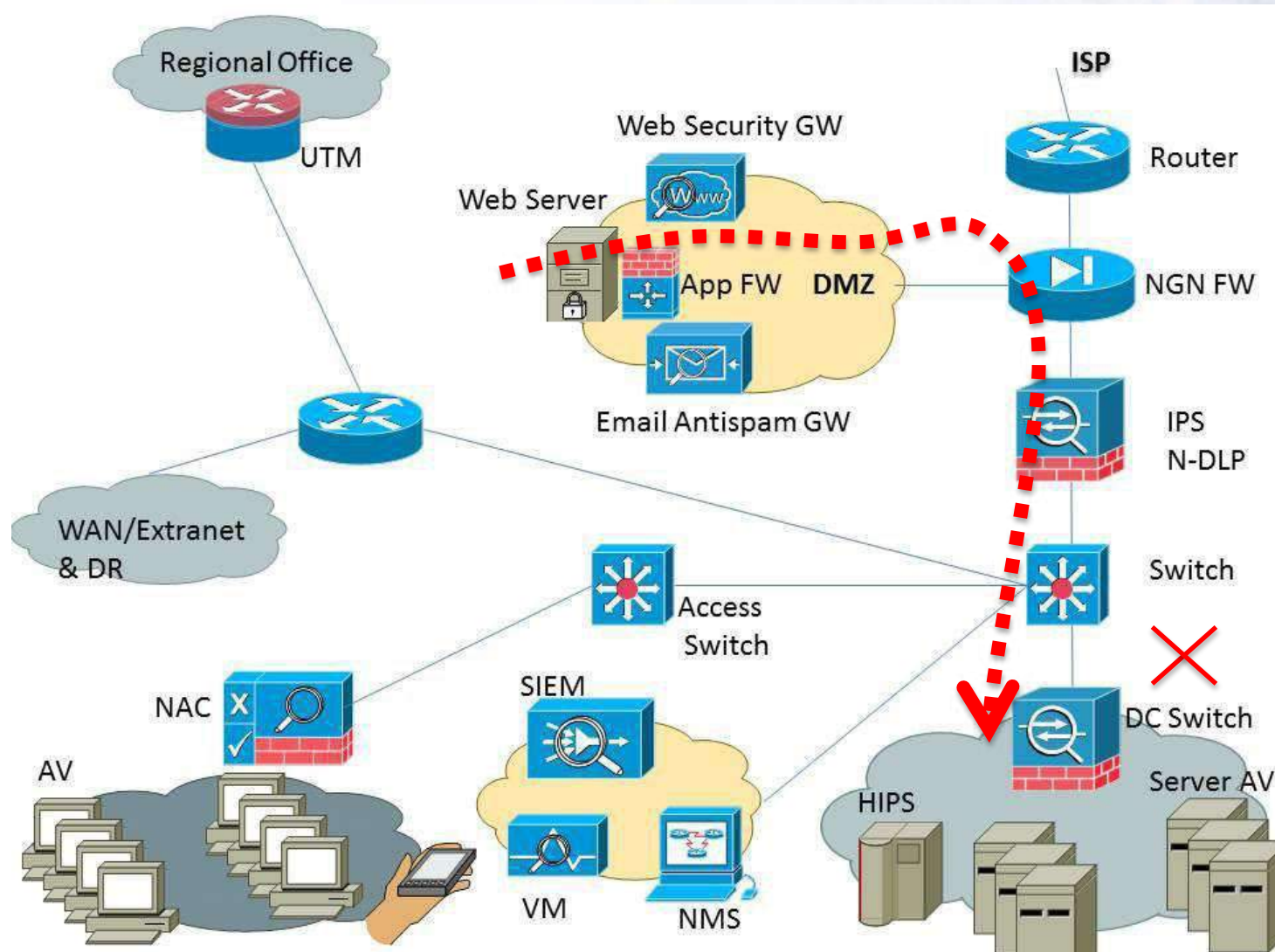
Security Overlay Of Enterprise (Part 2)



Security Overlay Of Enterprise (Part 2)



Security Overlay Of Enterprise (Part 2)



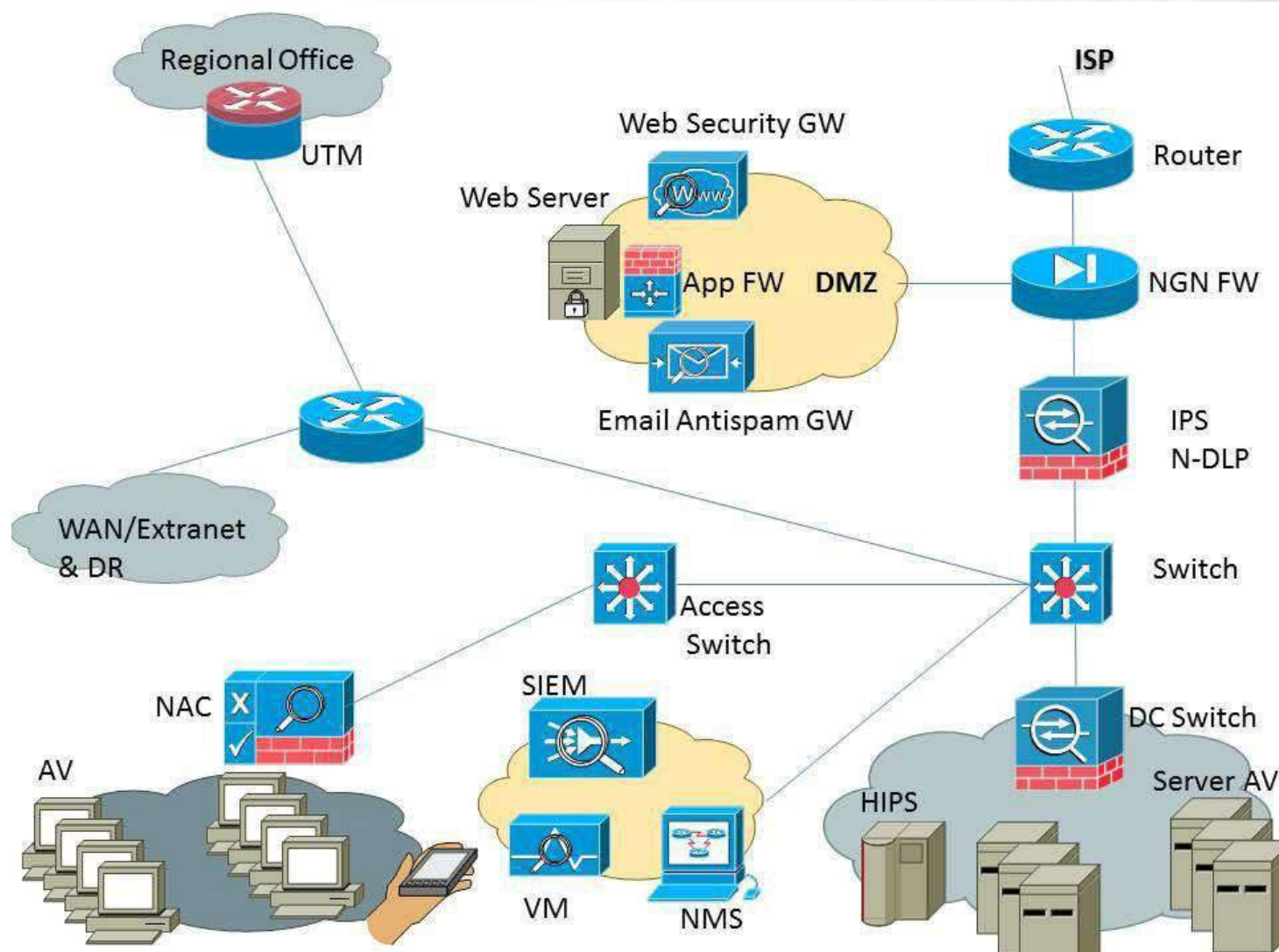
Security Overlay Of Enterprise (Part 2)

- Granular access list filtering and a well planned and tested security design are keys to success

Security Overlay Of Enterprise (Part 3)

- General security design principles

Security Overlay Of Enterprise (Part 3)



Security Overlay Of Enterprise (Part 3)

1. Block unauthorized traffic at edge (direct public www traffic to DMZ web server)
2. Edge malware protection & DMZ
3. Web & email are important vectors to secure against malware and attacks
4. NGN-FW (may be found in a UTM as well)

Security Overlay Of Enterprise (Part 3)

5. Web security GW and email anti-spam GW solutions
6. Granular access list filtering in edge and data center FWs (source, destination, and traffic type/port)
7. A good AV solution, and keep virus definitions updated
8. Monthly VM scans

Security Overlay Of Enterprise (Part 3)

More Advanced Security:

- APT & zero-day attack prevention
- SIEM solution
- Network DLP and system DLP
- Network admission control (NAC)
- Server HIPS
- Web application FW (WAF)

Security Overlay Of Enterprise (Part 3)

Even More Advanced Security:

- Network forensics
- Host-based APT / IoC solution
- Identity & access management (IAM)
- Privileged identity management (PIM)
- Database security solution

Security Overlay Of Enterprise (Part 3)

- Further guidelines for strong security controls:
 - CIS 20 critical security controls

Security Overlay Of Enterprise (Part 3)

First 5 CIS Controls

Eliminate the vast majority of your organisation's vulnerabilities

- 1: Inventory of Authorized and Unauthorized Devices →
- 2: Inventory of Authorized and Unauthorized Software →
- 3: Secure Configurations for Hardware and Software →
- 4: Continuous Vulnerability Assessment and Remediation →
- 5: Controlled Use of Administrative Privileges →

All 20 CIS Controls

Secure your entire organization against today's most pervasive threats

- 6: Maintenance, Monitoring, and Analysis of Audit Logs →
- 7: Email and Web Browser Protections →
- 8: Malware Defenses →
- 9: Limitation and Control of Network Ports →
- 10: Data Recovery Capability →
- 11: Secure Configurations for Network Devices →
- 12: Boundary Defense →
- 13: Data Protection →
- 14: Controlled Access Based on the Need to Know →
- 15: Wireless Access Control →
- 16: Account Monitoring and Control →
- 17: Security Skills Assessment and Appropriate Training to Fill Gaps →
- 18: Application Software Security →
- 19: Incident Response and Management →
- 20: Penetration Tests and Red Team Exercises →



CIS Controls

Security Overlay Of Enterprise (Part 3)

- Further guidelines for strong security controls:
 - CIS 20 critical security controls

High Availability (HA)

- What is high availability (HA)?
 - High availability of a system or component assures a high level of operational performance (uptime) for a given period of time

<https://www.digitalocean.com/community/tutorials/what-is-high-availability>

High Availability (HA)

- High availability is a strategy
- Fault tolerance refers to a system designed in such a way that when one component fails, a backup component takes over operations immediately to avoid loss of service

High Availability (HA)

Availability %	Downtime per year	Downtime per month	Downtime per week
90% aka "one nine"	36.5 days	72 hours	16.8 hours
95%	18.25 days	36 hours	8.4 hours
97%	10.96 days	21.6 hours	5.04 hours
98%	7.30 days	14.4 hours	3.36 hours
99% aka "two nines"	3.65 days	7.20 hours	1.68 hours
99.5%	1.83 days	3.60 hours	50.4 minutes
99.8%	17.52 hours	86.23 minutes	20.16 minutes
99.9% aka "three nines"	8.76 hours	43.8 minutes	10.1 minutes
99.95%	4.38 hours	21.56 minutes	5.04 minutes
99.99% aka "four nines"	52.56 minutes	4.32 minutes	1.01 minutes
99.999% aka "five nines"	5.26 minutes	25.9 seconds	6.05 seconds
99.9999% aka "six nines"	31.5 seconds	2.59 seconds	0.605 seconds
99.99999% aka "seven nines"	3.15 seconds	0.259 seconds	0.0605 seconds

<https://jazz.net/wiki/bin/view/Deployment/HighAvailability>

High Availability (HA)

- High availability is designed in the following manner:
 - System level (data center or service)
 - Device level (within single device)
 - Device level (combination of multiple redundant devices)
 - Alternate site level

High Availability (HA)

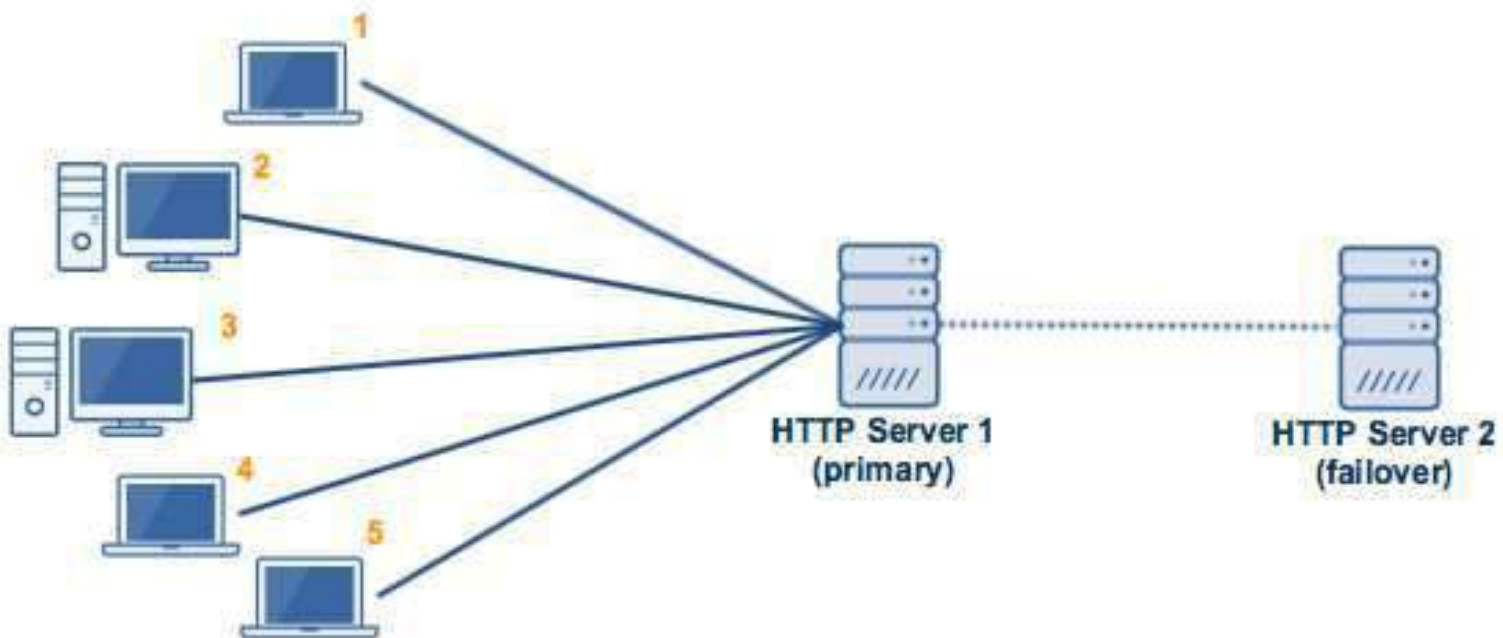
- High availability and fault tolerance:
 - Designed to minimize downtime with the help of redundant components
- Disaster Recovery:
 - A pre-planned approach for re-establishing IT functions at an alternate site

High Availability Design

- Lets look at various HA designs

High Availability Design

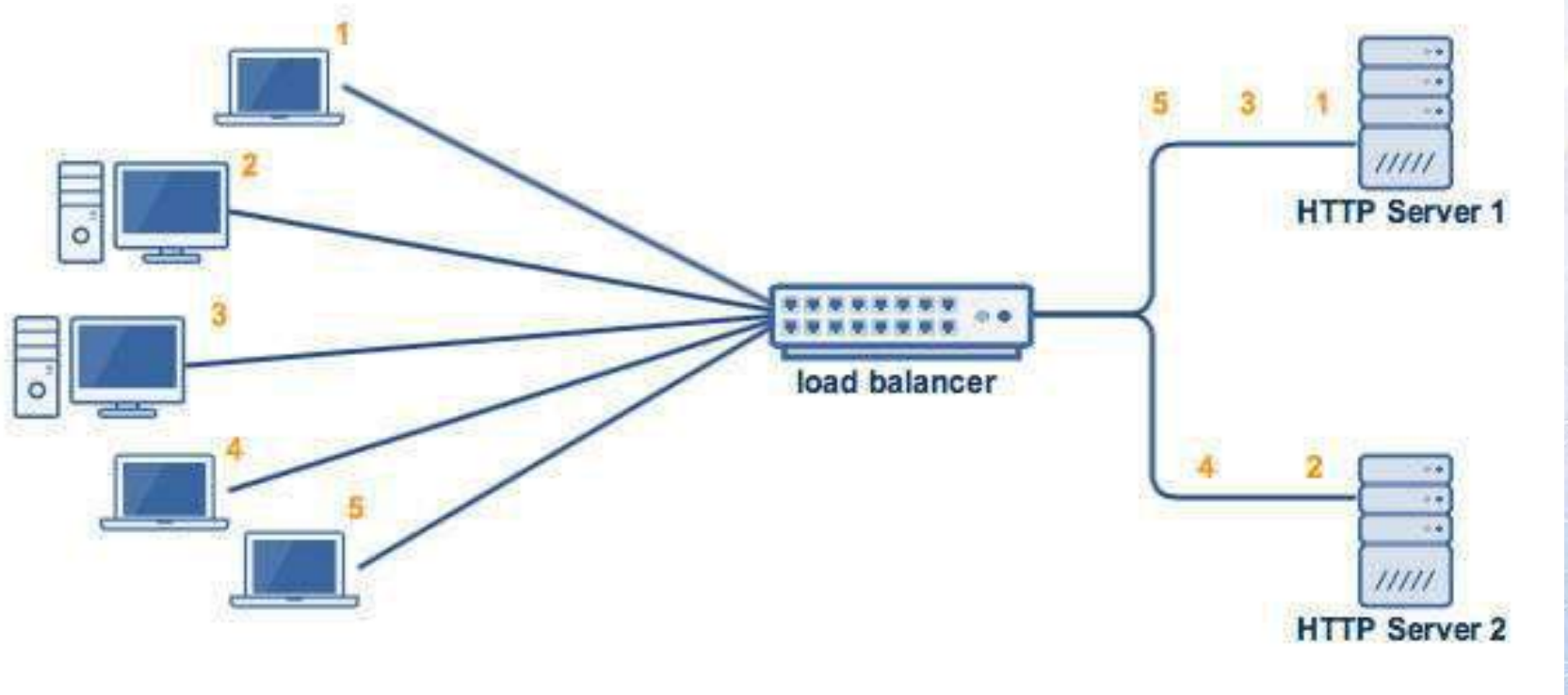
ACTIVE-STANDBY SERVER CONFIGURATION



<https://www.getfilecloud.com/blog/2015/12/architectural-patterns-for-high-availability/#.WVeex4SGPIU>

High Availability Design

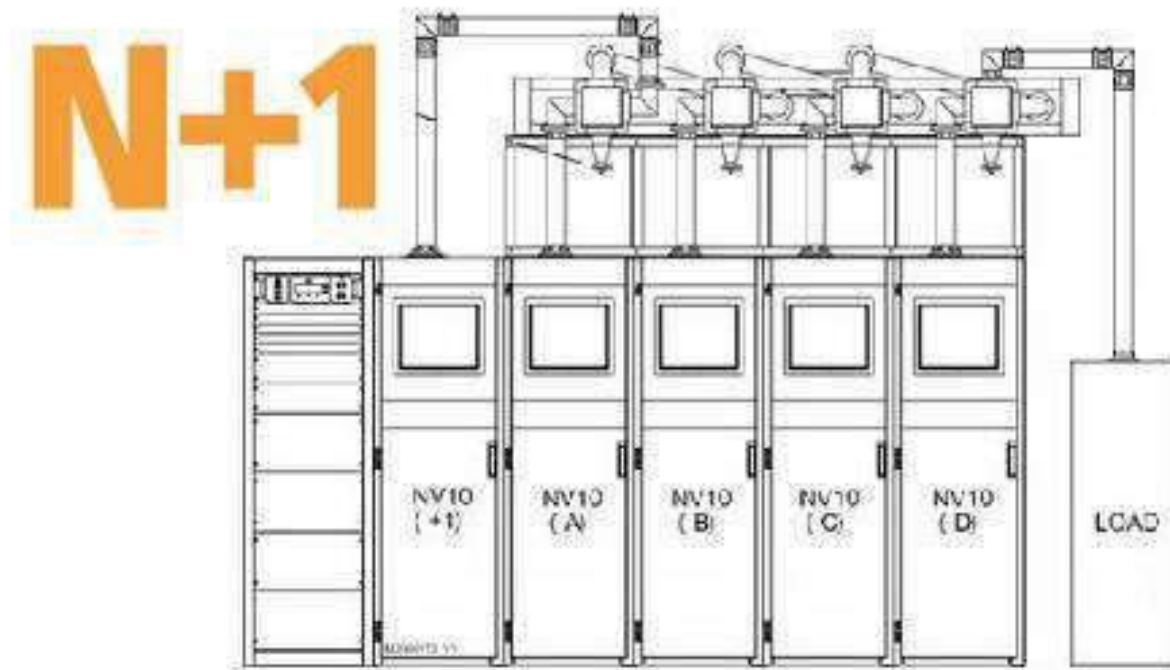
ACTIVE-ACTIVE SERVER CONFIGURATION



<https://www.getfilecloud.com/blog/2015/12/architectural-patterns-for-high-availability/#.WVeex4SGPIU>

High Availability Design

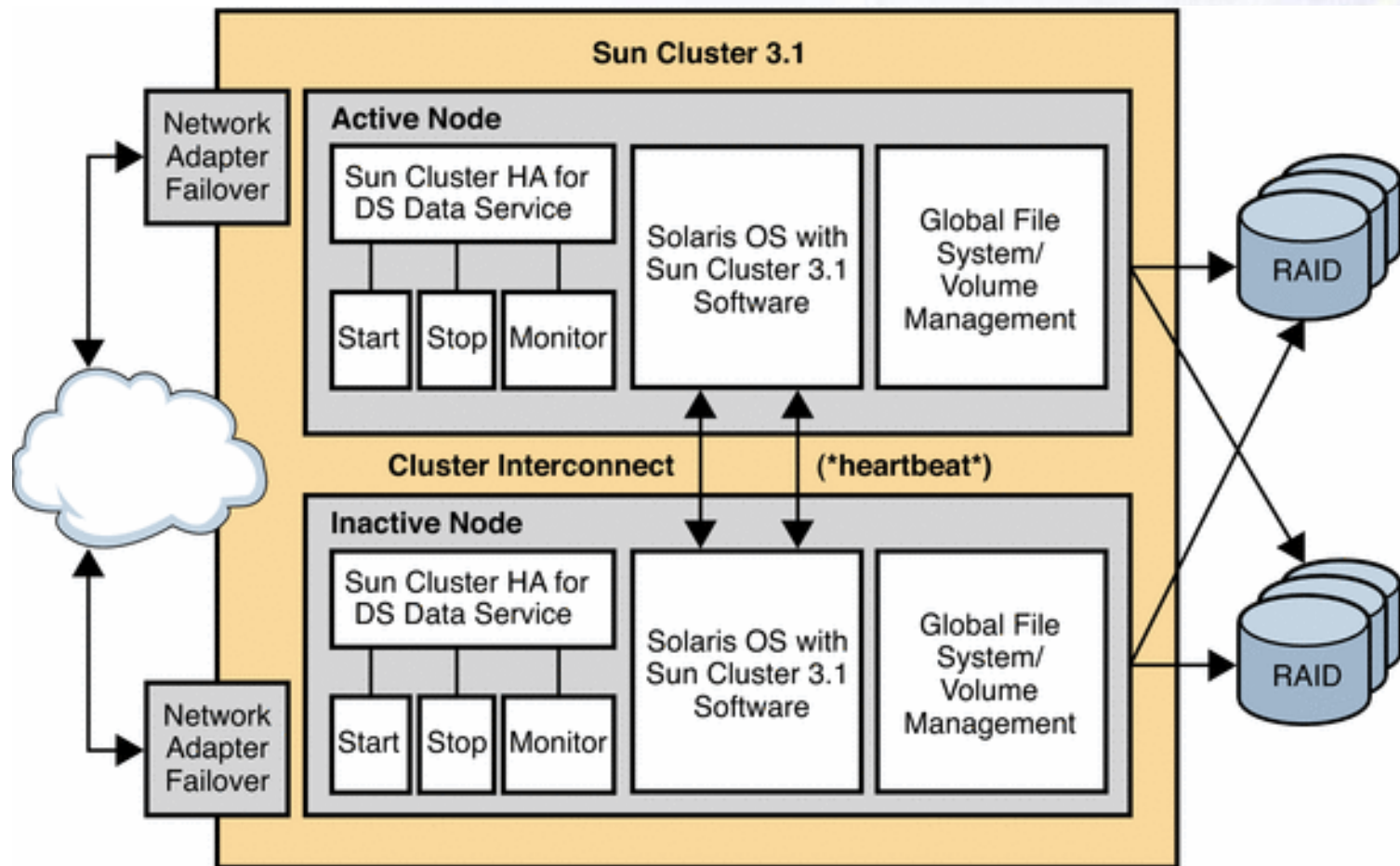
N+1 UPS REDUNDANT CONFIGURATION



<https://www.getfilecloud.com/blog/2015/12/architectural-patterns-for-high-availability/#.WVeex4SGPIU>

High Availability Design

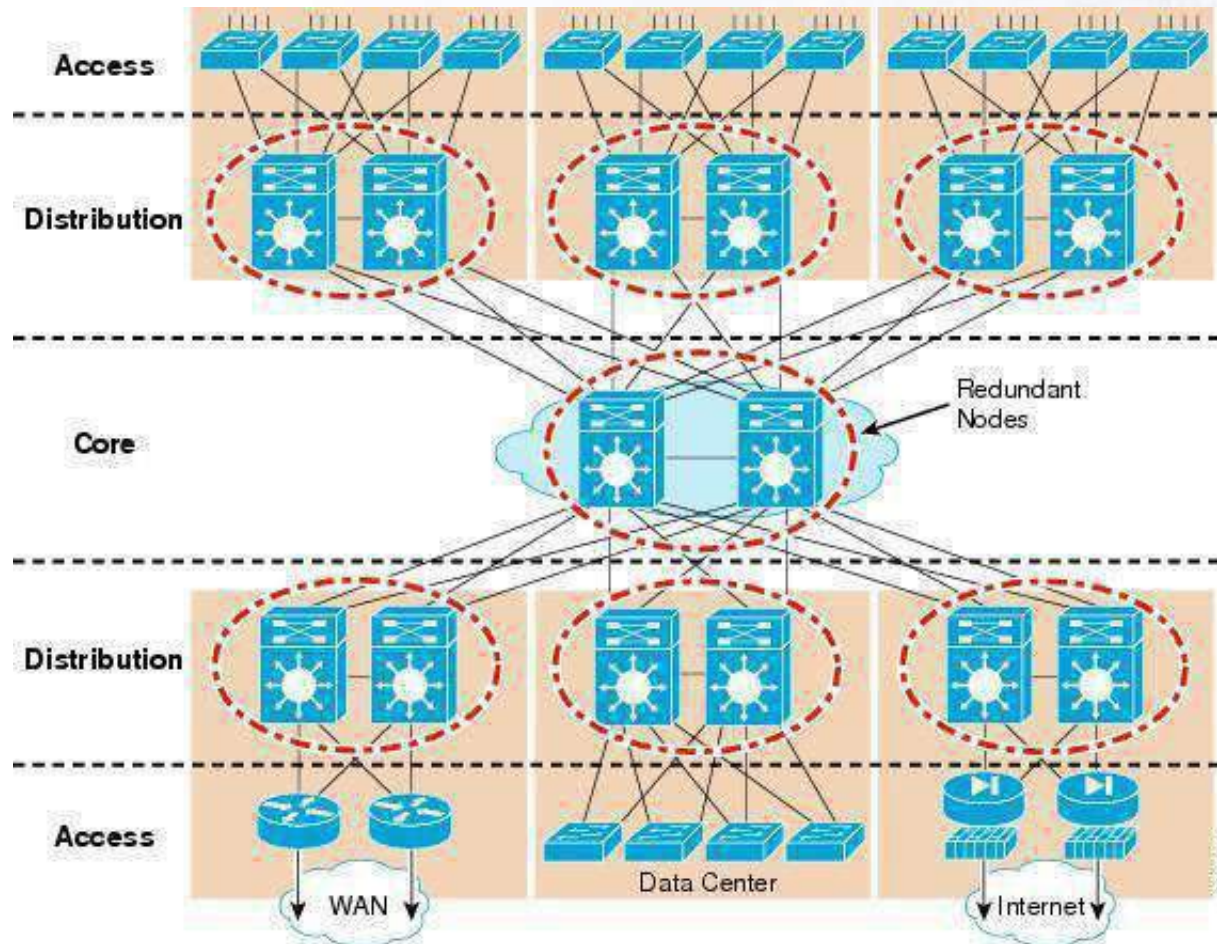
ACTIVE-STANDBY SUN SERVER CLUSTER



<https://docs.oracle.com/cd/E19693-01/819-0992/6n3cn7p3n/index.html>

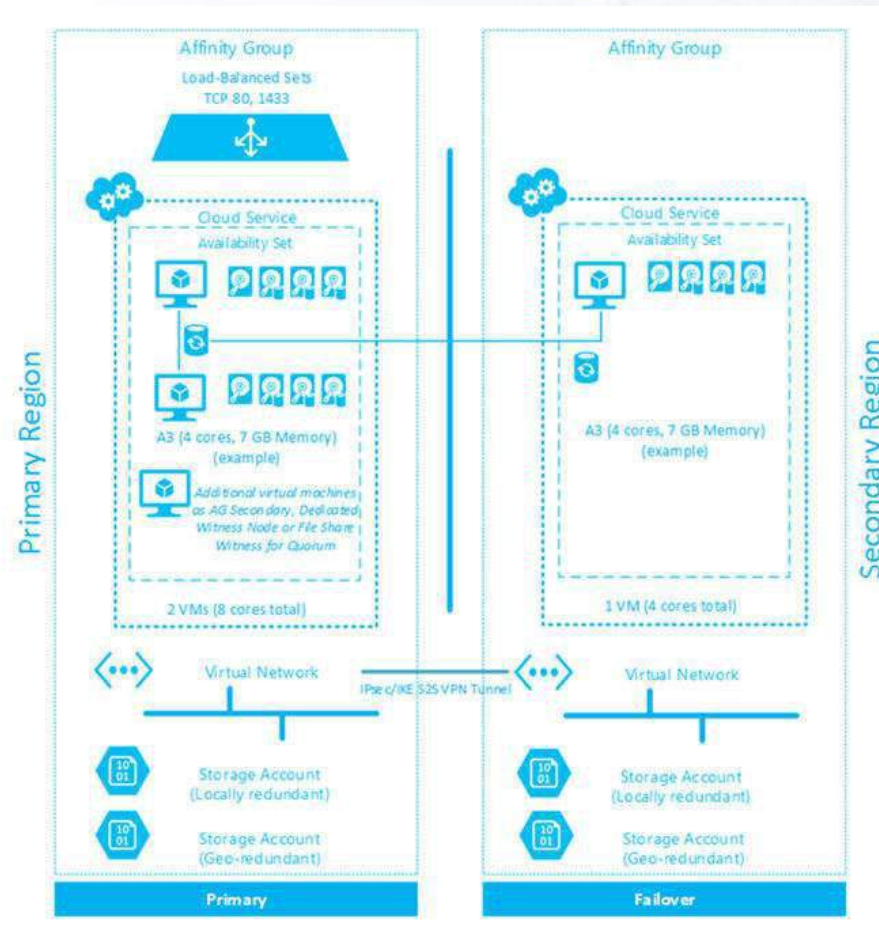
High Availability Design

NETWORK REDUNDANT CONFIGURATION



High Availability Design

DATA CENTER REDUNDANT CONFIGURATION



High Availability Design

- Don't forget to test the failover and fault tolerant capabilities of our network

Site Redundancy

- Three types of redundant site models:
- Hot site
- Cold site
- Warm site

Site Redundancy

- Hot site (expensive):
 - Mirror of primary data center
 - Populated with servers, cooling, power, and office space
 - Running concurrently with main/primary data center (synching)
 - Minimal impact

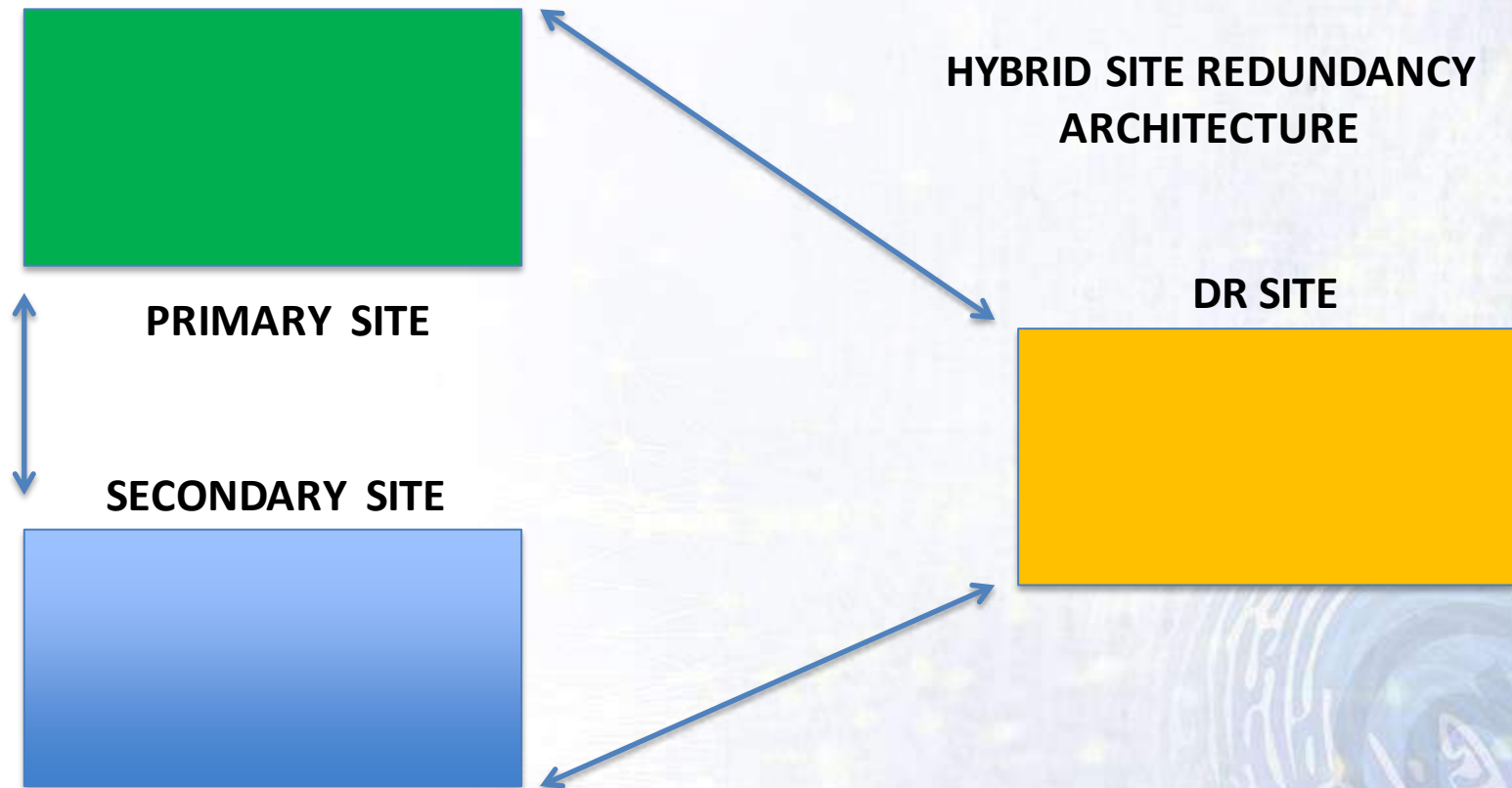
Site Redundancy

- Cold site (cheapest):
 - Office or data center space without any server related equipment installed
 - Power, cooling and office space
 - Servers/equipment migrated in event of primary site failure

Site Redundancy

- Warm site (middle ground):
 - Middle ground between hot site and cold site
 - Some pre-installed server hardware (ready for installation of production environments)
 - Requires engineering support to activate

Site Redundancy



Site Redundancy

- RTO:
 - Max amount of time, following a disaster, for an organization to recover files from backup storage and resume normal operations (max amount of downtime an organization can handle)

<http://searchdisasterrecovery.techtarget.com/definition/disaster-recovery>

Site Redundancy

- RPO:
 - Max age of files that an organization must recover from backup storage for normal operations to resume after a disaster (minimum frequency of backups)

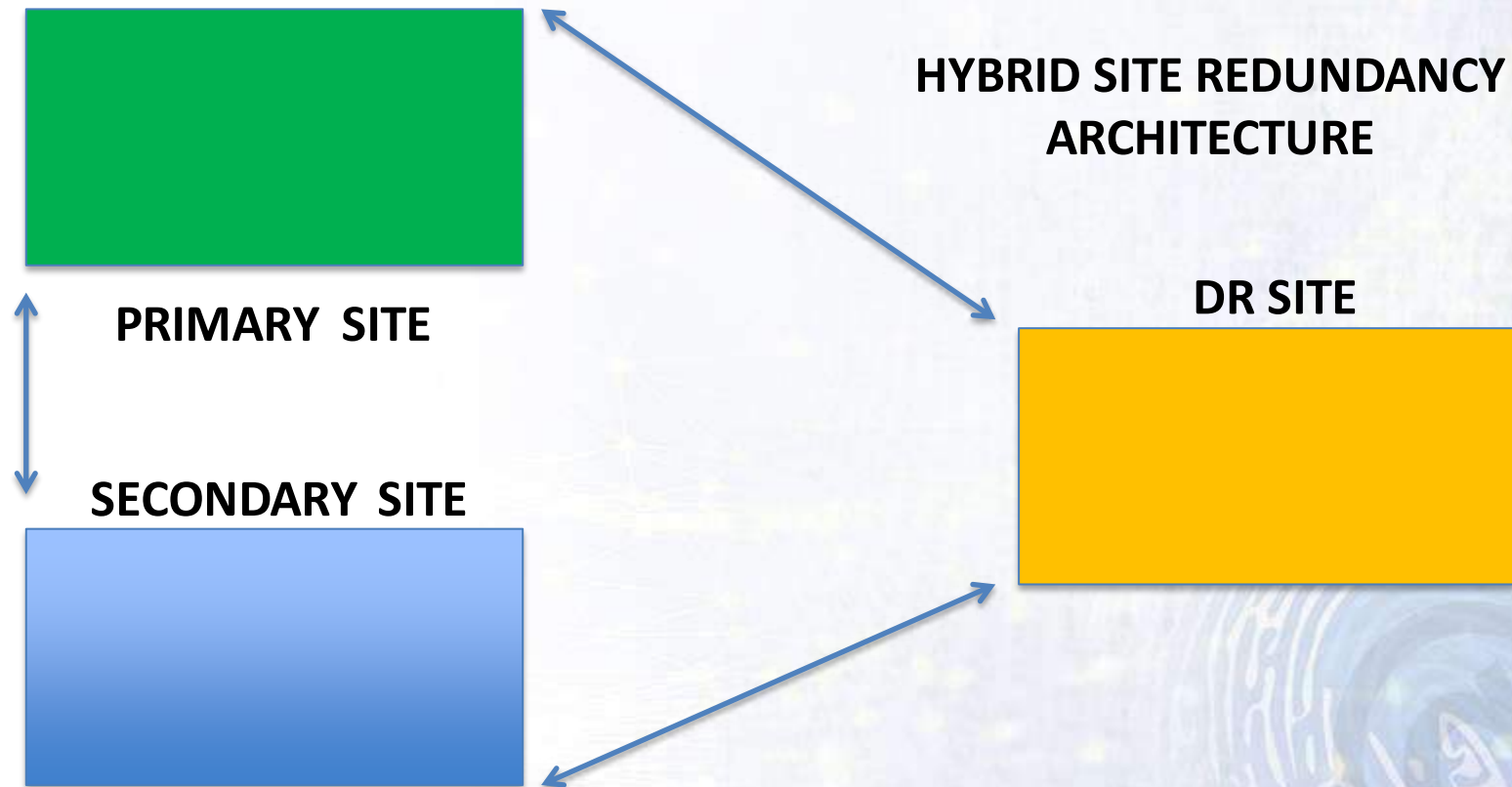
Site Redundancy

- Example:
 - If an organization has an RTO of two hours, it cannot be down for longer than that.
 - if an organization has an RPO of four hours, the system must back up at least every four hours.

High Availability & Redundancy Case Study

- Mid-sized enterprise
- 3000 total staff
- 2000 IT users
- 30 IT team
- One DC, one secondary (regional) data center (warm site & backup site), and one DR site
- 99.9 % uptime designed

High Availability & Redundancy Case Study



High Availability & Redundancy Case Study

- IT setup:
 - Oracle ERP system
 - Sharepoint portal for workflow automation
 - Head office in Karachi
 - Primary DC in Karachi (hosted with 3rd party)
 - DR site in Lahore (hosted with 3rd party)
 - Secondary DC in ISB

High Availability & Redundancy Case Study

- Primary DC:
 - Fully redundant (HA) design for network, systems, and storage
 - Cisco HA (active-standby)
 - Oracle cluster technology for servers and DBs (active-active)

High Availability & Redundancy Case Study

- Secondary DC (ISB):
 - All network, systems, and storage backups maintained here (also mirrored in DR)
 - Regional servers (AD, file servers, etc)
 - Test & staging environment here (segregated from main DC)
 - Office working space

High Availability & Redundancy Case Study

- DR site
 - Bare minimum HA (as DR site) for network, systems, and storage
 - Mirror of all backups from secondary site maintained here
 - Office working space
 - Some additional computing capacity (minimum for unforeseen events)

High Availability & Redundancy Case Study

- DR site
 - All critical systems and devices maintained in active mode (hot) for immediate DR failover
 - Data maintained as per org RTO/RPO for immediate utility
 - Monthly DR testing/drill

High Availability & Redundancy Case Study

- Backup strategy:
 - Primary backup at secondary DR site
 - Mirror at DR site
 - For critical systems: monthly full backup, daily incremental backup
 - For critical network devices: weekly full backup; backups based on change

Backup Strategies

- Backup considerations:
 - What to backup ?
 - Backup location ?
 - Freq of backup ?
 - Backup operator ?
 - Backup checker (verification)?
 - Backup test & security methods ?
 - Technology & tools used for backup ?

<http://www.techsoup.org/support/articles-and-how-tos/your-organizations-backup-strategy>

Backup Strategies

- What to backup ?
 - Network configuration files
 - OS backups
 - Database & application data
 - Other critical data

Backup Strategies

- Backup location ?
 - Onsite for faster recovery
 - Offsite for DR purposes
 - Intermediate site (secondary site) as a middle-ground

Backup Strategies

- Backup frequency ?
 - Depends entirely on criticality of data, nature of the information being backed up (how frequently does info change?), storage space available, and overall backup plan

Backup Strategies

- Backup operator and checker?
 - Backups should ideally be automated
 - Operator should ensure that backups have taken place
 - Verifier should sign-off that check has been made

Backup Strategies

- Backup testing & security considerations:
 - Backup testing should be performed on a periodic basis and greater than the frequency of the DR drill (e.g. DR drill once a QTR, & testing once a month)
 - Encryption & compression

Backup Strategies

- Backup tools and technology:
 - Consider NAS, SAN, SCSI/IDE/SATA drives
 - Various tools and technology to perform full, differential, and incremental backups
 - Encryption
 - Access control
 - Alerts & reporting

Security Tools Used In An Enterprise

- Typical security tools used in an enterprise:
 - Enterprise antivirus
 - MS Active Directory (AD)
 - Vulnerability manager
 - Logs management
 - Network & performance monitoring
 - Automated backups

Security Tools Used In An Enterprise

- Typical security tools used in an enterprise:
 - Microsoft Windows Server Update (WSUS) & SCM/SCCM
 - Asset management software
 - Trouble-ticket system
 - SIEM
 - DLP
 - Encryption software
 - 2FA

Security Tools Used In An Enterprise

Tool	Function	Complexity level	Examples
Enterprise Antivirus	System antivirus and malware protection	Low	Sophos, Avast, Kaspersky, Symantec, McAfee
MS AD (GP)	Pushing out security policies through AD GPO	Low	Pushing out windows password settings
VM	Vulnerability scanning	Medium	OpenVAS, Nessus, Qualys

Security Tools Used In An Enterprise

Tool	Function	Complexity level	Examples
Log Management	Logs collection & analysis	Medium	OSSEC
Network & Performance Management	NOC	Low	CACTI, ORION
Automated Backups	Backups	Medium	Veritas
Windows Updates	Windows Updates & Configs	Low	WSUS, SCCM, SCM

Security Tools Used In An Enterprise

Tool	Function	Complexity level	Examples
Asset Management	Detect, Track, Manage Assets	Medium	Asset Explorer, PulseWay
Trouble Ticket System	TT Workflow	Medium	BMC Track-IT, SysAid
SIEM	Event Management	High	OSSEC, Splunk, Q-Radar
DLP	Data Loss Prevention	High	Symantec,
Encryption Software	Encryption	High	TrueCrypt

Security Tools Used In An Enterprise

- Lots of tools available
- People, process, technology

Security Tools – Typical Enterprise (Part 1)

industry leader issue in the industry report

- Gartner Magic Quadrant reports
- List of some other industry reports

Security Tools – Typical Enterprise (Part 1)

Endpoint
Protection
Jan, 2017
Gartner

Trend Micro
Sophos
Kaspersky
Symantec



<https://www.gartner.com/doc/reprints?id=1-3SCOKCW&ct=170131&st=sb>

Security Tools – Typical Enterprise (Part 1)

Secure Web
GW

June, 2017

Gartner

Symantec

Zscaler



<https://www.gartner.com/doc/reprints?id=1-3SCOKCW&ct=170131&st=sb>

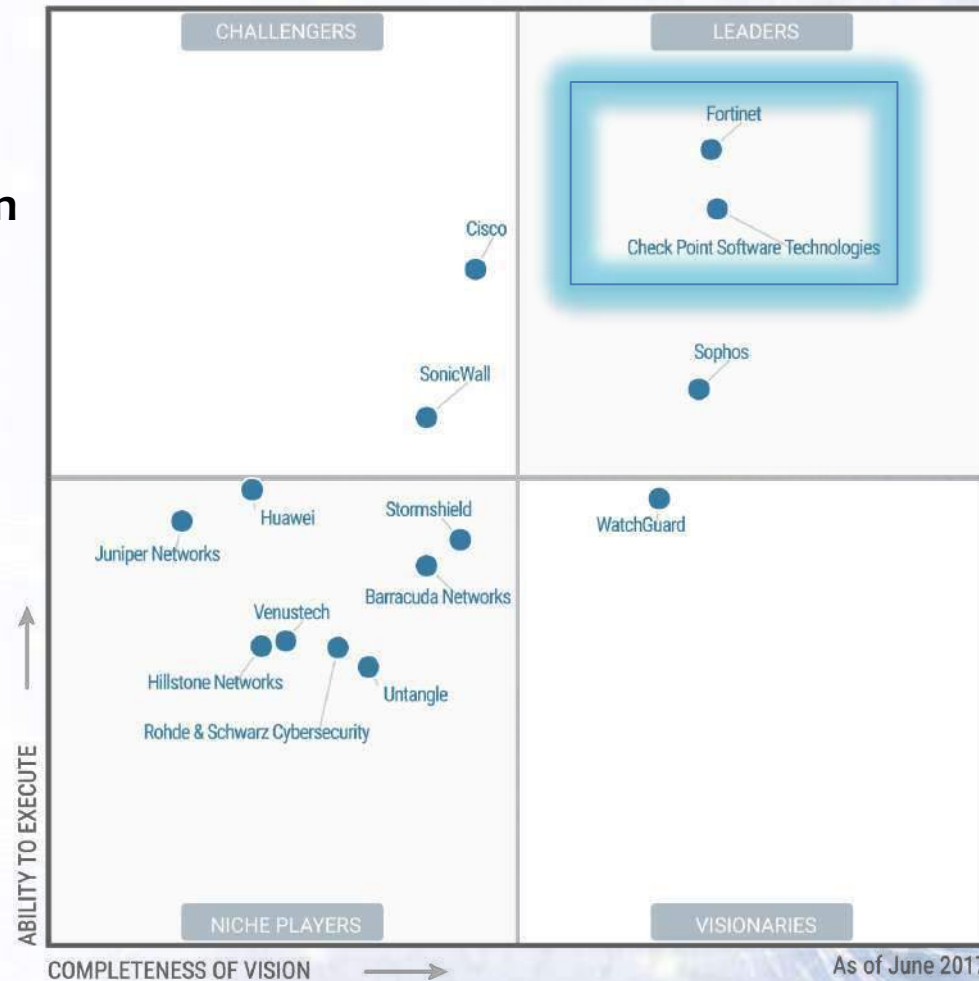
Security Tools – Typical Enterprise (Part 1)

UTM
(SMB Multi-function
FW)

June, 2017

Gartner

Fortinet
Checkpoint



<https://www.gartner.com/doc/reprints?id=1-3SCOKCW&ct=170131&st=sb>

Security Tools – Typical Enterprise (Part 1)

**Enterprise
Network FWs
May 2016
Gartner**

**Palo Alto
Networks**



<https://www.gartner.com/doc/reprints?id=1-3805JH8&ct=160525&st=sb>

Security Tools – Typical Enterprise (Part 1)

SIEM
AUGUST 2016
GARTNER

IBM
Splunk
LogRhythm



<https://www.gartner.com/doc/reprints?id=1-2JNR3RU&ct=150720&st=sb>

Security Tools – Typical Enterprise (Part 1)

DLP
FEB 2017
GARTNER

-Symantec
-Digital
Guardian
-Forcepoint



<https://www.gartner.com/doc/reprints?id=1-3UKD88K&ct=170301&st=sb>

Security Tools – Typical Enterprise (Part 1)

APPLICATION
SECURITY
TESTING
FEB 2017
GARTNER

HPE
Veracode
IBM



<https://www.gartner.com/doc/reprints?id=1-3UKD88K&ct=170301&st=sb>

Security Tools – Typical Enterprise (Part 1)

- View and read various industry reports for security tools comparisons:
 - Gartner
 - Forrester
 - Security Awards
 - Lab reports: ICSSA, NSS

END

Security Tools – Typical Enterprise (Part 2)

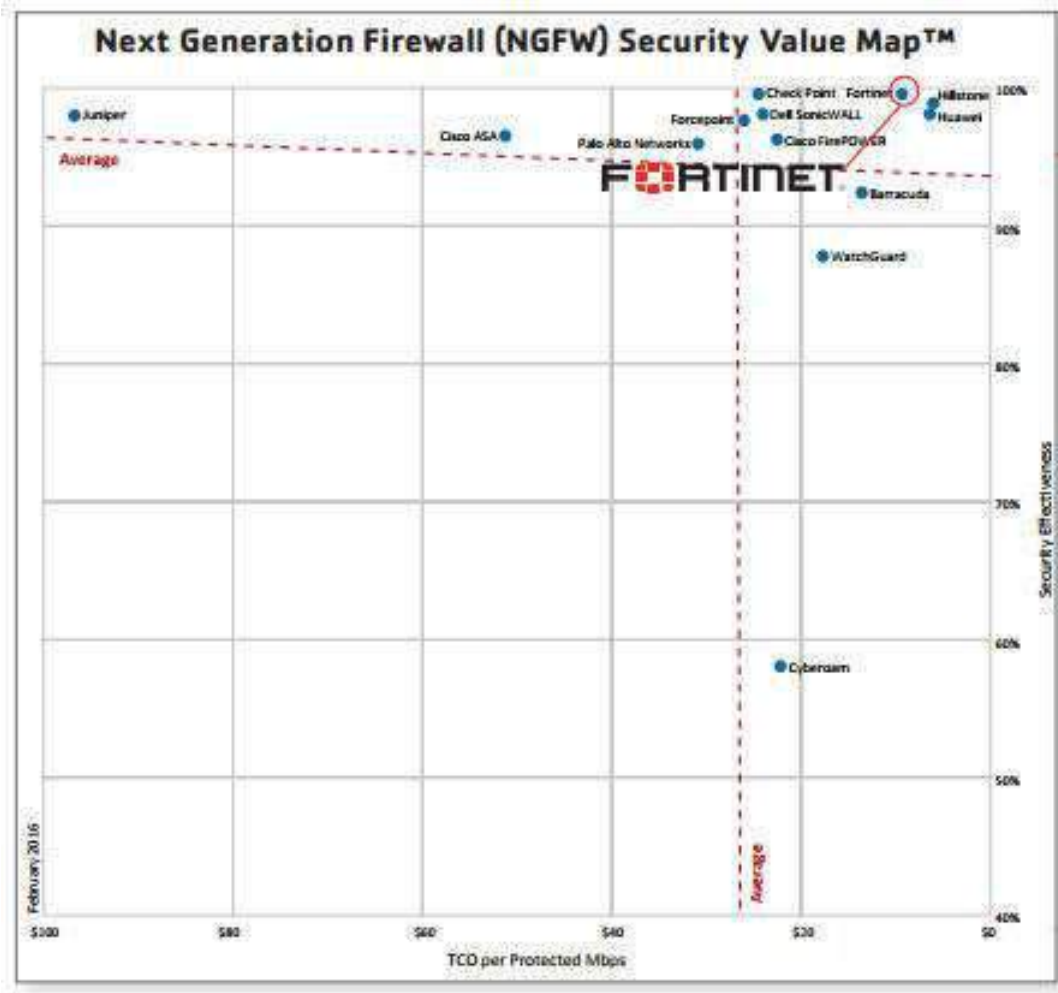
- NSS Labs Security Value Map (SVM)
- Some additional Gartner Magic Quadrant reports

Security Tools – Typical Enterprise (Part 2)

next generation firewall web

NGFW
NSS Labs
2016

Hillstone
Huawei
Fortinet



<https://www.fortinet.com/content/dam/fortinet/assets/analyst-reports/Brochure-NSS-Lab-Independent-Validation.pdf>

Security Tools – Typical Enterprise (Part 1)

**Enterprise
Mobility
Management
(EMM)
June 2017**

**VMWARE
MobileIron
IBM
Blackberry**



As of June 2017

<https://www.gartner.com/doc/reprints?id=1-42A6Q84&ct=170607&st=sb>

Security Tools – Typical Enterprise (Part 1)

**DC Backup
& Recovery
June 2016**

**Commvault
IBM
EMC
Veritas**



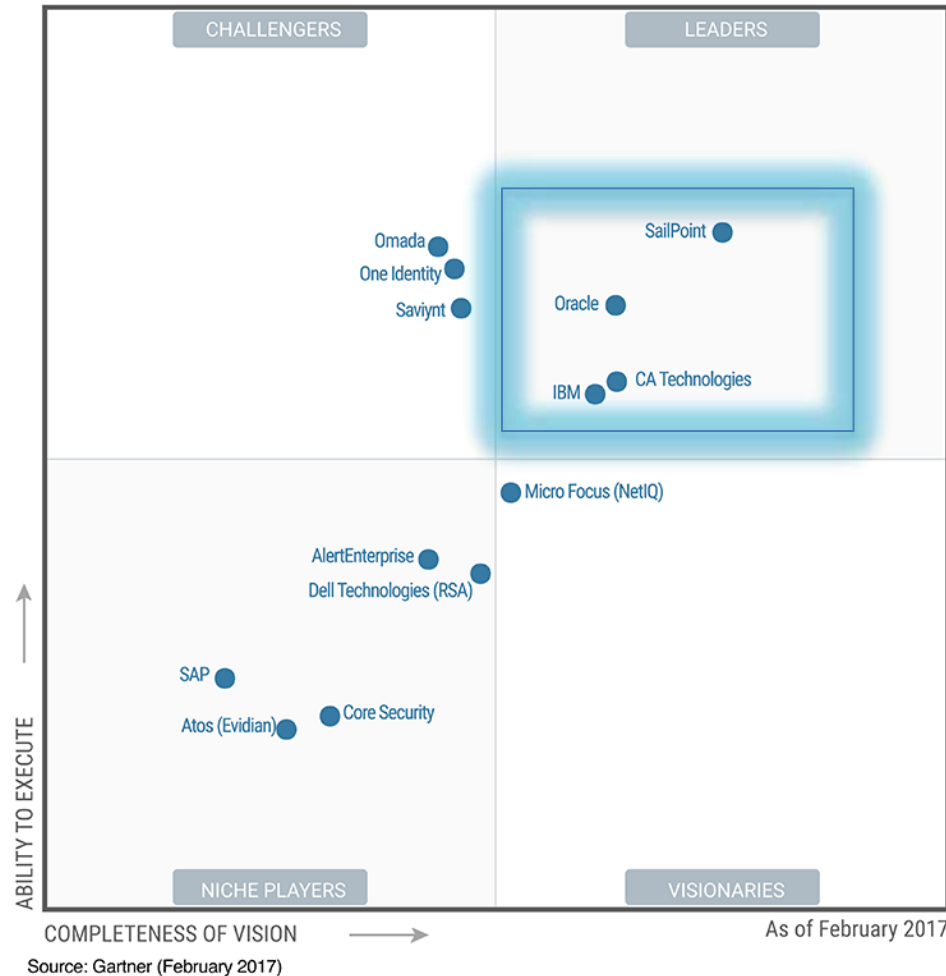
<https://www.gartner.com/doc/reprints?id=1-38JSYOW&ct=160602&st=sb>

Security Tools – Typical Enterprise (Part 1)

Identity,
Governance
Feb 2017

Sailpoint
Oracle
CA
IBM

Figure 1. Magic Quadrant for Identity Governance and Administration



<https://www.sailpoint.com/identity-governance-leader-gartner-magic-quadrant/>

Security Tools – Typical Enterprise (Part 1)

Network Perf
Monitoring
& Diagnostics
Feb 2017

NetScout
Viavi
Riverbed



As of February 2017

<https://www.gartner.com/doc/reprints?id=1-3TYUQFH&ct=170221&st=sb>

Security Tools – Typical Enterprise (Part 1)

Web App FW
July 2016

Imperva



<https://www.gartner.com/doc/reprints?id=1-3TYUQFH&ct=170221&st=sb>

Security Tools – Typical Enterprise (Part 2)

- Gartner
- Forrester
- NSS labs
- ICISA Labs

END

What Does “Box Security” Mean ?

- “Box Security” refers to a prevalent approach in the industry, especially in larger organizations in which the solution for every security challenge is in the form of a “box” or device

What Does “Box Security” Mean ?

- Box for:
 - Email security
 - Web security
 - FW
 - IPS
 - APT attack prevention
 - DDOS prevention
 - Network DLP
 - Network Forensics
 - Others

What Does “Box Security” Mean ?

- Security is a combination of people, process, and technology
- Industry observation: most of the devices are not used to full capability or capacity after purchase
- Case in point: SIEM solution or DB security solution

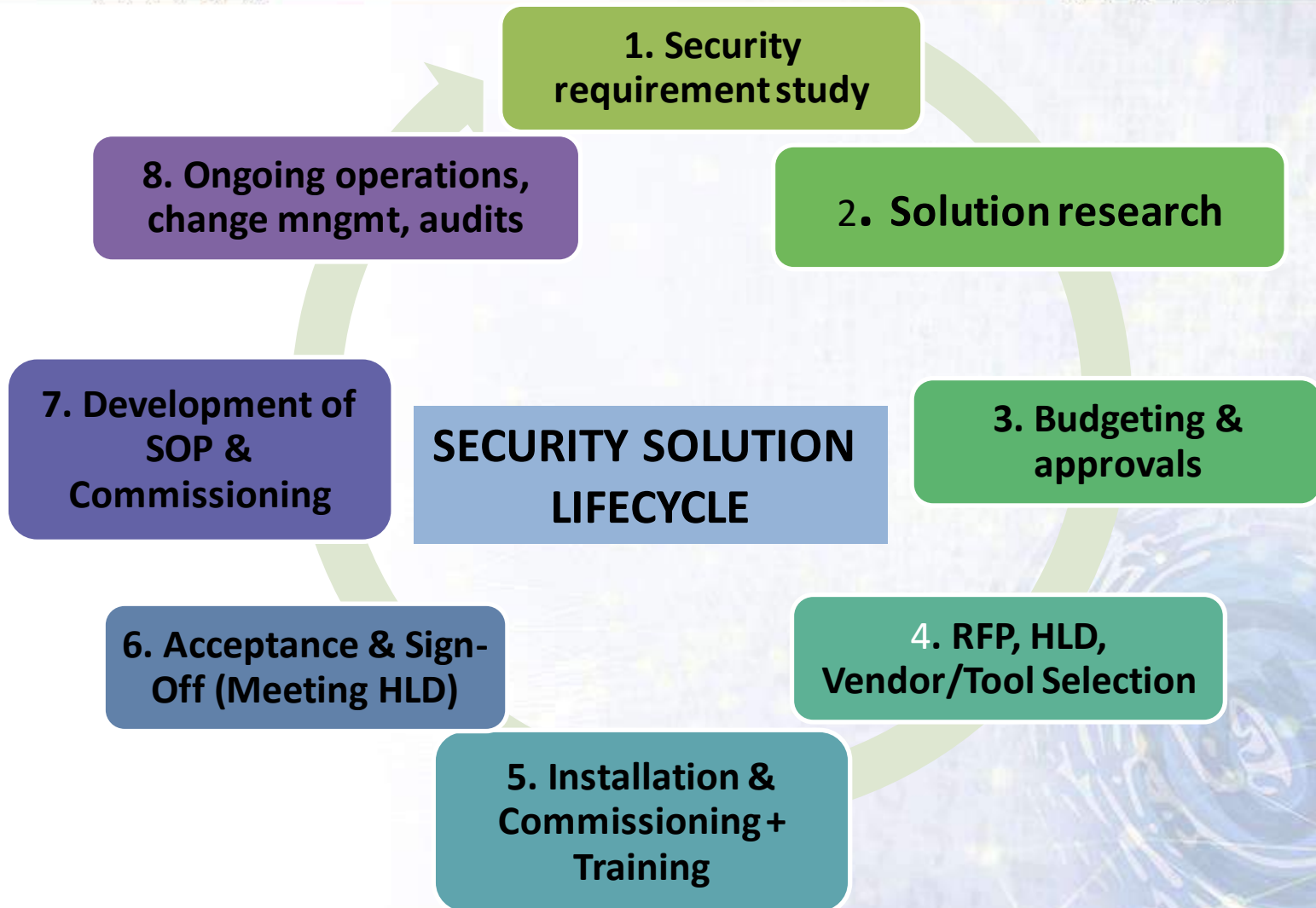
What Does “Box Security” Mean ?

- “Box security” is not the silver bullet
- Although many devices and boxes are required, they do not ensure a good security posture
- This approach is unfortunately promoted by many vendors who have equipment to sell
- Consider organizational maturity & readiness

What Does “Box Security” Mean ?

- Other challenges with “box security” approach:
 - Shortage of staff (IT & security)
 - Training and skill required to operate the sophisticated devices and features

What Does “Box Security” Mean ?



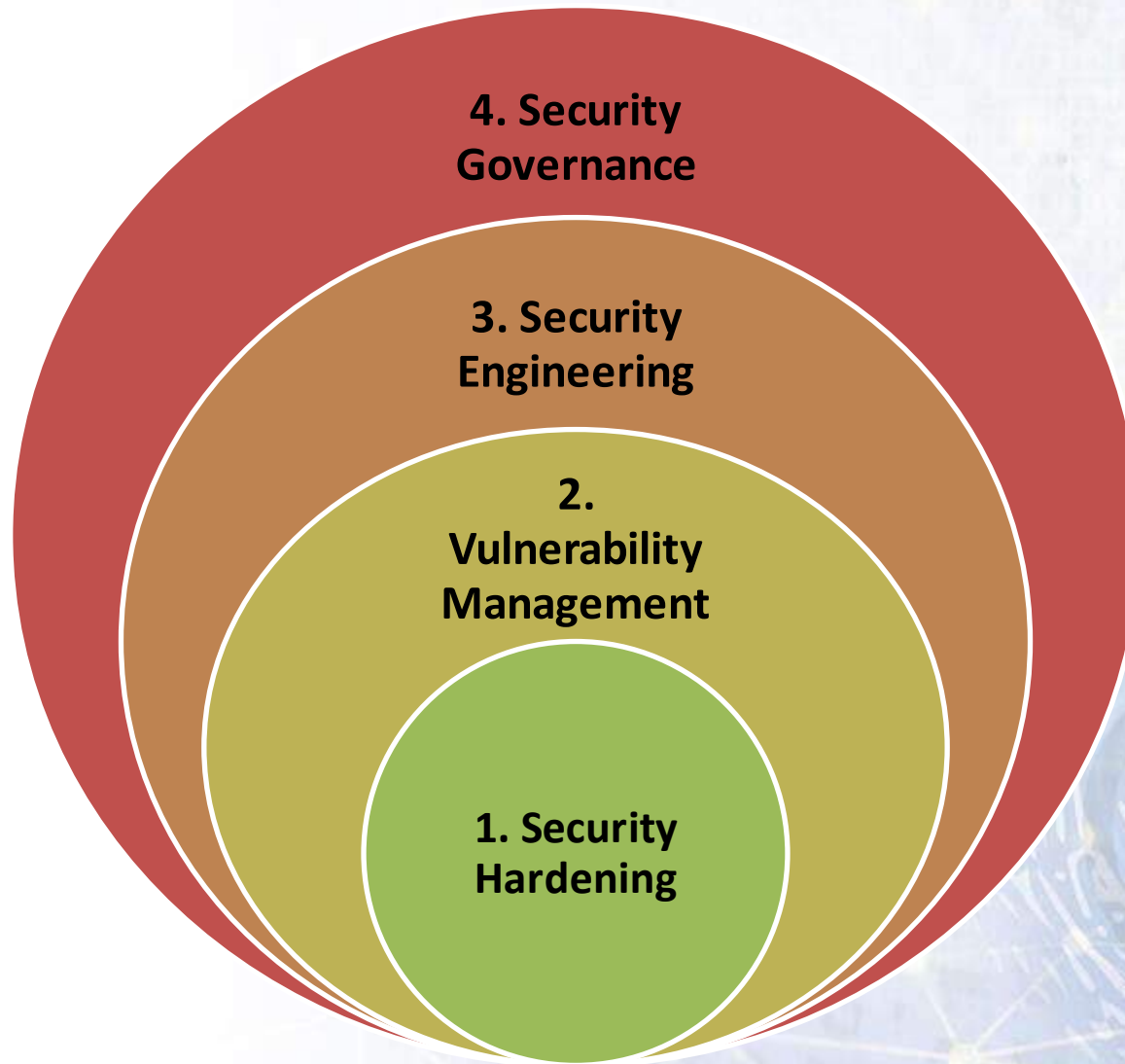
What Does “Box Security” Mean ?

- Device objectives, and high-level-design (HLD) should be planned prior to commissioning
- Min operational baseline and configuration should be documented in SOP
- Device feature set and configuration audits should be conducted on a periodic basis (annual)

Best Approach: IT Enterprise Security ?

- The 4-layer security transformation model is the only way to effectively and practically address security posture
- 4-layer security transformation model is tried & tested for geographies where the overall security awareness & posture is weak

Best Approach: IT Enterprise Security ?



Best Approach: IT Enterprise Security ?

1. Security hardening:
address security
configuration of all IT
assets which security
“boxes” won’t do for
you
2. Vulnerability
management: scanning
to inspect patching of
IT assets (essential)
3. Security engineering
4. Security governance

Best Approach: IT Enterprise Security ?

3. Security engineering:
this is where more
serious investments
may be made once
layers 1 & 2 have been
completed
satisfactorily (or are
being addressed)

Best Approach: IT Enterprise Security ?

4. Security governance: ensure the proper utilization (as intended), ROI, and audits of purchased devices & solutions

Also ensure configs are as per design, and SOPs.

What Is Disaster Recovery (DR)?

- What is a disaster ?
 - Any significant event that causes disruption of information technology processing facilities, thus affecting the operations of the business

<https://www.sans.org/reading-room/whitepapers/recovery/disaster-recovery-plan-strategies-processes-564>

What Is Disaster Recovery (DR)?

- What is disaster recovery (DR)?
 - DR is an area of security that allows an organization to maintain or quickly resume mission-critical (IT) functions following a disaster

<http://searchdisasterrecovery.techtarget.com/definition/disaster-recovery>

What Is Disaster Recovery (DR)?

- What could cause the invocation of a DR failover to DR site?
 - Natural disasters such as flood, earthquake, lightning, storm
 - Disaster caused by human actions such as riot, fire, terrorist act, etc

What Is Disaster Recovery (DR)?

- What is the difference between DR and business continuity (BC)?
 - DR is an IT function, whereas business continuity addresses keeping all essential aspects of a business functioning despite disruptive events (DR is a part of BC)

https://en.wikipedia.org/wiki/Disaster_recovery

What Is Disaster Recovery (DR)?



<http://grcbizassurance.com/services/disaster-recovery/>

What Is Disaster Recovery (DR)?

- Three step process:
 - Failover to the DR site (DR invocation)
 - Restoration of the services/facilities on primary site
 - Recovery (switchover back to primary site)

<https://www.sans.org/reading-room/whitepapers/recovery/disaster-recovery-plan-strategies-processes-564>

What Is Disaster Recovery (DR)?

- What is a DR plan ?
 - A documented, structured approach to dealing with unplanned incidents

<http://searchdisasterrecovery.techtarget.com/definition/disaster-recovery-plan>

What Is Disaster Recovery (DR)?

- DR plan checklist:
 - Scope of the activity
 - Gathering relevant network infrastructure documents
 - Identifying the most serious threats and vulnerabilities, and the most critical assets

<http://searchdisasterrecovery.techtarget.com/definition/disaster-recovery-plan>

What Is Disaster Recovery (DR)?

- Identifying current DR strategies
- Identifying emergency response team
- Management review & approval of DR plan
- Testing the plan (drill)
- Updating the plan
- Implementing a DR plan audit

<http://searchdisasterrecovery.techtarget.com/definition/disaster-recovery-plan>

What Is Disaster Recovery (DR)?

- Sample DR plan template:
 - http://www.it.miami.edu/_assets/pdf/security/ITPol_A135-Disaster%20Recovery%20Plan%20Example%202.pdf

What is Business Continuity (BC) ?

- What is business continuity ?
 - Business Continuity (BC) is the capability of the org to continue delivery of products or services at acceptable predefined levels following a disruptive incident (Source: ISO 22301:2012)

<http://www.thebci.org/index.php/resources/what-is-business-continuity>

What is Business Continuity (BC) ?

the advanced planning and preparation of an organization to maintaining business functions or quickly resuming after a disaster has occurred.

- What is business continuity management?
 - Holistic management process that identifies potential threats to an organization and the impacts to business operations those threats, if realized, might cause, and which provides a ...

<http://www.thebci.org/index.php/resources/what-is-business-continuity>

What is Business Continuity (BC) ?

- What is business continuity management?
 - ... framework for building org resilience with an effective response that safeguards interests of key stakeholders, reputation, brand and value-creating activities. (Source: ISO 22301:2012)

<http://www.thebci.org/index.php/resources/what-is-business-continuity>

What is Business Continuity (BC) ?



ANALYSIS

DESIGN
IMPELEMENTION
VALIDATION

<http://www.thebci.org/index.php/resources/what-is-business-continuity>

What is Business Continuity (BC) ?

- What is a BC plan ?
 - A document that consists of critical information an organization needs to continue operating during an unplanned event

<http://searchdisasterrecovery.techtarget.com/definition/business-continuity-action-plan>

What is Business Continuity (BC) ?

A business continuity plan (BCP) is a document that consists of the critical information an organization needs to continue operating during an unplanned event. The BCP states the essential functions of the business, identifies which systems and processes must be sustained, and details how to maintain them.

- What is a BC plan ?
 - The BCP should state essential functions of the business, identify which systems and processes must be sustained, & detail how to maintain them. It should take into account any possible business disruption

<http://searchdisasterrecovery.techtarget.com/definition/business-continuity-action-plan>

DR In Enterprise Architecture – Part 1

DISASTER RECOVERY

- DR considerations:
 - DR plan
 - RTO & RPO

DR In Enterprise Architecture – Part 1

- DR plan:
 - A disaster recovery policy statement, plan overview and main goals of the plan
 - Key personnel and DR team contact information

<http://searchdisasterrecovery.techtarget.com/definition/disaster-recovery>

DR In Enterprise Architecture – Part 1

- DR plan (contd)...:
 - Description of emergency response actions immediately following an incident.
 - A diagram of the entire network and recovery site.
 - Directions for how to reach the recovery site.

<http://searchdisasterrecovery.techtarget.com/definition/disaster-recovery>

DR In Enterprise Architecture – Part 1

- DR plan (contd)...:
 - A list of software and systems that will be used in the recovery.
 - Sample templates for a variety of technology recoveries, including technical documentation from vendors.

<http://searchdisasterrecovery.techtarget.com/definition/disaster-recovery>

DR In Enterprise Architecture – Part 1

A disaster recovery plan (DRP) is a formal document created by an organization that contains detailed instructions on how to respond to unplanned incidents such as natural disasters, power outages, cyber attacks and any other disruptive events. The plan contains strategies on minimizing the effects of a disaster, helping an organization to quickly resume key operations or continue to operate as if there was no disruption

- DR plan (contd)...:
 - Summary of insurance coverage.
 - Proposed actions for dealing with financial and legal issues.
 - Ready-to-use forms to help complete the plan.

DR In Enterprise Architecture – Part 1



<http://grcbizassurance.com/services/disaster-recovery/>

DR In Enterprise Architecture – Part 1

- RTO:
 - Max amount of time, following a disaster, for an org to recover files from backup storage and resume normal operations; max amount of downtime an org can handle.

<http://searchdisasterrecovery.techtarget.com/definition/disaster-recovery>

DR In Enterprise Architecture – Part 1

- RTO:
 - If an organization has an RTO of two hours, it cannot be down for longer than that

<http://searchdisasterrecovery.techtarget.com/definition/disaster-recovery>

DR In Enterprise Architecture – Part 1

- RPO:
 - RPO is the max age of files that an organization must recover from backup storage for normal operations to resume after a disaster; determines the minimum frequency of backups.

<http://searchdisasterrecovery.techtarget.com/definition/disaster-recovery>

DR In Enterprise Architecture – Part 1

- RPO:
 - For example, if an organization has an RPO of four hours, the system must back up at least every four hours

<http://searchdisasterrecovery.techtarget.com/definition/disaster-recovery>

DR In Enterprise Architecture – Part 2

- DR considerations:
 - DR facility
 - DR drills & testing
 - DR testing checklist
 - BC plan alignment

DR In Enterprise Architecture – Part 2

- DR facility:
 - Location
 - Media circuits and backup circuits
 - Power and environment
 - IT data center design
 - Based on DR plan
 - Operations & maintenance

DR In Enterprise Architecture – Part 2

- DR drills & testing:
 - Frequency and execution of DR drills as per IT policy of the org
 - Min twice a year and preferable quarterly for critical business reqmts
 - Backup testing

DR In Enterprise Architecture – Part 2

- DR testing checklist:
 - Secure management approval and funding for the test.
 - Provide detailed information about the test.
 - Make sure the entire test team is available on the planned test date.

<http://searchdisasterrecovery.techtarget.com/definition/disaster-recovery>

DR In Enterprise Architecture – Part 2

- DR testing checklist ...:
 - Ensure your test does not conflict with other scheduled tests or activities.
 - Confirm test scripts are correct.
 - Verify that the test environment is ready.
 - Schedule a dry run of the test.

<http://searchdisasterrecovery.techtarget.com/definition/disaster-recovery>

DR In Enterprise Architecture – Part 2

- DR testing checklist...:
 - Be ready to halt the test if needed.
 - Have a scribe take notes.
 - Complete an after-action report about what worked and what failed.
 - Use the test results to update DR plan

<http://searchdisasterrecovery.techtarget.com/definition/disaster-recovery>

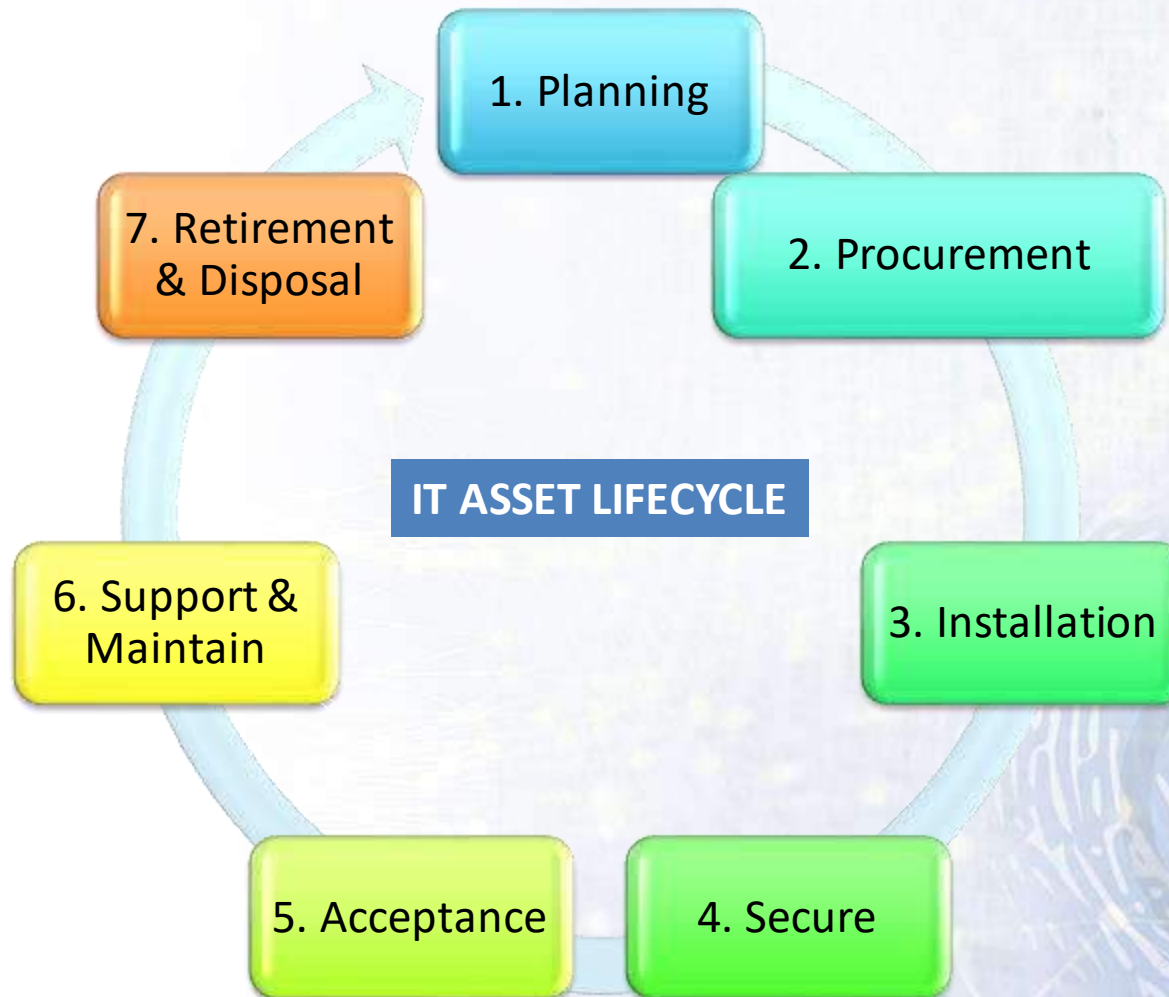
DR In Enterprise Architecture – Part 2

- BC plan alignment:
 - DR is under IT ownership, whereas BC is under business operations ownership
 - DR is part of overall BC
 - Both plans must integrate and align seamlessly

Role Of An IT Asset In Enterprise Security

- What is an IT asset ?
 - An IT asset is any resource such as hardware, software, information, human resource, or facility owned or utilized by the organization for IT processing

Role Of An IT Asset In Enterprise Security



Role Of An IT Asset In Enterprise Security

1. PLANNING

- Requirements
- Owner & Risk Owner
- High Level Design
- Budget Approvals
- Project Planning

2. PROCUREMENT

- RFP
- Vendor Selection
- PO
- Contract & SLA
- Kick-Off Meeting

3. INSTALLATION

- Site Preparation
- Delivery
- Configuration
- Testing
- Commissioning

4. SECURE

- Security Controls
- Security Checklist
- Security SOP
- Security Testing

5. ACCEPTANCE

- Test Scripts
- UAT
- Security Accreditation
- Commissioning Sign-off
- Change Management

6. SUPPORT/MAINTAIN

- Vendor Support
- Maintenance/Repair
- Change Requests
- Renewals & Upgrades
- Regular Updates
- Monitoring & Audits

7. RETIRE/DISPOSE

- Decommission
- Dispose/Salvage
- Update Inventory

Role Of An IT Asset In Enterprise Security



Role Of An IT Asset In Enterprise Security

- Asset Owner: a person in the org responsible for managing an asset (e.g. for laptop)
- Risk owner: manages risks associated with the IT asset. Authorized to make decisions associated with managing risks, and in a management position

Role Of An IT Asset In Enterprise Security

- Acceptable Use (Of IT Assets):
 - Laptops
 - Mobiles
 - Web browsing
 - Email usage
 - Servers
 - Company data

How To Determine Security Posture ?

- Questions to ask:
 - Information security policy ?
 - Organization security culture and tone at the top ?
 - Clearly designated responsibility for security ?
 - How many staff in security team [10%] and their roles ?

Case Study: Typical Security Posture

- Security hardening done on IT assets ?
- Which standard used for hardening ?
- Internal VM program ?
- Frequency of VM scanning ?
- Licensed software for OS/DB/Programs ?

Case Study: Typical Security Posture

- Last time penetration test was conducted by 3rd party ?
- Maturity of system security policies pushed through AD/GP
- DR and/or backup site ?
- When was the last time a DR drill was performed ?

Case Study: Typical Security Posture

- Is internal software developed? (Secure - SDLC)
- What is the mechanism to take backups of IT assets and to test backups?
- What is the maturity of access control for users, admins
- Regular audits for access control?

Case Study: Typical Security Posture

- What type of security controls implemented on any transactional systems such as mobile banking or internet banking (2FA)?
- Is critical data in org encrypted?
- How do you protect test data?

Case Study: Typical Security Posture

- What is the mechanism to perform security accreditation of new applications or systems?
- Is security embedded in critical business processes?
- Is there a business continuity and DR policy / mechanism?

Case Study: Typical Security Posture

- Security standard or framework followed for governance?
- Internal security awareness program?
- Maturity of change management and incident management
- Board Steering Committee (Information Security)

Case Study: Typical Security Posture

- Note: the implementers of the security measures are often not the ones giving the best answers
- Auditors & compliance team should also be queried
- Important question: have there been any recent incidents ?

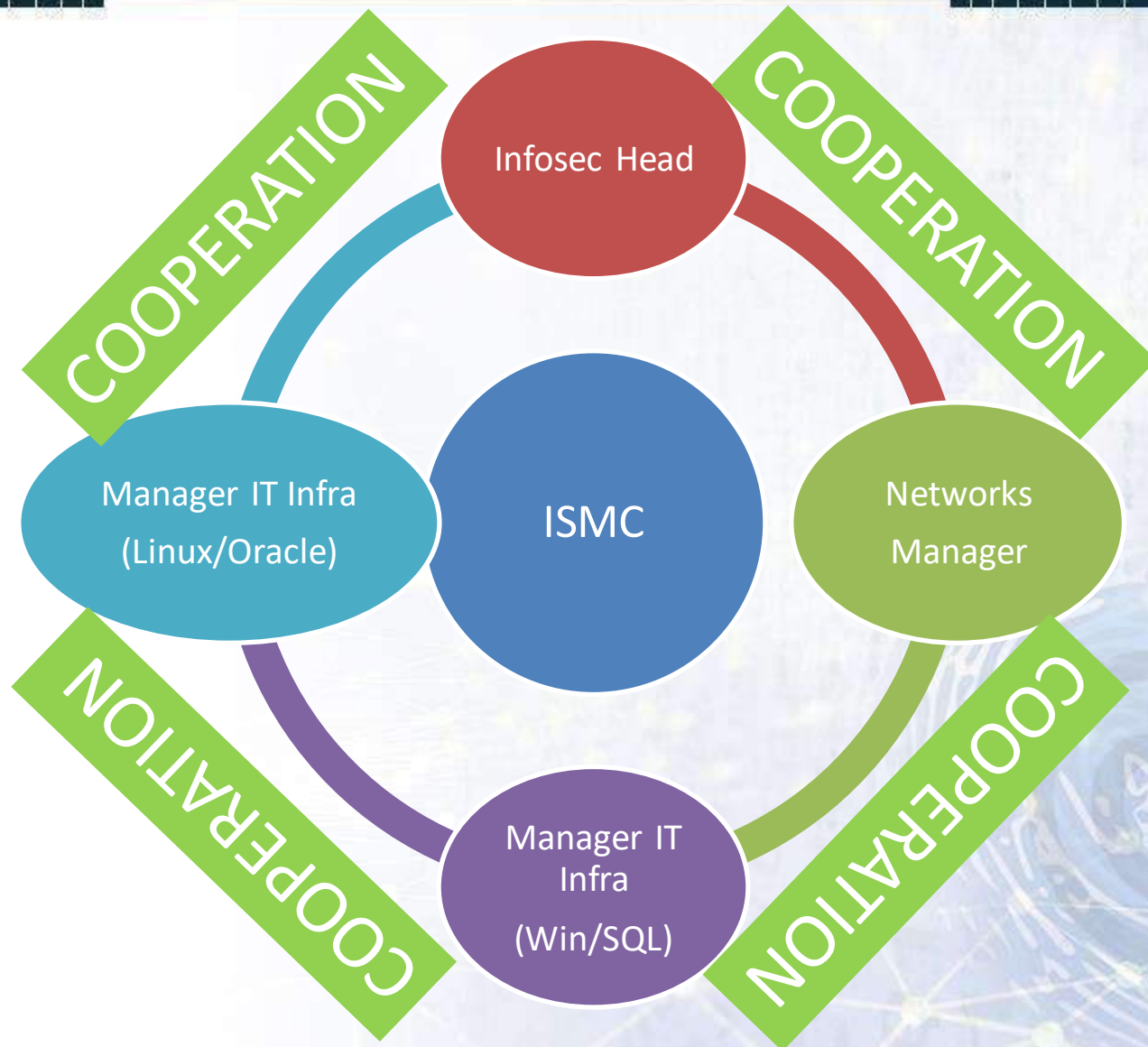
Driving Successful Security Transformation

- Critical factors for successful security transformation projects:
 - Board-level buy-in and sponsorship
 - Regular Board or Executive management project reviews and decisions
 - Allocation of sufficient priority & resources

Driving Successful Security Transformation

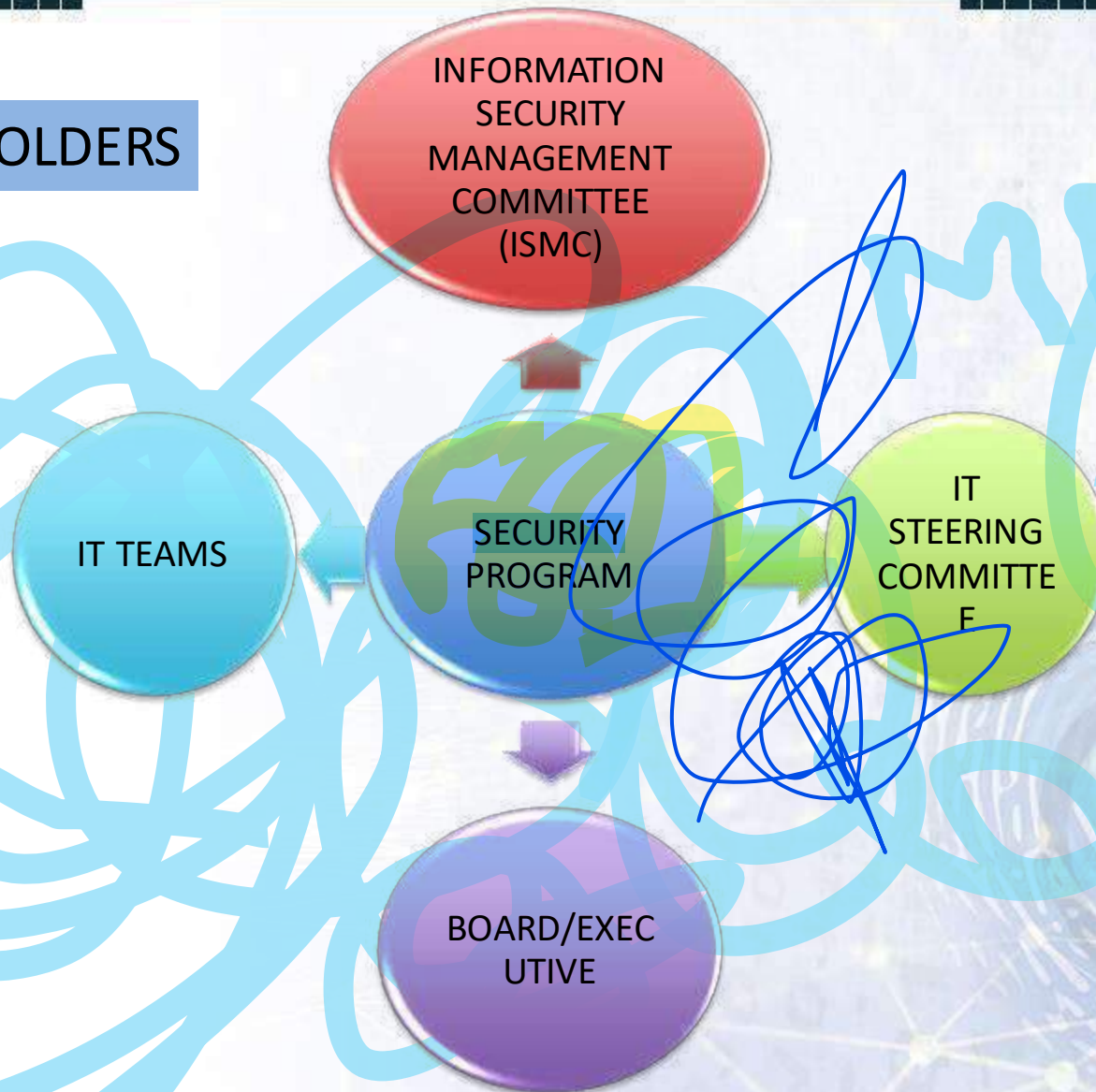
- Projects either fail or succeed before they begin !

Driving Successful Security Transformation

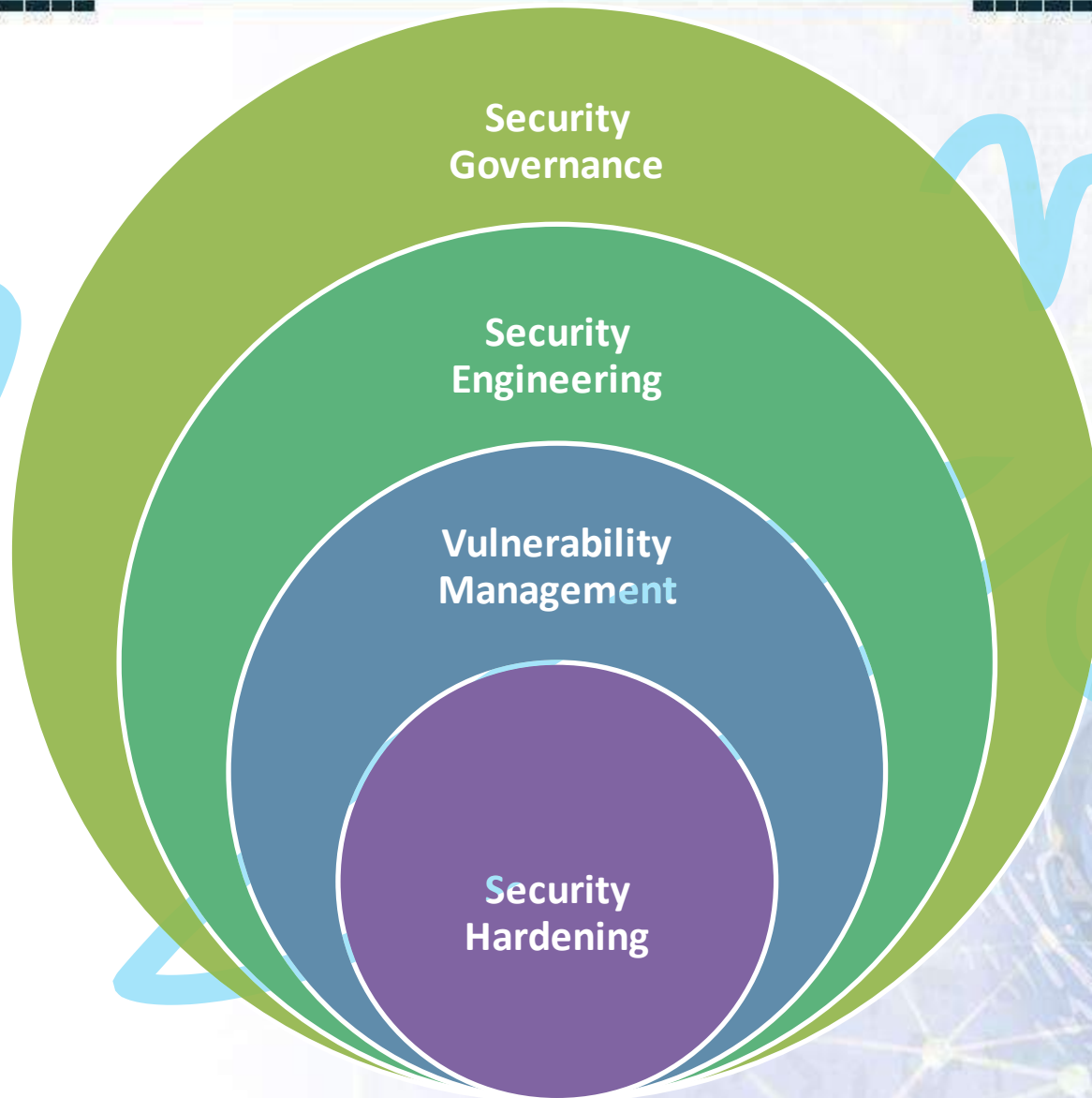


Driving Successful Security Transformation

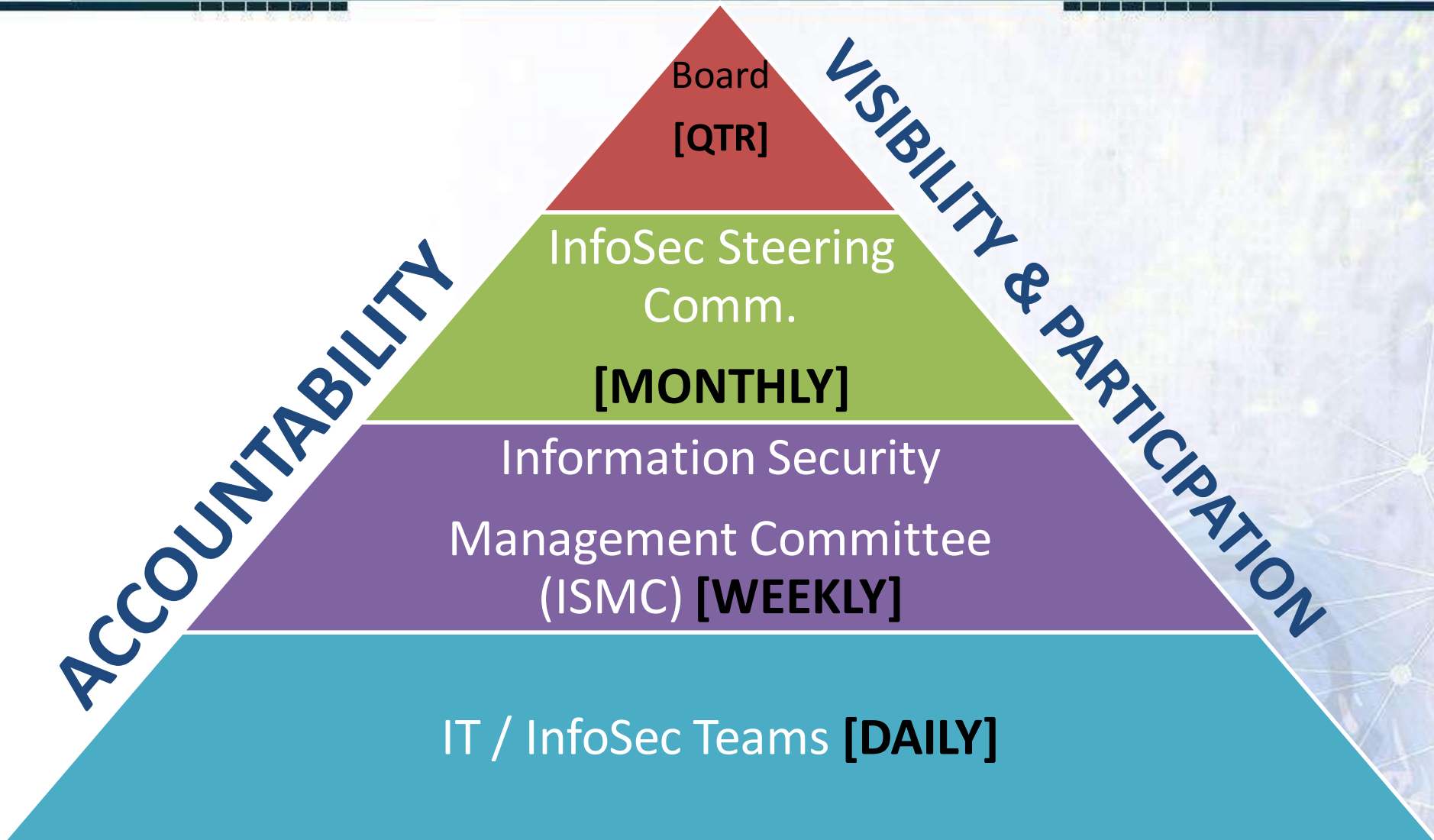
STAKEHOLDERS



Driving Successful Security Transformation



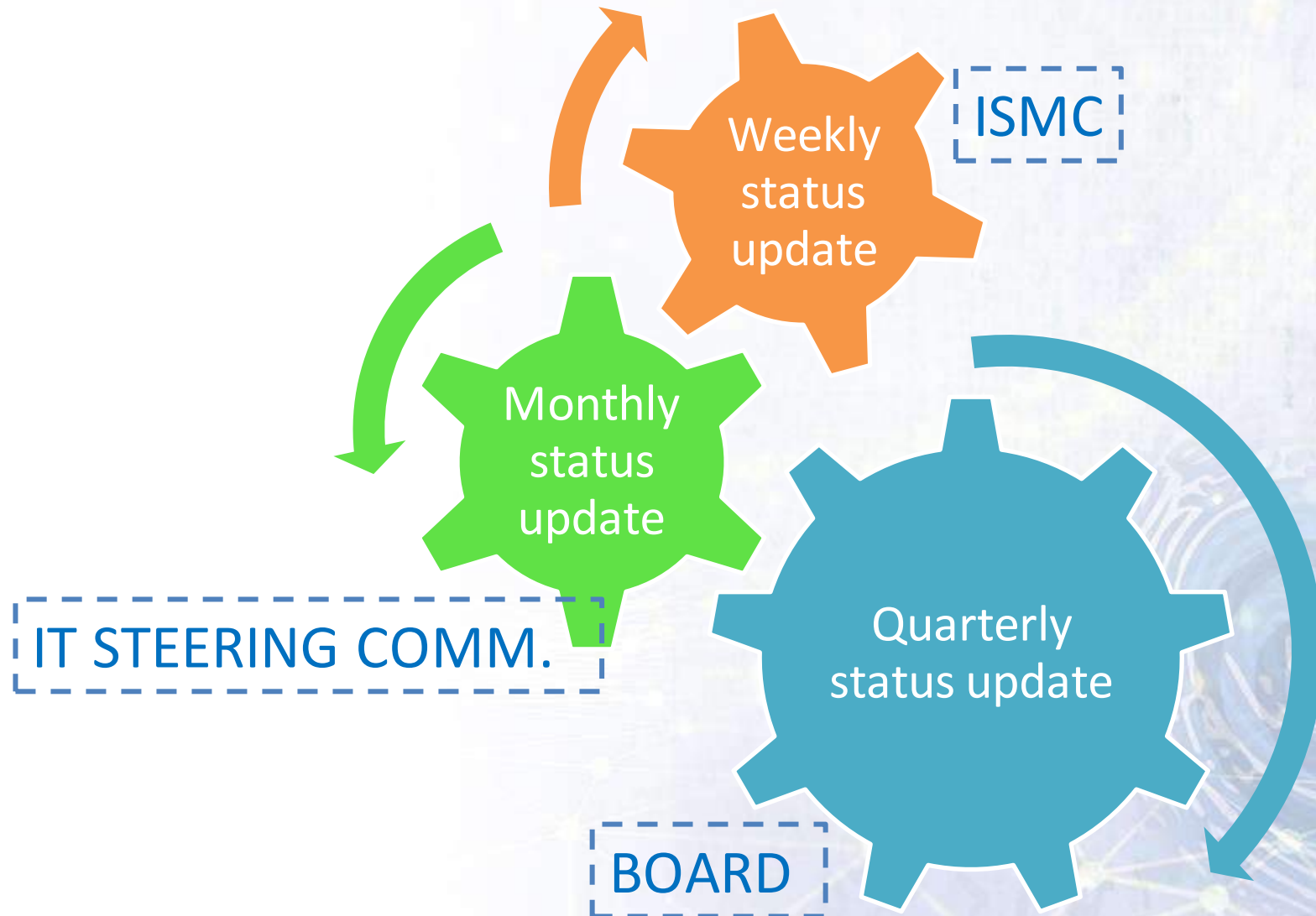
Driving Successful Security Transformation



Driving Successful Security Transformation



Driving Successful Security Transformation



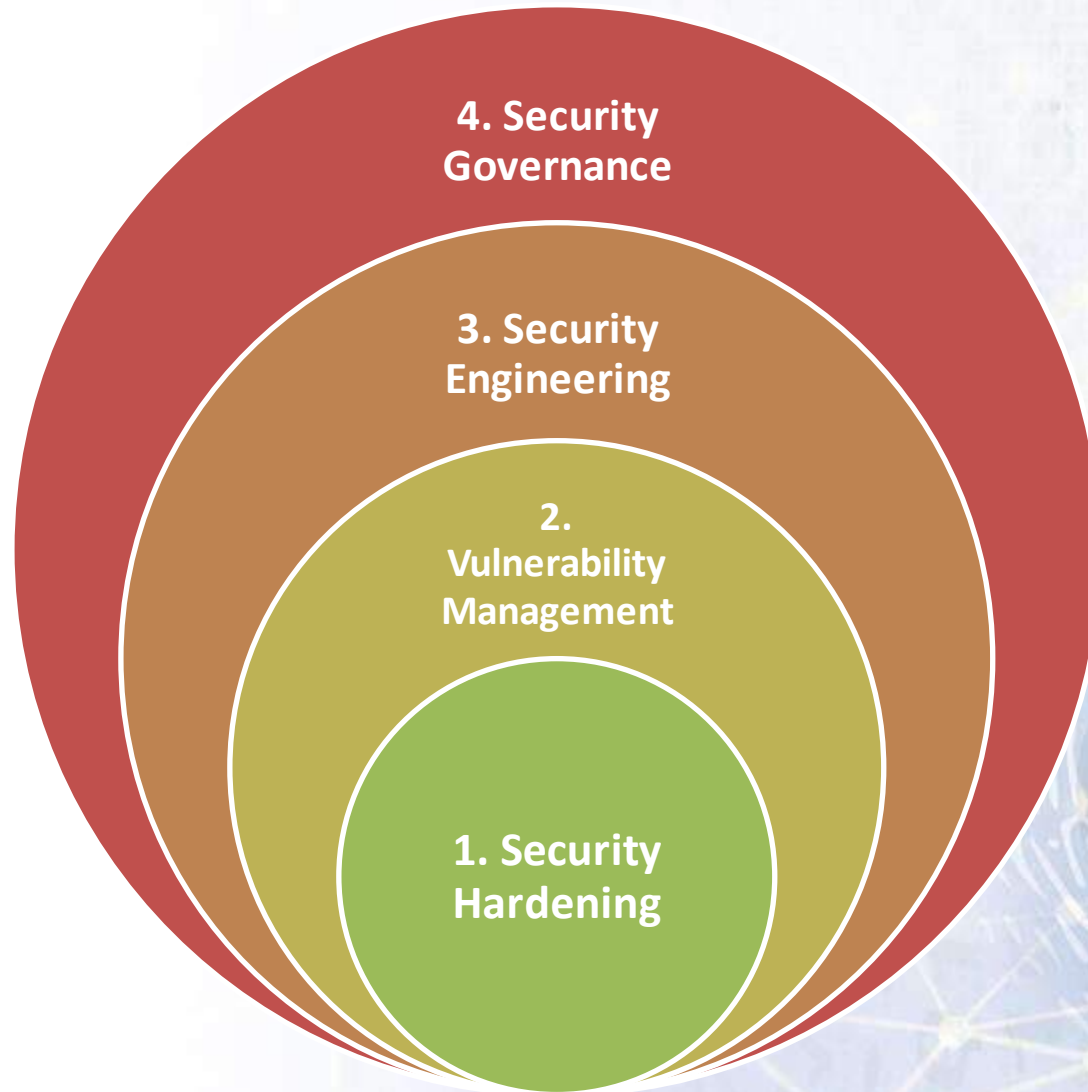
Driving Successful Security Transformation

- Successful security transformation projects can be made successful with correct sponsorship, structure, strategy, and strong project management

Difference Between Patching & Hardening

- Chapter 3
 - Security Transformation Stage 1: Security Hardening Of IT Assets

Revisit Of Security Transformation Model



Revisit Of Security Transformation Model

- Security hardening:
 - IT assets such as hardware and software come with default (insecure) configurations which become the basis for attacks
 - Typical case in point: username and password: “admin, admin”

Revisit Of Security Transformation Model

- Security hardening:
 - Process of securing a system by reducing its surface of vulnerability, which is larger when a system performs more functions; in principle a single-function system is more secure than a multipurpose one (Wikipedia)

Revisit Of Security Transformation Model

- Patching: Fixing vulnerabilities (which may be exploited by malware or attackers) in software or firmware with vendor released patches (auto or manual updates)
- Patches are also called fixes

<https://www.kenexis.com/patching-hardening-cybersecurity/>

Revisit Of Security Transformation Model

- Patching considerations:
 - Vendors release patch when they become aware of a vulnerability
 - Patches may be rolled up into a release
 - Off-the shelf software works well but testing reqd for customized instances

<https://www.kenexis.com/patching-hardening-cybersecurity/>

Revisit Of Security Transformation Model

- Hardening: includes additional steps beyond patching to limit the ways a hacker or malware could gain entry.
- Accomplished by turning on only the ports and services required, secure configuration of services & additional steps to limit system access

<https://www.kenexis.com/patching-hardening-cybersecurity/>

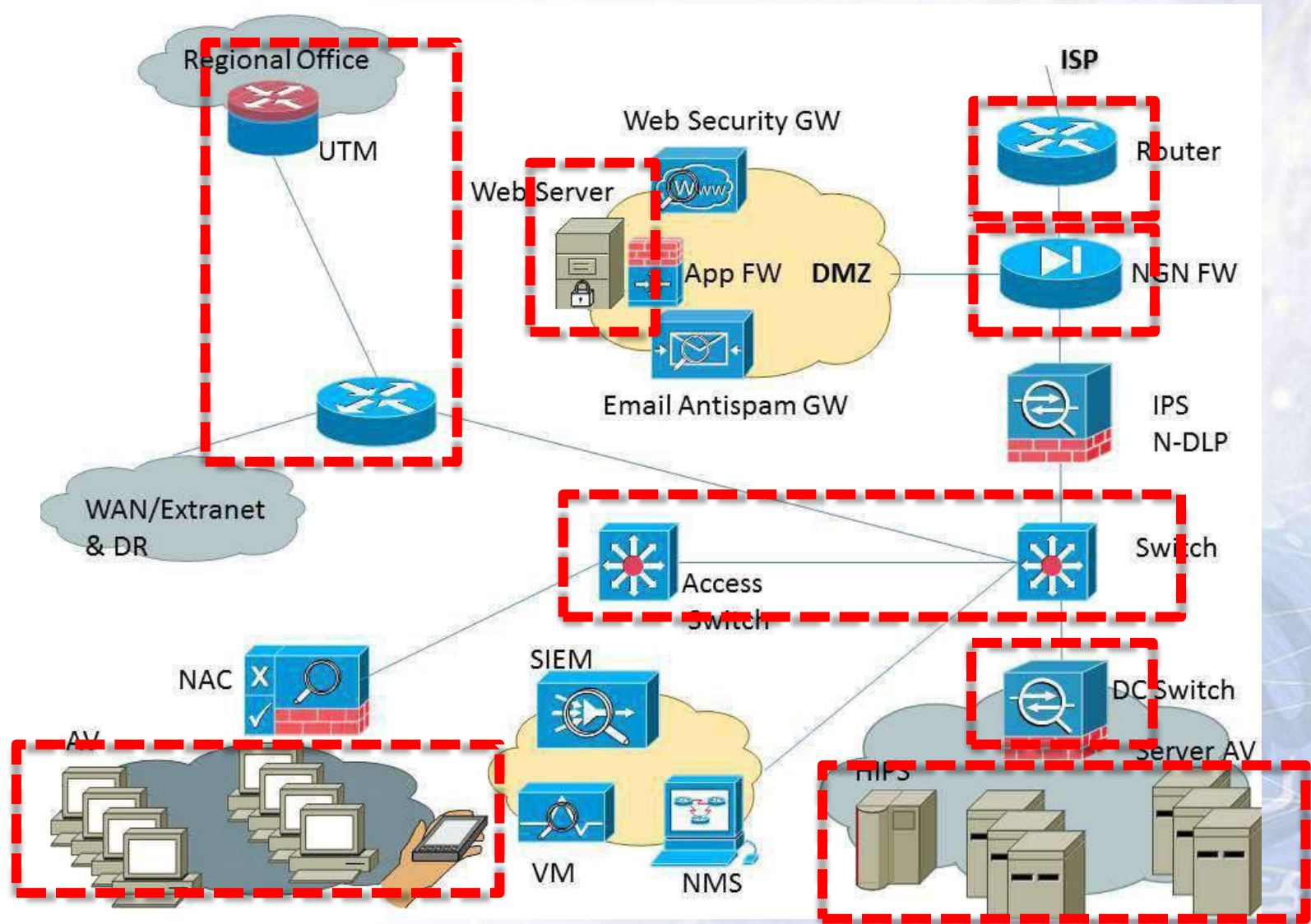
Revisit Of Security Transformation Model

- Note that both hardening & patching are required
 - Hardening prevents existing and future vulnerabilities by tightening configuration
 - Patching is more of a vendor driven process but essential nonetheless

Security Hardening Strategy

- Depending upon the size and type of the organization, there will be dozens, hundreds, or even thousands of IT assets to secure
- Priority is a key factor in all security undertakings
- Prioritize what is most important and needs to be done first
- Cascade as we go along

Security Hardening Strategy



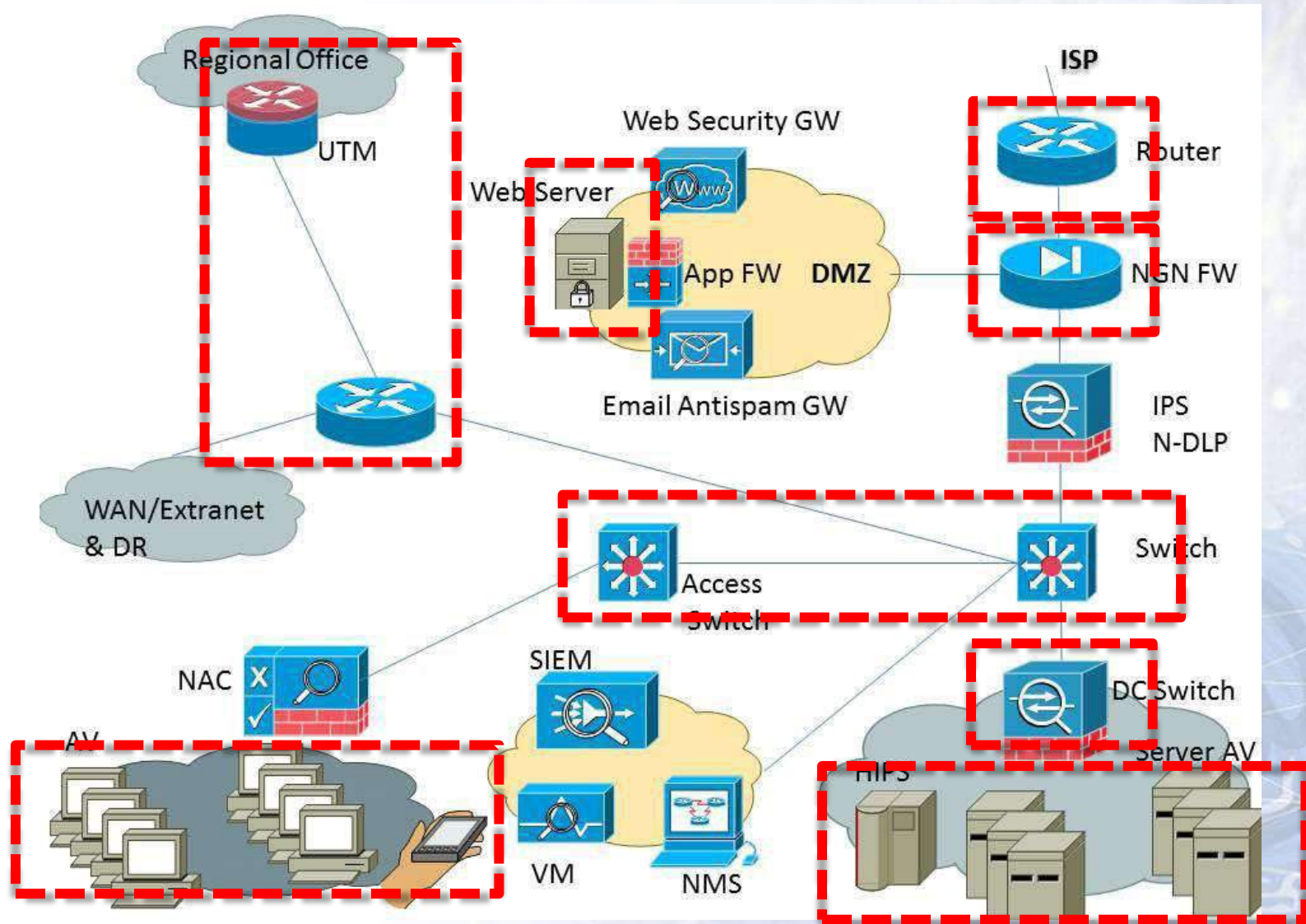
Security Hardening Strategy

- Separate security engineering (Step 3) from security hardening (step 1)
- Security engineering requires more thorough working so will slow down the security implementation
- Do the low hanging fruit first (security hardening)

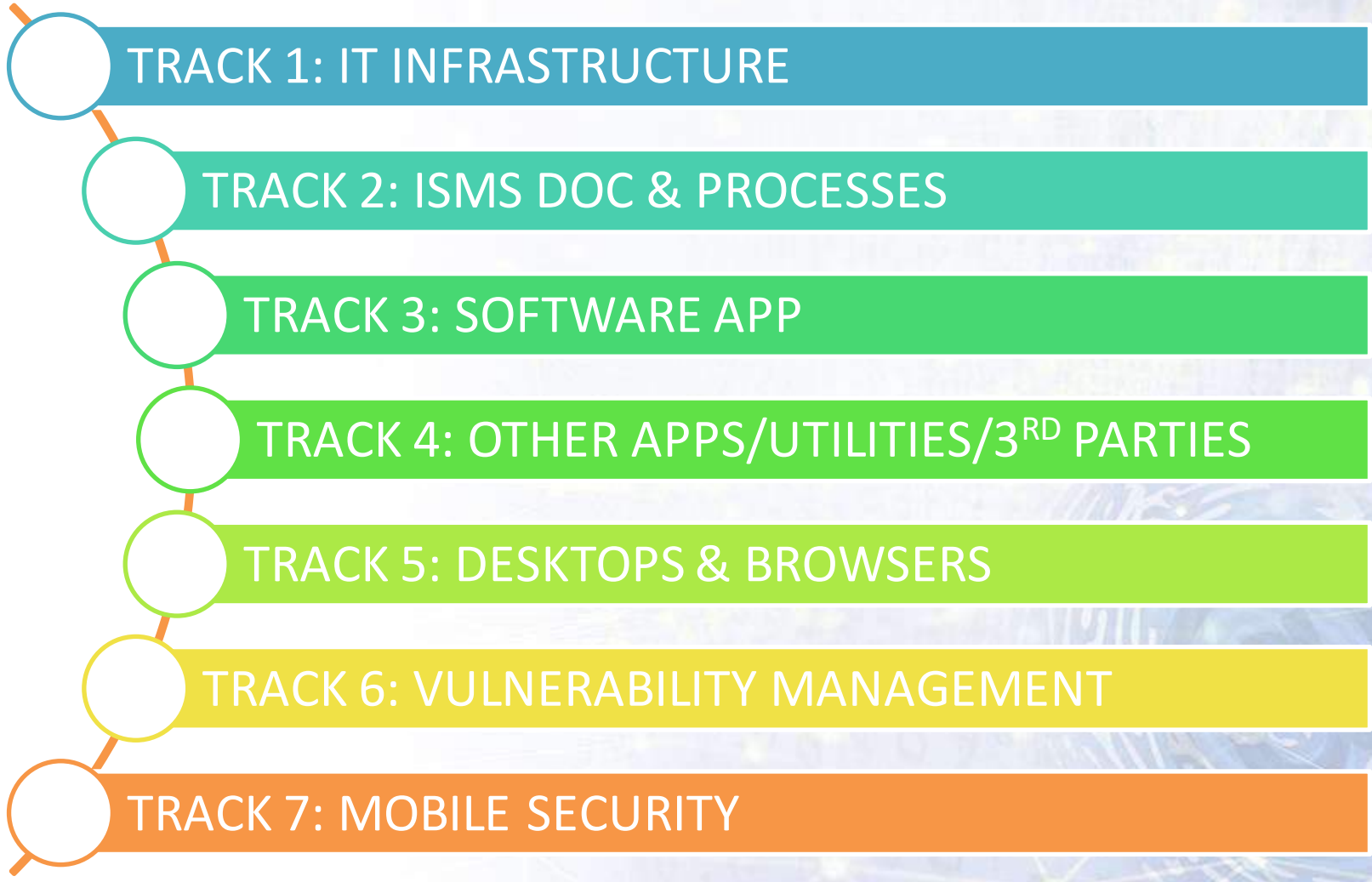
Security Hardening Strategy

- Minimum security baseline (MSB) refers to the obvious assets which need to be secured and the threshold which is the minimum expectation from the security program

Security Hardening Strategy



Security Hardening Strategy



TRACK 1: IT INFRASTRUCTURE

TRACK 2: ISMS DOC & PROCESSES

TRACK 3: SOFTWARE APP

TRACK 4: OTHER APPS/UTILITIES/3RD PARTIES

TRACK 5: DESKTOPS & BROWSERS

TRACK 6: VULNERABILITY MANAGEMENT

TRACK 7: MOBILE SECURITY

Security Hardening Strategy

- For a successful security transformation project, good planning, organization, and effective project management is essential

Pre-requisites For Security Hardening

1. Security program approved
2. Consultant on board
3. Project kick-off meeting held
4. ISMC team identified and their loading for this project communicated
5. Appraisal linkage of core resources announced by CIO

Pre-requisites For Security Hardening

1. Security program approved
 - Project director
 - Timeline
 - General project sequence and strategy
 - Understanding of main players and roles
 - Understanding of project structure

Pre-requisites For Security Hardening

2. Consultant on board
 - Expert consultants in security transformation can facilitate the project success
 - Third party & independent
 - Bring a focus on delivering results
 - Strong domain knowledge

Pre-requisites For Security Hardening

3. Project kick-off meeting held
 - Project goals & mission
 - All key stakeholders made aware of their roles
 - Responsibilities & authority
 - Success criteria & reporting mechanism

Pre-requisites For Security Hardening

4. ISMC team identified and their loading for this project communicated
 - ISMC plays a critical role
 - Cooperation & teamwork
 - Security leadership culture
 - Clarity on goals

Pre-requisites For Security Hardening

5. Appraisal linkage of core resources announced by CIO
 - Broader team
 - Announcement by CIO
 - Clarity on evaluation mechanism

Who Will Conduct The Security Hardening?

- Involvement of various stakeholders for security hardening
 - Operations teams
 - Security team
 - IT management
 - Consultant
 - Business

Who Will Conduct The Security Hardening?

IT Ops teams

Security
team

IT
management

Consultant

Business

Who Will Conduct The Security Hardening?

- IT Operations teams:
 - Study the security controls (CIS/DISA)
 - Apply the security controls in pilot/test environment
 - Report the completion of control implementation to ISMC
 - Assist InfoSec team with validation

Who Will Conduct The Security Hardening?

- InfoSec team:
 - Conduct validation of security controls implementation
 - Acquire checklist of controls from relevant IT team
 - Document the status of controls in the form of a checklist
 - Forward validation report to ISMC

Who Will Conduct The Security Hardening?

- IT management:
 - Ensure IT operations teams receive required guidance and support
 - Sign-off on change management requests
 - Assist with planning down-time and business related downtime

Who Will Conduct The Security Hardening?

- Consultant or project director:
 - Drives the security program
 - Ensures that strategy is aligned with project objectives
 - Ensures process and activities are moving at good momentum as per timeline

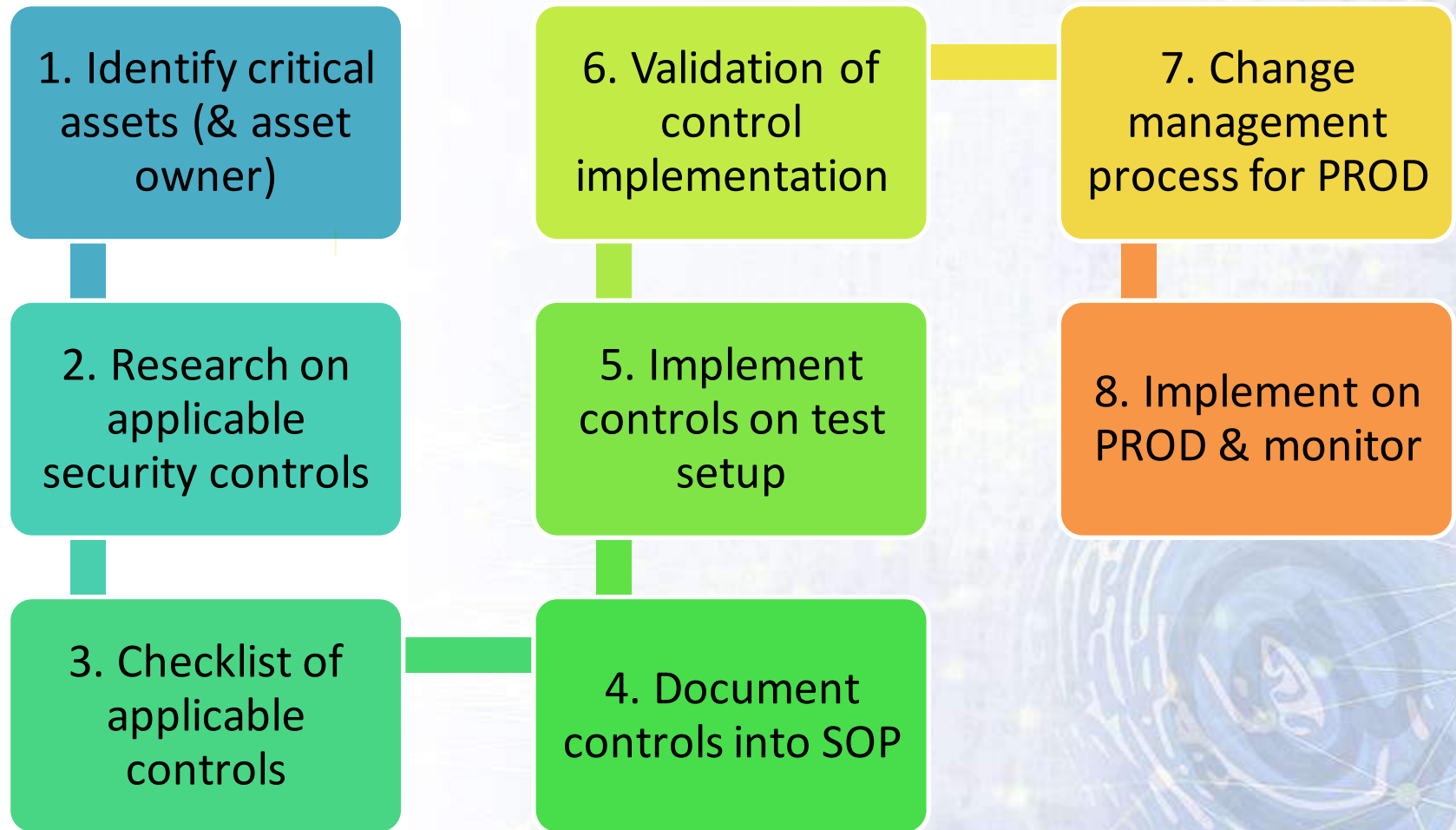
Who Will Conduct The Security Hardening?

- Business stakeholders:
 - Provide downtime approvals if required
 - Help to engage other vendors if applicable

8 Step Methodology – Security Hardening (1)

- What is the 8 step security hardening methodology?

8 Step Methodology – Security Hardening (1)



8 Step Methodology – Security Hardening (1)

- Purpose:
 - Many assets need to be hardened at various times, by various teams, for various requirements and projects
 - Standardize and follow a consistent approach

8 Step Methodology – Security Hardening (1)

- Benefits:
 - Process for security hardening
 - Discipline to always follow the same steps
 - Helps avoid missing any steps in the process
 - Gives team clarity on what to do and what sequence to follow

8 Step Methodology – Security Hardening (1)

- If You Skip This Process:
 - Will follow a new approach every time
 - Every resource has their own method
 - Dependence on resource rather than the process
 - Complicate rather than simplify
 - Divergence in security activities

8 Step Methodology – Security Hardening (1)

HEAD OF DEPT

ISMC

- DRIVES THE PROGRAM
- DECISION MAKING
- INCLUDES ALL 3-4 DOMAIN TEAM LEADS

TEAM LEAD

- MEMBER OF ISMC
- REPORTS TO HEAD OF THE DEPT

IT OPS TEAM

- TEAM THAT WILL IMPLEMENT THE SECURITY CONTROLS

INFOSEC TEAM

- REPORTS TO CISO OR INFOSEC HEAD
- OR LED BY CONSULTANT

8 Step Methodology – Security Hardening (1)

STEP	DESCRIPTION	PERFORMED BY	FACILITATED BY
1	IDENTIFY CRITICAL ASSETS (& ASSET OWNER)	ISMC	HEAD OF IT SECTION
2	RESEARCH APPLICABLE SECURITY CONTROLS	INFOSEC TEAM	ISMC
3	CHECLIST OF APPLICABLE SECURITY CONTROLS	INFOSEC TEAM	TEAM LEAD
4	DOCUMENT CONTROLS INTO SOP	TEAM LEAD	INFOSEC TEAM
5	IMPLEMENT CONTROLS ON TEST SETUP	IT OPERATIONS TEAM	TEAM LEAD
6	VALIDATION OF CONTROL IMPLEMENTATION	INFOSEC TEAM	IT OPERATIONS TEAM
7	CHANGE MANAGEMENT PROCESS FOR PRODUCTION	TEAM LEAD	ISMC
8	PRODUCTION & MONITOR	IT OPERATIONS TEAM	TEAM LEAD

8 Step Methodology – Security Hardening (1)

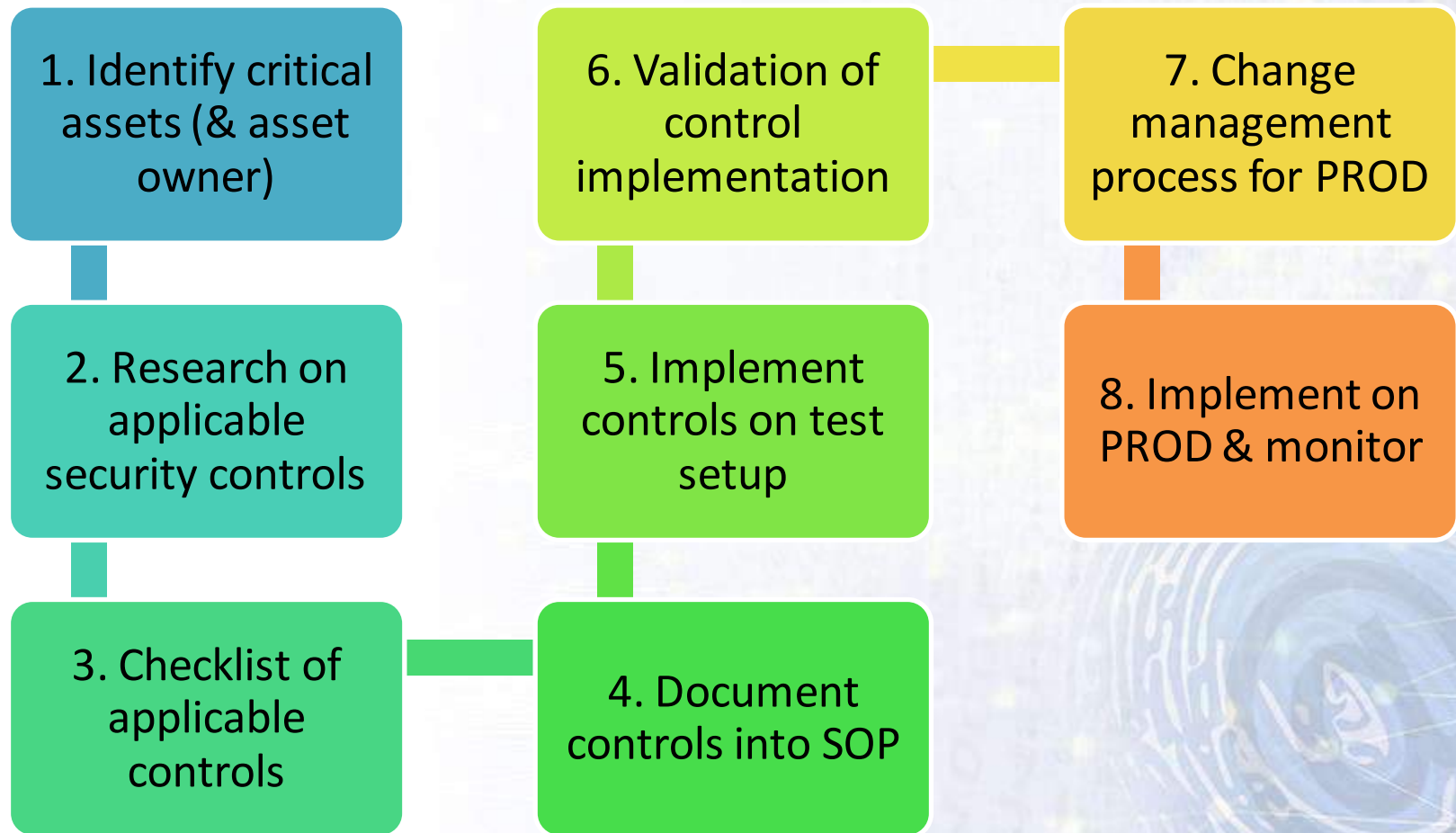
- Lets look at the steps in detail in the next module

END

8 Step Methodology – Security Hardening (2)

- Step 1: Identify Critical Assets & Asset Owner:
 - Asset inventory & infrastructure diagram
 - Examine risks
 - Analyze assets at a high level and prioritize
 - Minimum security baseline (MSB)
 - Break into phases

8 Step Methodology – Security Hardening (2)



8 Step Methodology – Security Hardening (2)

- Step 2: Research on applicable security controls
 - CIS, DISA
 - Search on google
 - Review standards/frameworks (ISO27001, PCI, etc)
 - Look at OWASP, CSA, NIST, CIS Top 20
 - Selection of controls

8 Step Methodology – Security Hardening (2)

- Step 3: Checklist of applicable security controls
 - Checklist for progress tracking
 - Share with appropriate IT team
 - Forms record for controls trail

8 Step Methodology – Security Hardening (2)

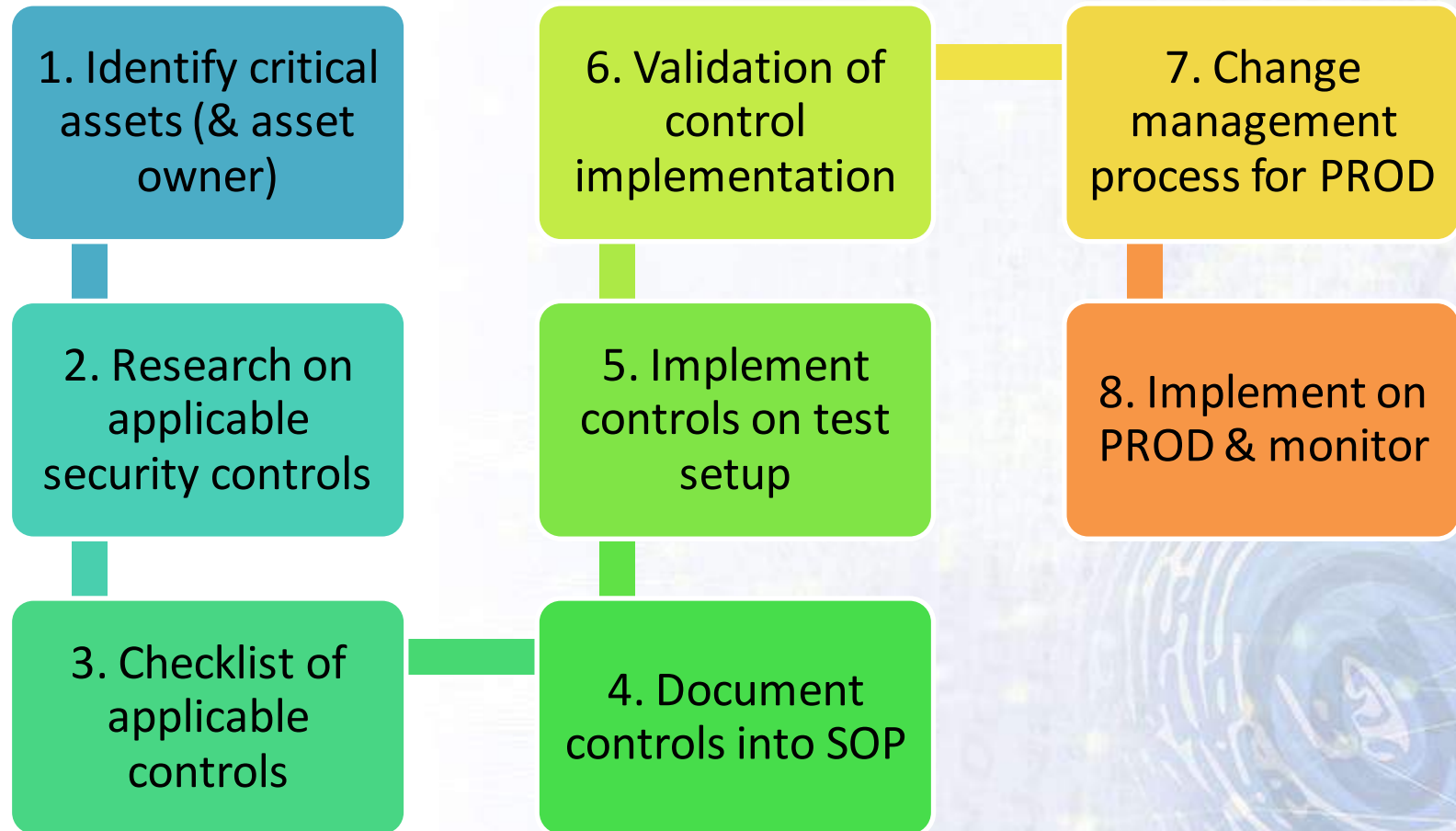
- Step 4: Document controls into SOP
 - Enter controls set into draft SOP
 - Who will do what when, (and briefly how)
 - Get Dept Head agreement and sign-off on checklist and SOP

END

8 Step Methodology – Security Hardening (3)

- Step 5: Implement controls on test setup
 - Relevant IT team to implement controls on test setup
 - Update checklist
 - Update SOP (if necessary)
 - Send checklist back to InfoSec team

8 Step Methodology – Security Hardening (3)



8 Step Methodology – Security Hardening (3)

- Step 6: Validation of control implementation (by InfoSec team)
 - InfoSec resource with relevant domain knowledge
 - Conduct preparation before actual validation (study controls)
 - Update checklist with status column

8 Step Methodology – Security Hardening (3)

- Step 7: Change management process for PRODUCTION:
 - ISMC receives validation status from InfoSec team
 - Relevant dept head takes up change management process and prepares for shifting to PROD
 - Rollback, impact etc

8 Step Methodology – Security Hardening (3)

- Step 8: Implement on PROD & monitor:
 - Monitor closely for 24-48 hours after moving to PROD
 - Rollback in case of unforeseen circumstances
 - IT team SOP finalized and now ops task

END

A Look At CIS Security Benchmarks (1)

- Center for Internet Security (CIS)
 - <https://www.cisecurity.org/cis-benchmarks/>
 - Fill out your details and will receive an email with link

A Look At CIS Security Benchmarks (1)



CIS Benchmarks

You now have access to all of our CIS Benchmark PDFs. Feel free to download as many as you like!

If you have any issues accessing the files, please let us know at learn@cisecurity.org.

Looking for a previous version of a CIS Benchmark? See our [archive](#).

Operating Systems

Distribution Independent Linux Linux

CIS Distribution Independent Linux Benchmark v1.0.1

[Download PDF](#)

Microsoft Windows Desktop Microsoft Windows

CIS Microsoft Windows 10 Enterprise Release 1607 Benchmark v1.2.0

[Download PDF](#)

A Look At CIS Security Benchmarks (2)

#	OVERALL CIS BENCHMARK CATEGORIES	TOTAL
1	OPERATING SYSTEMS	36
2	SERVER SOFTWARE	33
3	CLOUD PROVIDERS	2
4	MOBILE DEVICES	8
5	NETWORK DEVICES	6
6	DESKTOP SOFTWARE	21
7	MULTIFUNCTION PRINT DEVICES	1
	GRAND TOTAL CIS BENCHMARKS	107

A Look At CIS Security Benchmarks (1)

#	OPERATING SYSTEMS	TOTAL
1	DISTRIBUTION INDEPENDENT LINUX	1
2	MICROSOFT WINDOWS DESKTOP	5
3	DEBIAN LINUX	2
4	UBUNTU LINUX	3
5	AMAZON LINUX	1
6	CENTOS LINUX	2
7	ORACLE LINUX	2

A Look At CIS Security Benchmarks (1)

#	OPERATING SYSTEMS (CONTD)...	TOTAL
8	REDHAT LINUX	3
9	SUSE LINUX	2
10	APPLE OS (UNIX)	5
11	IBM AIX (UNIX)	1
12	ORACLE SOLARIS (UNIX)	3
13	MS WINDOWS SERVER	6
	TOTAL BENCH MARKS OPERATING SYSTEMS	36

A Look At CIS Security Benchmarks (1)

Microsoft Windows Desktop

Microsoft Windows

CIS Microsoft Windows 10 Enterprise Release 1607 Benchmark v1.2.0

CIS Microsoft Windows 8.1 Workstation Benchmark v2.2.1

CIS Microsoft Windows 7 Workstation Benchmark v3.0.1

CIS Microsoft Windows XP Benchmark v3.1.0

CIS Microsoft Windows 8 Benchmark v1.0.0

A Look At CIS Security Benchmarks (1)

Microsoft Windows Server

Microsoft Windows

CIS Microsoft Windows Server 2016 RTM (Release 1607) Benchmark v1.0.0

CIS Microsoft Windows Server 2008 (non-R2) Benchmark v3.0.1

CIS Microsoft Windows Server 2008 R2 Benchmark v3.0.1

CIS Microsoft Windows Server 2012 R2 Benchmark v2.2.1

CIS Microsoft Windows Server 2012 (non-R2) Benchmark v2.0.1

CIS Microsoft Windows Server 2003 Benchmark v3.1.0

A Look At CIS Security Benchmarks (1)

#	SERVER SOFTWARE	TOTAL
1	MICROSOFT IIS (WEB SERVER)	3
2	VMWARE (VIRTUALIZATION)	2
3	MONGODB (DATABASE SERVER)	3
4	IBM DB2 (DATABASE SERVER)	3
5	BIND (DNS SERVER)	1
6	APACHE TOMCAT (WEB SERVER)	2
7	MICROSOFT SQL SERVER (DB SERVER)	3

A Look At CIS Security Benchmarks (1)

#	SERVER SOFTWARE (CONTD)...	TOTAL
8	APACHE (HTTP SERVER)	2
9	DOCKER (VIRTUALIZATION)	5
10	ORACLE (DATABASE SERVER)	3
11	KUBERNETES (VIRTUALIZATION)	1
12	MIT KERBEROS (AUTHENTICATION)	1
13	ORACLE MySQL (DB SERVER)	4
	TOTAL BENCH MARKS SERVER SOFTWARE	33

A Look At CIS Security Benchmarks (1)

Microsoft SQL Server Database Server

CIS Microsoft SQL Server 2008 R2 Benchmark v1.4.0

CIS Microsoft SQL Server 2012 Benchmark v1.3.0

CIS Microsoft SQL Server 2014 Benchmark v1.2.0

A Look At CIS Security Benchmarks (1)

#	CLOUD PROVIDERS	TOTAL
1	AMAZON WEB SERVICES	2
	TOTAL CLOUD PROVIDERS	2

A Look At CIS Security Benchmarks (1)

- Next module...remaining categories

END

A Look At CIS Security Benchmarks (2)

- Mobile devices, network devices, desktop software, multifunction print devices

A Look At CIS Security Benchmarks (2)

#	MOBILE DEVICES	TOTAL
1	APPLE IOS	5
2	GOOGLE ANDROID	3
	TOTAL BENCH MARKS MOBILE DEVICES	8

A Look At CIS Security Benchmarks (2)

#	NETWORK DEVICES	TOTAL
1	CISCO	4
2	PALO ALTO NETWORKS	2
	TOTAL BENCH MARKS NETWORK DEVICES	6

A Look At CIS Security Benchmarks (2)

#	DESKTOP SOFTWARE	TOTAL
1	MICROSOFT OFFICE	13
2	GOOGLE CHROME (WEB BROWSER)	1
3	MS EXCHANGE SERVER	3
4	MS INTERNET EXPLORER	2
5	MOZILLA FIREFOX	2
	TOTAL BENCH MARKS DESKTOP SOFTWARE	21

A Look At CIS Security Benchmarks (2)

#	MULTIFUNCTION PRINT DEVICES	TOTAL
1	MULTIFUNCTION DEVICE	1
	TOTAL BENCH MARKS MULTIFUNCTION PRINT DEVICES	1

A Look At CIS Security Benchmarks (2)

Apple iOS

CIS Apple iOS 10 Benchmark v2.0.0

CIS Apple iOS 9 Benchmark v1.0.0

CIS Apple iOS 8 Benchmark v1.0.0

CIS Apple iOS 7 Benchmark v1.1.0

CIS Apple iOS 6 Benchmark v1.0.0

A Look At CIS Security Benchmarks (2)

Google Android

CIS Google Android 7 Benchmark v1.0.0

CIS Google Android 4 Benchmark v1.0.0

CIS Google Android 2.3 Benchmark v1.1.0

A Look At CIS Security Benchmarks (2)

Cisco

CIS Cisco Firewall Benchmark v4.0.0

CIS Cisco IOS 12 Benchmark v4.0.0

CIS Cisco IOS 15 Benchmark v4.0.0

CIS Cisco Wireless LAN Controller 7 Benchmark v1.1.0

A Look At CIS Security Benchmarks (2)

Microsoft Office

Productivity Software

CIS Microsoft Office 2016 Benchmark v1.1.0

CIS Microsoft Office PowerPoint 2016 Benchmark v1.0.1

CIS Microsoft Office PowerPoint 2013 Benchmark v1.0.1

CIS Microsoft Office Excel 2016 Benchmark v1.0.1

CIS Microsoft Office Excel 2013 Benchmark v1.0.1

CIS Microsoft Office Access 2016 Benchmark v1.0.1

CIS Microsoft Office Access 2013 Benchmark v1.0.1

A Look At CIS Security Benchmarks (2)

CIS Microsoft Office 2013 Benchmark v1.1.0

CIS Microsoft Office Word 2016 Benchmark v1.1.0

CIS Microsoft Office Word 2013 Benchmark v1.1.0

CIS Microsoft Office Outlook 2016 Benchmark v1.1.0

CIS Microsoft Office Outlook 2013 Benchmark v1.1.0

CIS Microsoft Outlook 2010 Benchmark v1.0.0

A Look At CIS Security Benchmarks (1)

- Next module... further details

END

A Look At CIS Security Benchmarks (3)

- CIS Benchmarks example (Network Devices)

A Look At CIS Security Benchmarks (3)

#	OVERALL CIS BENCHMARK CATEGORIES	TOTAL
1	OPERATING SYSTEMS	36
2	SERVER SOFTWARE	33
3	CLOUD PROVIDERS	2
4	MOBILE DEVICES	8
5	NETWORK DEVICES	6
6	DESKTOP SOFTWARE	21
7	MULTIFUNCTION PRINT DEVICES	1
	GRAND TOTAL CIS BENCHMARKS	107

A Look At CIS Security Benchmarks (3)

CIS Cisco Firewall Benchmark

v4.0.0 - 06-29-2016

- June 29, 2016
- 174 pages PDF doc

A Look At CIS Security Benchmarks (3)

- Control content:
 - Profile applicability (ASA 8.X, ASA 9.X)
 - Description
 - Rationale
 - Audit
 - Remediation
 - Default value
 - References

A Look At CIS Security Benchmarks (3)

- 1.8 (page 88); Session Timeout
 - Profile applicability: Level 1, Cisco ASA9.X
 - Description: Sets the idle timeout for a console session before the security appliance terminates it.

A Look At CIS Security Benchmarks (3)

- 1.8 (page 88); Session Timeout
 - Rationale: Limiting session timeout prevents unauthorized users from using abandoned sessions to perform malicious activities.

A Look At CIS Security Benchmarks (3)

Audit:

- Step 1: Run the following command to show what the console timeout is set to

```
hostname#sh run console | in timeout.5
```

The output should look like

```
console timeout 5
```

Example:

```
Asa-fw#sh run console | in timeout.5  
console timeout 5
```

Here the session timeout is 5 minutes

- Step 2: If an output is displayed, the system is compliant. If not, there is a finding.

A Look At CIS Security Benchmarks (3)

Remediation:

- Step 1: Run the following command to set the console timeout to less than or equal to 5 minutes

```
hostname(config)# console timeout 5
```


A Look At CIS Security Benchmarks (3)

- 1.8 (page 88); Session Timeout
 - Default Value: The default timeout is 0, which means the console session will not time out

A Look At CIS Security Benchmarks (3)

- 1.8 (page 88); Session Timeout
 - Reference: CLI Book 1: Cisco ASA Series General Operations CLI Configuration Guide, 9.1

A Look At CIS Security Benchmarks (4)

- CIS Benchmarks
example (Operating
Systems)
 - MS Windows Server
2012-R2

A Look At CIS Security Benchmarks (4)

#	OVERALL CIS BENCHMARK CATEGORIES	TOTAL
1	OPERATING SYSTEMS	36
2	SERVER SOFTWARE	33
3	CLOUD PROVIDERS	2
4	MOBILE DEVICES	8
5	NETWORK DEVICES	6
6	DESKTOP SOFTWARE	21
7	MULTIFUNCTION PRINT DEVICES	1
	GRAND TOTAL CIS BENCHMARKS	107

A Look At CIS Security Benchmarks (4)

CIS Microsoft Windows Server 2012 R2 Benchmark

v2.2.1 - 01-31-2017

- January 31, 2017
- 760 pages PDF doc

A Look At CIS Security Benchmarks (4)

- Profile applicability:
 - Level 1 domain controller
 - Level 1 member server
 - **Level 2 domain controller**
 - **Level 2 member server**

A Look At CIS Security Benchmarks (4)

- Level 1: Items in this profile intend to:
 - be practical and prudent;
 - provide a clear security benefit; and
 - not inhibit the utility of the technology beyond acceptable means

A Look At CIS Security Benchmarks (4)

- Level 2: extends the Level 1 - profile
 - intended for environments or use cases where security is paramount
 - acts as defense in depth measure
 - may negatively inhibit the utility or performance of the technology

A Look At CIS Security Benchmarks (4)

- Control content:
 - Profile applicability (ASA 8.X, ASA 9.X)
 - Description
 - Rationale
 - Audit
 - Remediation
 - **Impact**
 - Default value
 - References

A Look At CIS Security Benchmarks (4)

- 1.1.2 [L1]: *Ensure 'Maximum password age' is set to '60 or fewer days, but not 0' (Scored)*
 - *Profile applicability:
Level 1 Domain
Controller, Level 1
Member Server*

A Look At CIS Security Benchmarks (4)

- 1.1.2 [L1] Description:
 - This policy setting defines how long a user can use their password before it expires.
 - Values for this policy setting range from 0 to 999 days. If you set the value to 0, the password will never expire.

A Look At CIS Security Benchmarks (4)

- 1.1.2 [L1] Audit:
 - Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed.

A Look At CIS Security Benchmarks (4)

Remediation:

To establish the recommended configuration via GP, set the following UI path to 60 or fewer days, but not 0:

```
Computer Configuration\Policies\Windows Settings\Security Settings\Account Policies\Password Policy\Maximum password age
```

A Look At CIS Security Benchmarks (4)

- 1.1.2 [L1] Default Value: 42 days
- 1.1.2 [L1] Reference: CCE-37167-4
 - Common Configuration Enumeration (Unique identifiers for common system config issues)

END

A Look At DISA STIGs (1)

department of defence

cis refer to as banche mark
disa refer to as stigs

CIA in the form of pdf
disa has a stigs viewer
and have a java file that imports into a viewer the
operate the stigs

- USA DoD
- Security Technical Implementation Guides (STIGs)
- Most expansive security benchmarks available
- Most regularly updated
- Unclassified version
- <http://iase.disa.mil/stigs/Pages/index.aspx>
- 425 STIGs available

A Look At DISA STIGs (1)

What are DISA and STIG?

Security Technical Implementation Guides (STIGs) are configuration standards developed by the Defense Information Systems Agency (DISA). They are designed to make device hardware and software as secure as possible, safeguarding the Department of Defense (DoD) IT network and systems.

- STIGs master list (A-Z):
 - <http://iase.disa.mil/stigs/Pages/a-z.aspx>
- STIG viewer:
 - <http://iase.disa.mil/stigs/Pages/stig-viewing-guidance.aspx>

home
MASTER LIST
VIEWER
VIEWR DOWNLOAD
LIBRARY COMPLATION
VEWER DOWNLOAD
IMPORT STIGS

A Look At DISA STIGs (1)



IASE

Information Assurance
Support Environment

All Sites



Home

Cybersecurity Training ▼

Topic Map ▼

STIGs ▼

Tools ▼

News

Help

RSS Feeds

► STIGs Home

Control Correlation Identifier (CCI)

DoD Annex for NIAP Protection Profiles

DoD Secure Host Baseline Repository *PKI

FAQs

Quarterly Release Schedule and Summary

► SRG/STIG Tools

SRG-STIG Library Compilations

STIG Mailing List

STIGs Master List (A to Z)

► STIGs Technologies

Vendor Process

Contact Us

*PKI = DoD PKI Cert Required

STIGs HOME

Home > STIGs

Security Technical Implementation Guides (STIGs)

STIGs Updates!

- Draft Voice Video Policy STIG Version 1 - Update 6/26/2017
- Draft Voice Video Policy STIG Version 1 - Release Memo - Update 6/26/2017
- Draft Voice Video Policy STIG Version 1 - Comment Matrix - Update 6/26/2017
- STIG Viewer 2.5.4 - Update 6/23/2017
- STIG Viewer 2.5.4 Hashes - Update 6/23/2017
- Draft Apple OS X 10.12 STIG - Version 1 - Update 5/25/2017
- Draft Apple OS X 10.12 STIG - Release Memo - Update 5/25/2017
- Draft Apple OS X 10.12 STIG - Comment Matrix - Update 5/25/2017

The Security Technical Implementation Guides (STIGs) and the NSA Guides are the configuration standards for DOD IA and IA-enabled devices/systems. Since 1998, DISA has played a critical role enhancing the security posture of DoD's security systems by providing the Security Technical Implementation Guides (STIGs). The STIGs contain technical guidance to "lock down" information systems/software that might otherwise be vulnerable to a malicious computer attack.

A Look At DISA STIGs (1)



IASE

Information Assurance
Support Environment

All Sites



Home

Cybersecurity Training ▼

Topic Map ▼

STIGs ▼

Tools ▼

News

Help

RSS Feeds

Home > STIGs > STIGs A-Z

STIGs Master List (A to Z)

*PKI = DoD PKI Certificate Required

STIGs A to Z

Download	Date	Size	Format
A10 Networks Application Delivery Controller (ADC) ALG STIG Version 1	4/27/2016	267 KB	ZIP
A10 Networks Application Delivery Controller (ADC) NDM STIG Version 1	4/27/2016	270 KB	ZIP
A10 Networks Application Delivery Controller (ADC) Overview, Version 1	4/27/2016	87 KB	ZIP
Active Directory Domain STIG - Ver 2, Rel 8	1/27/2017	456 KB	ZIP
Active Directory Forest STIG - Ver 2, Rel 7	1/27/2017	1.58 MB	ZIP
Adobe Acrobat Reader DC Classic Track STIG - Version 1, Release 1	2/5/2016	269 KB	ZIP
Adobe Acrobat Reader DC Continuous Track STIG - Ver 1, Rel 2	4/22/2016	526 KB	ZIP
Adobe Acrobat Reader Document Cloud (DC) Classic Track STIG Benchmark - Ver 1, Rel 1 (SCC tool use only)	8/1/2016	12 KB	ZIP
Adobe Acrobat Reader Document Cloud (DC) Continuous Track STIG Benchmark - Ver 1, Rel 2 (SCC tool use only)	7/25/2016	11.5 KB	ZIP
Adobe Coldfusion 11 STIG - Ver 1, Rel 2	10/28/2016	324 KB	ZIP
AIMS4 STIG - Version 4, Release 40	1/27/2017	1.28 MB	ZIP

STIGs Related Links

[+ STIGs Home](#)

[Cloud Computing Security](#)

[Control Correlation Identifier \(CCI\)](#)

[DoD Annex for NIAP Protection Profiles](#)

[FAQs](#)

[Quarterly Release Schedule and Summary](#)

[+ SRG/STIG Tools](#)

[SRG-STIG Library Compilations](#)

[STIG Mailing List](#)

[STIGs Master List \(A to Z\)](#)

[+ STIGs Technologies](#)

[Vendor Process](#)

[Contact Us](#)

A Look At DISA STIGs (1)

STIGs Viewer

Support Environment

Home Cybersecurity Training ▼ Topic Map ▼ **STIGs ▼** Tools ▼ News Help RSS Feeds

Home > STIGs > STIGs A-Z

STIGs Master List (A to Z)

*PKI = DoD PKI Certificate Required

STIGs A to Z

Download

A10 Networks Application Delivery Controller (ADC) A				
A10 Networks Application Delivery Controller (ADC) M				
A10 Networks Application Delivery Controller (ADC) C				
Active Directory Domain STIG - Ver 2, Rel 8				
Active Directory Forest STIG - Ver 2, Rel 7				
Adobe Acrobat Reader DC Classic Track STIG - Versi				
Adobe Acrobat Reader DC Continuous Track STIG - Ver 1, Rel 2	4/22/2016	526 KB	ZIP	
Adobe Acrobat Reader Document Cloud (DC) Classic Track STIG Benchmark - Ver 1, Rel 1 (SCC tool use only)	8/1/2016	12 KB	ZIP	
Adobe Acrobat Reader Document Cloud (DC) Continous Track STIG Benchmark - Ver 1, Rel 2 (SCC tool use only)	7/25/2016	11.5 KB	ZIP	

- STIGs Home
- Control Correlation Identifier (CCI)
- DoD Annex for NIAP Protection Profiles
- FAQs
- Quarterly Release Schedule and Summary
- SRG/STIG Tools
 - SRG-STIG Library Compilations
 - STIG Mailing List
 - STIGs Master List (A to Z)
- STIGs Technologies
 - Vendor Process
 - Contact Us

STIG Viewing Guidance

SRG/STIG Applicability Guide and Col

STIG Viewing Guidance

STIGs Related

- + STIGs Home
- Cloud Computi
- Control Correla (CCI)
- Quarterly Relea Summary
- + SRG/STIG T
- SRG-STIG Libr
- STIG Mailing L
- STIGs Master L
- + STIGs Techn
- Vendor Proces

A Look At DISA STIGs (1)

STIG Viewer Download

STIG Viewing Guidance

*PKI = DoD PKI Certificate Required

XCCDF formatted SRGs and STIGs are intended be ingested into an SCAP validated tool for use in validating compliance of a Target of Evaluation (TOE). As such, getting to the content of a XCCDF formatted STIG to read and understand the content is not as easy as opening a .doc or .pdf file and reading it. The process can be a little confusing and trying. Below are tools which can be used to view the STIGs and a Whitepaper describing the STIG Viewing processes.

How to View SRGs and STIGs

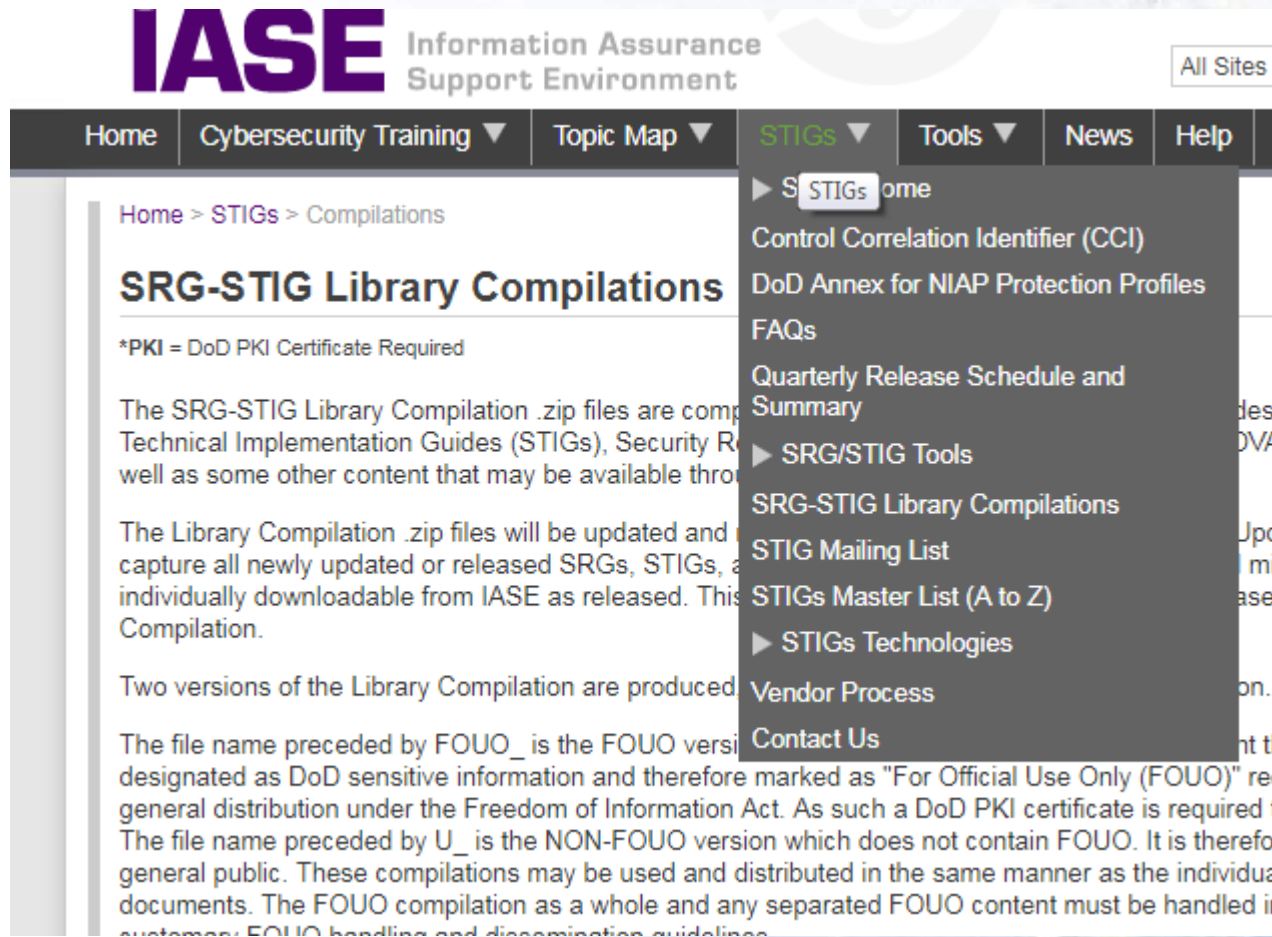
Download	Date	Size	Format
How to View SRGs and STIGs	8/29/2016	80 KB	DOCX

STIG Viewer

Download	Date	Size	Format
STIG Viewer 2.x User Guide	3/21/2017	993 KB	PDF
STIG Viewer Version 2.5.4	6/23/2017	780 KB	ZIP
STIG Viewer Version 2.5.4 Hashes	5/4/2017	1 KB	TXT

A Look At DISA STIGs (1)

STIG Library Compilation



IASE Information Assurance Support Environment

All Sites

Home Cybersecurity Training ▼ Topic Map ▼ **STIGs ▼** Tools ▼ News Help

Home > STIGs > Compilations

SRG-STIG Library Compilations

*PKI = DoD PKI Certificate Required

The SRG-STIG Library Compilation .zip files are compiled from Technical Implementation Guides (STIGs), Security Requirements (SRGs), and other content that may be available through the IASE website.

The Library Compilation .zip files will be updated and released to capture all newly updated or released SRGs, STIGs, and other content individually downloadable from IASE as released. This is a continuous compilation.

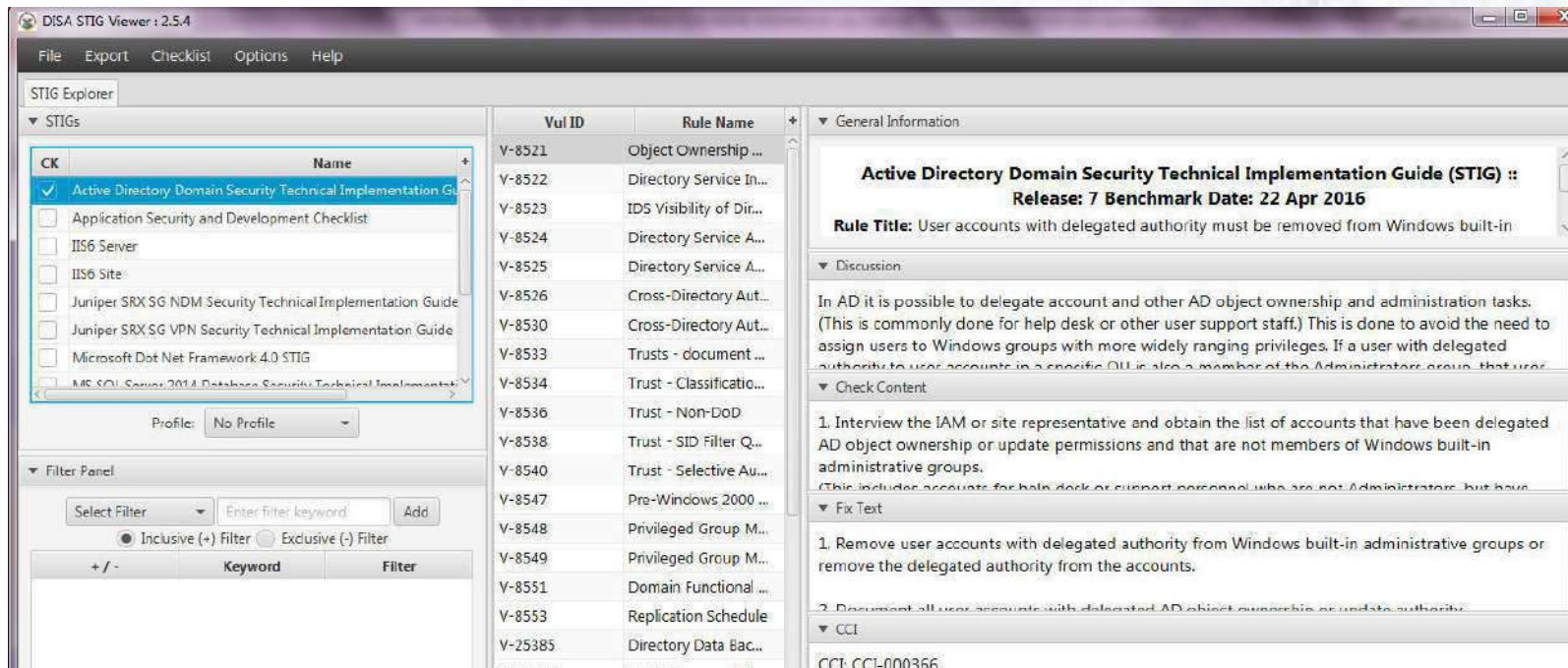
Two versions of the Library Compilation are produced: a FOUO version and a public version.

The file name preceded by FOUO_ is the FOUO version, which is designated as DoD sensitive information and therefore marked as "For Official Use Only (FOUO)" requiring general distribution under the Freedom of Information Act. As such a DoD PKI certificate is required to access this content. The file name preceded by U_ is the NON-FOUO version which does not contain FOUO. It is therefore available to the general public. These compilations may be used and distributed in the same manner as the individual documents. The FOUO compilation as a whole and any separated FOUO content must be handled in accordance with DoD FOUO handling and dissemination guidelines.

- STIGs Home
- Control Correlation Identifier (CCI)
- DoD Annex for NIAP Protection Profiles
- FAQs
- Quarterly Release Schedule and Summary
- SRG/STIG Tools
- SRG-STIG Library Compilations
- STIG Mailing List
- STIGs Master List (A to Z)
- STIGs Technologies
- Vendor Process
- Contact Us

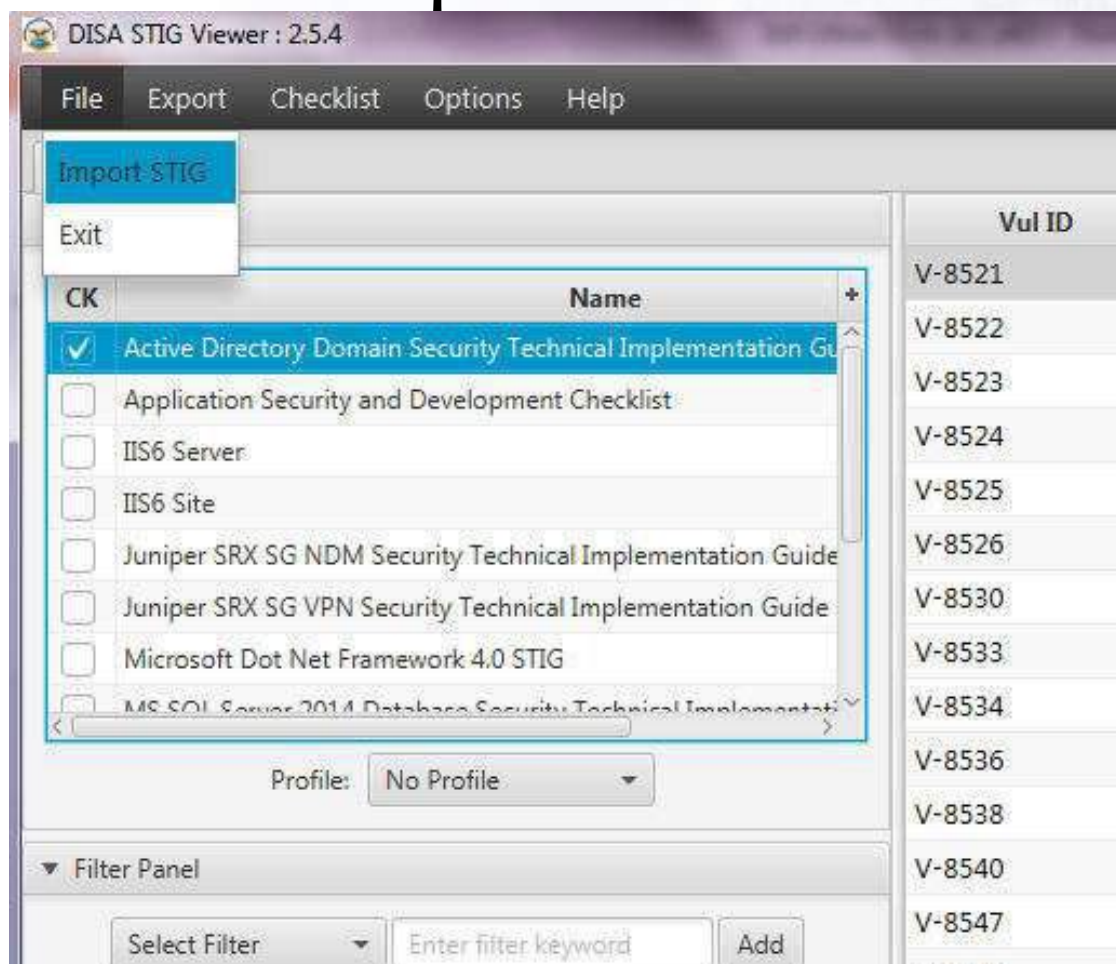
A Look At DISA STIGs (1)

STIG Viewer Window



A Look At DISA STIGs (1)

Import STIG



A Look At DISA STIGs (1)

- Completely different mechanism for DISA STIGs

END

A Look At DISA STIGs (2)

- STIG content:
 - General information (title)
 - Discussion
 - Check content
 - Fix text
 - CCI (References)

A Look At DISA STIGs (2)

SEVERITY	DISA CATEGORY CODE GUIDELINES
CAT 1	Any vulnerability, the exploitation of which will directly and immediately result in loss of Confidentiality, Availability, or Integrity.
CAT 2	Any vulnerability, the exploitation of which has a potential to result in loss of Confidentiality, Availability, or Integrity.
CAT 3	Any vulnerability, the existence of which degrades measures to protect against loss of Confidentiality, Availability, or Integrity

A Look At DISA STIGs (2)

FILTER PANEL

Filter Panel

CATI

Keyword

Rule Title

STIG ID

Vulnerability ID

Rule ID

IA Control

CATI

CAT II

CAT III

CCI

CATI

Filter ☐ Exclusive (-) Filter

Add

Keyword	Filter
content in table	

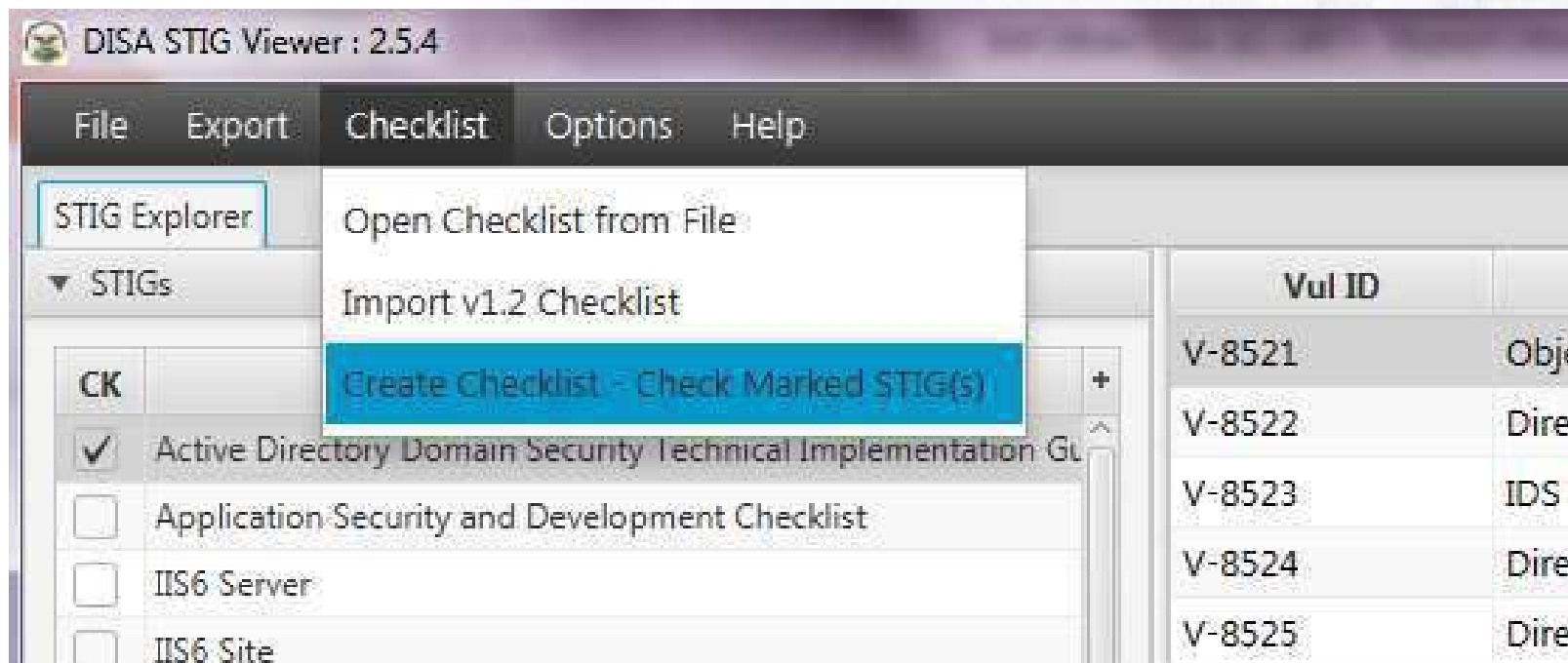
Remove Filter(s)

Remove All Filters

FILTER PANEL
CREATE
CHECK LIST
CHECK LIST

A Look At DISA STIGs (2)

CREATE CHECKLIST



A Look At DISA STIGs (2)

CHECKLIST

The screenshot displays the DISA STIG Viewer 2.5.4 application interface. The main window is titled "DISA STIG Viewer : 2.5.4" and features a menu bar with "File", "Import", and "Export". The "STIG Explorer" tab is active, showing a tree view of STIGs. The "Checklist X" tab is selected, displaying a table of security rules.

Totals

Overall Totals	CAT I	CAT II	CAT III
Opens:	0	Not Reviewed:	42
Not a Finding:	0	Not Applicable:	0

Target Data

Computing

Host Name:

IP Address:

MAC Address:

Fully Qualified Domain Name:

Get Host Data

Role

☒ None

☐ Workstation

☐ Member Server

☐ Domain Controller

☐ Web or Database STIG

STIGs

Name
Active Directory Domain Security Technical Implementation Guide (STIG)

Showing rule 1 out of 42

General Information

Active Directory Domain Security Technical Implementation Guide (STIG) ::
Release: 7 Benchmark Date: 22 Apr 2016

Rule Title: User accounts with delegated authority must be removed from Windows built-in administrative groups or remove the delegated authority from the accounts.

Status: ☒ Not Reviewed ☐ Open ☐ Not a Finding ☐ Not Applicable

Vuln Information

Discussion ☒ Check Content ☐ Fix Text ☐ CCI ☐ Misc

In AD it is possible to delegate account and other AD object ownership and administration tasks. (This is commonly done for help desk or other user support staff.) This is done to avoid the need to assign users to Windows groups with more widely ranging privileges. If a user with delegated authority to user accounts in a specific OU is also a member of the Administrators group, that user has the ability to reconfigure a wide range of domain security settings and change user accounts

Finding Details

Comments

A Look At DISA STIGs (2)

- Checklist screens:
 - Overall totals
 - Target data
 - Role
 - Finding details
 - Comments

A Look At DISA STIGs (2)

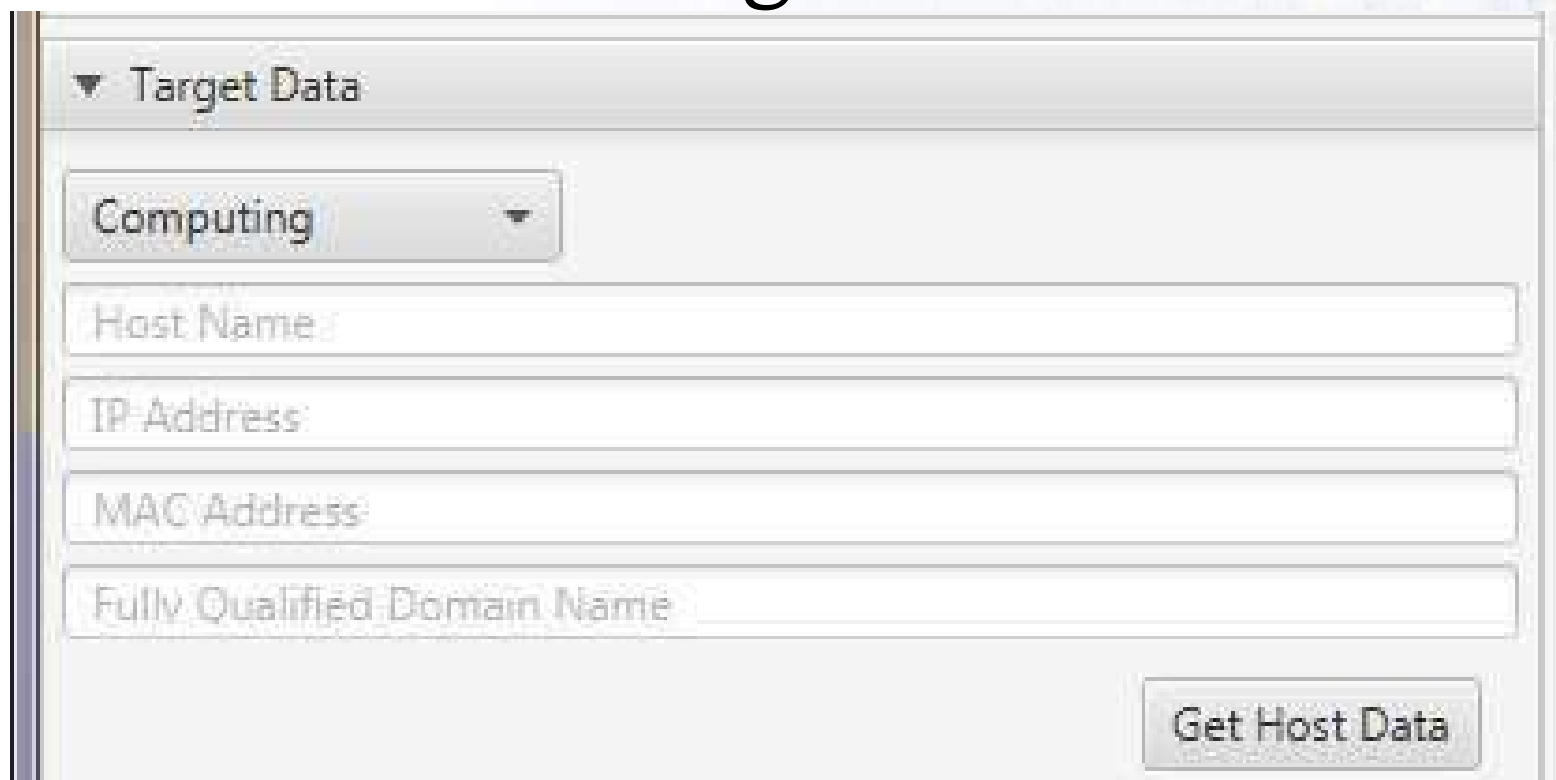
- Checklist screens (STATUS):
 - Not reviewed
 - Open
 - Not a finding
 - Not applicable

Totals

2

A Look At DISA STIGs (2)

Target Data



The screenshot shows a software interface for entering target data. It features a title bar with a dropdown arrow and the text "Target Data". Below the title bar is a dropdown menu currently set to "Computing". Underneath the menu are four text input fields, each with a label: "Host Name", "IP Address", "MAC Address", and "Fully Qualified Domain Name". At the bottom right of the form is a button labeled "Get Host Data".

▼ Target Data

Computing ▼

Host Name

IP Address

MAC Address

Fully Qualified Domain Name

Get Host Data

A Look At DISA STIGs (2)

Status

▼ General Information

**Active Directory Domain Security Technical Implementation Guide (STIG) ::
Release: 7 Benchmark Date: 22 Apr 2016**

Rule Title: User accounts with delegated authority must be removed from Windows built-in administrative groups or remove the delegated authority from the accounts.

Status: ☐ Not Reviewed ☒ Open ☐ Not a Finding ☐ Not Applicable

Severity Override ▼

A Look At DISA STIGs (2)

Vuln Information

Review of Hostin...

Status: ☐ Not Reviewed ☒ Open ☐ Not a Finding ☐ Not Applicable Severity Override ▾

▼ Vuln Information

Discussion Check Content Fix Text CCI Misc

In AD it is possible to delegate account and other AD object ownership and administration tasks. (This is commonly done for help desk or other user support staff.) This is done to avoid the need to assign users to Windows groups with more widely ranging privileges. If a user with delegated authority to user accounts in a specific OU is also a member of the Administrators group, that user

A Look At DISA STIGs (2)

- In the next module lets look at further details

END

A Look At DISA STIGs (3)

- Windows Server 2012 R2 Member Server
 - Import STIG
 - V1099 (Lockout duration)

A Look At DISA STIGs (2)

STIG Explorer

File Export Checklist Options Help

▼ STIGs

CK	Name
☐	MS SQL Server 2014 Database Security Technical Implementation Guide
☐	Firewall Security Technical Implementation Guide - Cisco
☐	Firewall Security Technical Implementation Guide
☐	SharePoint 2010 Security Technical Implementation Guide (STIG)
☐	Windows Server 2008 R2 Member Server Security Technical Implementation Guide
☐	Layer 2 Switch Security Technical Implementation Guide - Cisco
☐	Layer 2 Switch Security Technical Implementation Guide
☒	Windows Server 2012/2012 R2 Member Server Security Technical Implementation Guide

Profile: No Profile

▼ Filter Panel

CAT I CAT I Add

☒ Inclusive (+) Filter ☐ Exclusive (-) Filter

+ / - Keyword Filter

Vul ID ▲	Rule Name
V-1070	Physical security
V-1072	Shared User Accounts
V-1073	Unsupported Service Packs
V-1074	WIN00-000100
V-1075	Display Shutdown Button
V-1076	System Recovery Backups
V-1081	NTFS Requirement
V-1089	Legal Notice Display
V-1090	Caching of logon credentials
V-1093	Anonymous shares are not restricted
V-1097	Bad Logon Attempts
V-1098	Bad Logon Counter Reset
V-1099	Lockout Duration
V-1102	User Right - Act as part of OS
V-1104	Maximum Password Age

A Look At DISA STIGs (2)

Vul ID ▲	Rule Name	+	▼ General Information
V-1070	Physical security		
V-1072	Shared User Accounts		
V-1073	Unsupported Service Packs		
V-1074	WIN00-000100		
V-1075	Display Shutdown Button		
V-1076	System Recovery Backups		
V-1081	NTFS Requirement		
V-1089	Legal Notice Display		
V-1090	Caching of logon credentials		
V-1093	Anonymous shares are not restricted		
V-1097	Bad Logon Attempts		
V-1098	Bad Logon Counter Reset		
V-1099	Lockout Duration		Windows Server 2012/2012 R2 Member Server Security Technical Implementation Guide :: Release: 8 Benchmark Date: 28 Apr 2017 Rule Title: The lockout duration must be configured to require an
V-1102	User Right - Act as part of OS		▼ Discussion
V-1104	Maximum Password Age		The account lockout feature, when enabled, prevents brute-force password attacks on the system. This parameter specifies the period of time that an account will remain locked after the specified number of failed logon attempts. A value of 0 will require an administrator to unlock the account.
V-1105	Minimum Password Age		▼ Check Content
V-1107	Password Uniqueness		Verify the effective setting in Local Group Policy Editor. Run "gpedit.msc".
V-1112	Dormant Accounts		Navigate to Local Computer Policy -> Computer Configuration -> Windows Settings -> Security Settings -> Account Policies -> Account
V-1113	Disable Guest Account		▼ Fix Text
V-1114	Rename Built-in Guest Account		Configure the policy value for Computer Configuration -> Windows Settings -> Security Settings -> Account Policies -> Account Lockout Policy -> "Account lockout duration" to "0" minutes, "Account is locked out until administrator unlocks it".
V-1115	Rename Built-in Administrator Account		▼ CCI

A Look At DISA STIGs (3)

- Rule Title:
 - The lockout duration must be configured to require an administrator to unlock an account
 - Severity: CAT II

A Look At DISA STIGs (3)

- Discussion:
 - The account lockout feature, when enabled, prevents brute-force password attacks on the system. This parameter specifies the period of time that an account will remain locked after the specified number

A Look At DISA STIGs (3)

- Discussion...:
 - of failed logon attempts. A value of 0 will require an administrator to unlock the account.

A Look At DISA STIGs (3)

- Check Content:
 - Verify the effective setting in Local Group Policy Editor.
Run "gpedit.msc".

A Look At DISA STIGs (3)

- Check Content:
 - Navigate to Local Computer Policy -> Computer Configuration -> Windows Settings -> Security Settings -> Account Policies -> Account Lockout Policy.

A Look At DISA STIGs (3)

- Check Content...:
 - If the "Account lockout duration" is not set to "0", requiring an administrator to unlock the account, this is a finding.

A Look At DISA STIGs (3)

- Fix Text:
 - Configure the policy value for Computer Configuration -> Windows Settings -> Security Settings -> Account Policies -> Account Lockout Policy -> "Account lockout duration" to "0" minutes,

A Look At DISA STIGs (3)

- Fix Text....:
 - "Account is locked out until administrator unlocks it".
- CCI: NIST SP 800-53
Revision 4 :: AC-7 b

END

A Look At DISA STIGs (4)

- Firewall Security
Technical
Implementation Guide
- Vulnerability ID: V-3967
- Rule name: The console
port does not timeout
after 10 mins

A Look At DISA STIGs (4)

STIGVIEWER WINDOW

DISA STIG Viewer: 2.5.4

File Export Checklist Options Help

STIG Explorer

STIGs

CK	Name
☐	Firewall Security Technical Implementation Guide
☐	Layer 2 Switch Security Technical Implementation Guide - Cisco
☐	Layer 2 Switch Security Technical Implementation Guide
☐	SharePoint 2010 Security Technical Implementation Guide (STIG)
☐	Windows Server 2008 R2 Member Server Security Technical Im
☐	Windows Server 2012/2012 R2 Member Server Security Techni
☐	Firewall Security Technical Implementation Guide - Cisco
☒	Firewall Security Technical Implementation Guide

Profile: No Profile

Filter Panel

Select Filter Enter filter keyword Add

☒ Inclusive (+) Filter ☐ Exclusive (-) Filter

Keyword	Filter

No content in table

Remove Filter(s) Remove All Filters

Rule ID	Rule Name
V-3966	More than one local account is defined.
V-3967	The console port does not timeout after 10 minutes.
V-3969	Network element must only allow SNMP read access.
V-3982	L2TP is terminated in the private network.
V-4582	Authentication required for console access.
V-4619	Firewall is not operating on a STIG'd OS
V-5611	Management connections are not restricted.
V-5612	SSH session timeout is not 60 seconds or less.
V-5613	SSH login attempts value is greater than 3.
V-5646	Devices not configured to filter and drop half-open conn...
V-5731	Perimeter is not compliant with DOD Instr. 8551.1
V-7011	The auxiliary port is not disabled.
V-14637	IPv6 Router Advertisements must be suppressed.
V-14643	Firewall inspection is not performed adequately
V-14644	Firewall must block loopback address
V-14646	Alerts generated at 75% log storage capacity.
V-14647	No FW log dump procedures
V-14648	FA is not informed of critical alerts.
V-14649	FW alert not written to remote console.
V-14653	Audit record must display violation
V-14655	Alerts must remain until acknowledged.
V-14656	FW acknowledge messages must be recorded
V-14667	Key expiration exceeds 180 days.
V-14671	NTP messages are not authenticated

Showing rule 20 out of 73

General Information

Firewall Security Technical Implementation Guide ::
Release: 22 Benchmark Date: 28 Apr 2017

Rule Title: The network devices must time out access to the console port at 10 minutes or less of inactivity.

STIG ID: NET1624

Discussion

Terminating an idle session within a short time period reduces the window of opportunity for unauthorized personnel to take control of a management session enabled on the console or console port that has been left unattended. In addition quickly terminating an idle session will also free up resources committed by the managed network device. Setting the timeout of the session to 10 minutes or less increases the

Check Content

Review the configuration and verify a session using the console port will time out after 10 minutes or less of inactivity.

If console access is not configured to timeout at 10 minutes or less, this is a finding.

Fix Text

Configure the timeout for idle console connection to 10 minutes or less.

A Look At DISA STIGs (4)

- General Information:
 - **Rule Title:** The network devices must time out access to the console port at 10 minutes or less of inactivity
 - **STIG ID:** NET1624
 - **Severity:** CAT II

A Look At DISA STIGs (4)

- Discussion:
 - Terminating an idle session within a short time period reduces the window of opportunity for unauthorized personnel to take control of a management session enabled on the console or console...

A Look At DISA STIGs (4)

- Discussion...:
 - port that has been left unattended. In addition quickly terminating an idle session will also free up resources committed by the managed network device. Setting the timeout of the session to 10 minutes

A Look At DISA STIGs (4)

- Discussion...:
 - or less increases the level of protection afforded critical network components

A Look At DISA STIGs (4)

- Check Content:
 - Review the configuration and verify a session using the console port will time out after 10 mins or less of inactivity.
 - If console access is not configured to timeout at 10 minutes or less, this is a finding.

A Look At DISA STIGs (4)

- Fix Text:
 - Configure the timeout for idle console connection to 10 minutes or less.

END

Comparison of CIS Vs DISA

- Many controls are common
- Approaches are different
- Organization styles are different

Comparison of CIS Vs DISA

FEATURE	CIS	DISA
CONTROL COVERAGE	GOOD	EXCELLENT
ORG SUITABILITY	SMALL AND MEDIUM ORGS	LARGE ORGS
USER FRIENDLINESS	GOOD	SATISFACTORY
UNUSABLE TERMINOLOGY	NO	YES
CONTROL DETAIL	GOOD	SATISFACTORY
TOOLS	CAT (COMMERCIAL)	SCAP (MILITARY USE)

Comparison of CIS Vs DISA

FEATURE	CIS	DISA
CONTROL PRIORITIZATION	LEVEL 1, LEVEL 2	CAT I - CAT III
TRACKING EASE	CAT TOOL (COMMERCIAL)	FREE STIG VIEWER (CHECKLIST)
FREQUENCY OF UPDATES	FAIR	QUARTERLY
INDUSTRY CREDIBILITY	HIGH	VERY HIGH
INDUSTRY ADOPTION	HIGH	MODERATE

Comparison of CIS Vs DISA

- How to select CIS/DISA:
 - Size of organization
 - IT infrastructure extent
 - Nature of business
 - Security program goals
 - Maturity of IT & security staff

Comparison of CIS Vs DISA

- Rule of thumb:
 - Smaller orgs use CIS
 - Larger orgs use DISA
 - CIS is part of Homeland Security, DISA is part of US Military
 - DISA more frequently updated and maintained with wider coverage

END

Security Hardening – Windows Server 2012R2

- Windows Server 2012 – R2
- DISA, Release 8
 - 28 April 2017
- Domain Controller

Security Hardening – Windows Server 2012 R2

STIGVIEWER WINDOW

The screenshot displays the DISA STIG Viewer 2.5.4 application. The interface includes a menu bar (File, Export, Checklist, Options, Help) and a toolbar. The main window is divided into several panes:

- STIG Explorer:** A tree view on the left showing a list of STIGs. The selected STIG is "Windows Server 2012/2012 R2 Domain Controller Security Technical Implementation Guide".
- Filter Panel:** A panel below the STIG Explorer with a dropdown menu set to "CAT I", an "Add" button, and radio buttons for "Inclusive (+) Filter" and "Exclusive (-) Filter". Below this is a table with columns for "+ / -", "Keyword", and "Filter".
- Table:** A central table listing security rules with columns "Vul ID" and "Rule Name".
- General Information:** A pane on the right showing details for the selected rule (V-2374).
- Discussion:** A pane on the right providing a detailed description of the rule's purpose and potential findings.
- Check Content:** A pane on the right showing the specific configuration requirements for the rule.

Vul ID	Rule Name
V-1073	Unsupported Service Packs
V-1074	WIN00-000100
V-1081	NTFS Requirement
V-1093	Anonymous shares are not restricted
V-1102	User Right - Act as part of OS
V-1121	FTP System File Access
V-1127	Restricted Administrator Group Me...
V-1152	Anonymous Access to the Registry
V-1153	LanMan Authentication Level
V-2372	Reversible Password Encryption
V-2374	Disable Media Autoplay
V-3337	Anonymous SID/Name Translation
V-3338	Anonymous Access to Named Pipes
V-3339	Remotely Accessible Registry Paths
V-3340	Anonymous Access to Network Sha...
V-3343	Remote Assistance - Solicit Remote ...
V-3344	Limit Blank Passwords
V-3379	LAN Manager Hash stored

General Information:

- Rule Title:** Autoplay must be disabled for all drives.
- STIG ID:** WN12-CC-000074
- Rule ID:** SV-52879r2_rule
- Vuln ID:** V-2374
- Severity:** CAT I
- Class:** Unclass

Discussion:

Allowing Autoplay to execute may introduce malicious code to a system. Autoplay begins reading from a drive as soon media is inserted into the drive. As a result, the setup file of programs or music on audio media may start. By default, Autoplay is disabled on removable drives, such as the floppy disk drive (but not the CD-ROM drive) and on...

Check Content:

If the following registry value does not exist or is not configured as specified, this is a finding:

Registry Hive: HKEY_LOCAL_MACHINE
Registry Path:

Fix Text:

Configure the policy value for Computer Configuration -> Administrative Templates -> Windows Components -> AutoPlay Policies -> "Turn off Autoplay" to "Enabled: All Drives"

Security Hardening – Windows Server 2012R2

- General Information:
 - **Rule Title:** Autoplay must be disabled for all drives
 - **STIG ID:** WN12-CC-000074
 - **Severity:** CAT I

Security Hardening – Windows Server 2012R2

- Discussion:
 - Allowing Autoplay to execute may introduce malicious code to a system. Autoplay begins reading from a drive as soon media is inserted into the drive. As a result, the setup file of programs or

Security Hardening – Windows Server 2012R2

- Discussion...:
 - music on audio media may start. By default, Autoplay is disabled on removable drives, such as the floppy disk drive (but not the CD-ROM drive) and on network drives.

Security Hardening – Windows Server 2012R2

- Discussion...:
 - Enabling this policy disables Autoplay on all drives....

Security Hardening – Windows Server 2012R2

- Check Content:
 - If the following registry value does not exist or is not configured as specified, this is a finding:
 - Registry Hive:
HKEY_LOCAL_MACHINE

Security Hardening – Windows Server 2012R2

- Check Content:
 - Registry Path:
\\SOFTWARE\\Microsoft\\Windows\\CurrentVersion\\policies\\Explorer\\
 - Value Name:
NoDriveTypeAutoRun
 - Type: REG_DWORD
Value: 0x000000ff
(255)

Security Hardening – Windows Server 2012R2

- Fix Text:
 - Configure the policy value for Computer Configuration -> Administrative Templates -> Windows Components -> AutoPlay Policies -> "Turn off AutoPlay" to "Enabled:All Drives".

Security Hardening – Windows Server 2012R2

- CCI (Control Correlation Identifier):
 - CCI: CCI-001764
The information system prevents program execution in accordance with organization-defined policies regarding software program usage and restrictions...

Security Hardening – Windows Server 2012R2

- CCI (Control Correlation Identifier):
 - ... and/or rules authorizing the terms and conditions of software program usage.
NIST SP 800-53
Revision 4 :: CM-7 (2)

END

Case Study Security Hardening – Linux

- CIS Benchmarks case study (Red Hat Enterprise Linux 7)

Case Study Security Hardening – Linux

CIS Red Hat Enterprise Linux 7 Benchmark

v2.1.1 - 01-31-2017

- January 31, 2017
- 347 pages PDF doc

Case Study Security Hardening – Linux

SSH stands for Secure Shell and is also known as Secure Socket Shell. SSH is a secure network communication protocol.

- 5.2.2 (page 258); *Ensure SSH Protocol is set to 2 (Scored)*
- Profile applicability:
 - Level 1, Server
 - Level 1, Workstation

Case Study Security Hardening – Linux

- 5.2.2 (page 258); *Ensure SSH Protocol is set to 2* (Scored)
 - Description: SSH supports 2 different and incompatible protocols: SSH1 and SSH2. SSH1 was the original protocol & was subject to security issues. SSH2 is more advanced and secure.

Case Study Security Hardening – Linux

- 5.2.2 (page 258); *Ensure SSH Protocol is set to 2 (Scored)*
 - Rationale: SSH v1 suffers from insecurities that do not affect SSH v2.

Case Study Security Hardening – Linux

- 5.2.2 (page 258); *Ensure SSH Protocol is set to 2* (Scored)
 - Audit: Run the following command and verify that output matches:

```
# grep "^Protocol"  
/etc/ssh/sshd_config  
Protocol 2
```

Case Study Security Hardening – Linux

- 5.2.2 (page 258); *Ensure SSH Protocol is set to 2 (Scored)*
 - Remediation: Edit the `/etc/ssh/sshd_config` file to set the parameter as follows:

Protocol 2

Case Study Security Hardening – Linux

- 5.2.2 (page 258); *Ensure SSH Protocol is set to 2 (Scored)*
 - Critical Controls: 3.4
Use Only Secure
Channels For Remote
System
Administration

Case Study Security Hardening – Linux

- Critical Controls: 3.4
Perform all remote administration of servers, workstation, network devices, and similar equipment over secure channels. Protocols such as telnet, VNC, RDP, or others that do not actively support strong encryption

Case Study - Security Hardening – Linux

- ... should only be used if they are performed over a secondary encryption channel, such as SSL, TLS or IPSEC.

Security Hardening – Case Study – Solaris

- Solaris 10 X86
- DISA, Release 18
 - 28 April 2017

Security Hardening – Case Study – Solaris

STIGVIEWER WINDOW

The screenshot displays the DISA STIG Viewer 2.5.4 application. The interface includes a menu bar (File, Export, Checklist, Options, Help) and a toolbar. The main window is divided into several panes:

- STIG Explorer:** A tree view on the left showing a list of STIGs. The "SOLARIS 10 X86 SECURITY TECHNICAL IMPLEMENTATION GUIDE" is selected and highlighted in blue.
- Table:** A central table listing rules with columns for "Vul ID" and "Rule Name".
- General Information:** A pane on the right showing details for the selected STIG, including the title "SOLARIS 10 X86 SECURITY TECHNICAL IMPLEMENTATION GUIDE :: Release: 18 Benchmark" and the date "Date: 28 Apr 2017".
- Discussion:** A section providing context for the rules, such as "If an account is configured for password authentication but does not have an assigned password, it may be possible to log into the account without authentication."
- Check Content:** A section showing the specific content of the rules, such as "Verify no accounts have blank passwords." and "# logins -p".
- Fix Text:** A section showing the remediation steps, such as "Remove, lock, or configure a password for any account with a blank password."

Vul ID	Rule Name
V-770	GEN000560
V-847	GEN005080
V-848	GEN005100
V-910	GEN001640
V-922	GEN002220
V-993	GEN005300
V-1013	GEN008600
V-1046	GEN001100
V-4247	GEN008640
V-4248	GEN008660
V-4249	GEN008700
V-4255	GEN008680
V-4295	GEN005500
V-4382	GEN004220
V-4387	GEN005000
V-4399	GEN006380
V-4407	GEN000000

Security Hardening – Case Study – Solaris

- General Information:
 - **Rule Title:** All shell files must have mode 0755 or less permissive
 - **STIG ID:** GEN002220
 - **Severity:** CAT I

Security Hardening – Case Study – Solaris

- Discussion:
 - Shells with world/group-write permissions give the ability to maliciously modify the shell to obtain unauthorized access.

Security Hardening – Case Study – Solaris

- Check Content:
 - If /etc/shells exists, check the group ownership of each shell referenced.
`# cat /etc/shells | xargs -n1 ls -lL`
 - Otherwise, check any shells found on the system.
`# find / -name "*sh" | xargs -n1 ls -lL`

Security Hardening – Case Study – Solaris

- ... Check Content:
 - If a shell has a mode more permissive than 0755, this is a finding

Security Hardening – Case Study – Solaris

- Fix Text:
 - Change the mode of the shell
- ```
chmod 0755
<shell>
```

# Security Hardening – Case Study – Solaris

---

- CCI (Control Correlation Identifier):
  - CCI-000225  
The organization employs the concept of least privilege, allowing only authorized accesses for users (and processes acting on behalf of users) which are necessary...

# Security Hardening – Case Study – Solaris

---

- ... CCI (Control Correlation Identifier):
  - ... to accomplish assigned tasks in accordance with organizational missions and business functions



# Security Hardening – Case Study – Solaris

- ... CCI (Control Correlation Identifier):
  - ... NIST SP 800-53 ::  
AC-6  
NIST SP 800-53A ::  
AC-6.1  
NIST SP 800-53  
Revision 4 :: AC-6

# Case Study Security Hardening – Apache

---

- CIS Benchmarks case study (Apache Tomcat 7)

# Case Study Security Hardening – Apache

## CIS Apache Tomcat 7 Benchmark

v1.1.0 - 04-26-2016

- April 26, 2016
- 94 pages PDF doc

# Case Study Security Hardening – Apache

- 7.7 (page 65); Configure *log file size limit* (Scored)
- Profile applicability:
  - Level 2

# Case Study Security Hardening – Apache

- 7.7 (page 65); Configure log file size limit (Scored)
  - Description: By default, the logging.properties file will have no defined limit for the log file size. This is a potential denial of service attack as it would be possible to...



# Case Study Security Hardening – Apache

---

- 7.7 (page 65); Configure *log file size limit* (Scored)
  - Description: ... fill a drive or partition containing the log files

# Case Study Security Hardening – Apache

- 7.7 (page 65); Configure log file size limit (Scored)
  - Rationale:  
Establishing a maximum log size that is smaller than the partition size will help mitigate the risk of an attacker maliciously exhausting disk space

# Case Study Security Hardening – Apache

---

- 7.7 (page 65); Configure log file size limit (Scored)
  - Audit: Validate the max file limit is not greater than the size of the partition where the log files are stored.

# Case Study Security Hardening – Apache

- 7.7 (page 65); Configure log file size limit (Scored)
  - Remediation: Create the following entry in your logging.properties file. This field is specified in bytes:

**java.util.logging.FileHandler.limit=10000**

# Case Study Security Hardening – Apache

---

- 7.7 (page 65); *Configure log file size limit* (Scored)
  - Default Value: **No limit by default**



# Security Hardening – Case Study – Oracle

---

- Oracle Database 12c
- DISA, Release 18
  - 28 April 2017

# Security Hardening – Case Study – Oracle

## STIGVIEWER WINDOW

The screenshot displays the DISA STIG Viewer 2.5.4 application. The interface is divided into several sections:

- STIG Explorer:** A list of STIGs with checkboxes. The "Oracle Database 12c Security Technical Implementation Guide" is selected.
- Filter Panel:** Includes a "CAT I" dropdown, "Add" button, and filter options (Inclusive (+) Filter, Exclusive (-) Filter).
- Table:** A table with columns "Vul ID" and "Rule Name". It lists 20 rules, all with the same rule name "SRG-APP-000516-DB-999900".
- General Information:** Displays the title "Oracle Database 12c Security Technical Implementation Guide :: Release: 7 Benchmark Date: 28 Apr 2017" and the rule title "Audit trail data must be retained for at least one year."
- Discussion:** A text box stating: "Without preservation, a complete discovery of an attack or suspicious activity may not be determined. DBMS audit data also contributes to the complete investigation of unauthorized activity and needs to be included in audit retention plans and procedures."
- Check Content:** A text box stating: "Review and verify the implementation of an audit trail retention policy. Verify that audit data is maintained for a minimum of one year."
- Fix Text:** A text box stating: "Develop, document and implement an audit retention policy and procedures."

| Vul ID  | Rule Name                |
|---------|--------------------------|
| V-61409 | SRG-APP-000516-DB-999900 |
| V-61411 | SRG-APP-000516-DB-999900 |
| V-61413 | SRG-APP-000516-DB-999900 |
| V-61415 | SRG-APP-000516-DB-999900 |
| V-61417 | SRG-APP-000516-DB-999900 |
| V-61419 | SRG-APP-000516-DB-999900 |
| V-61421 | SRG-APP-000516-DB-999900 |
| V-61425 | SRG-APP-000516-DB-999900 |
| V-61427 | SRG-APP-000516-DB-999900 |
| V-61429 | SRG-APP-000516-DB-999900 |
| V-61431 | SRG-APP-000516-DB-999900 |
| V-61433 | SRG-APP-000516-DB-999900 |
| V-61435 | SRG-APP-000516-DB-999900 |
| V-61437 | SRG-APP-000516-DB-999900 |
| V-61439 | SRG-APP-000516-DB-999900 |
| V-61441 | SRG-APP-000516-DB-999900 |
| V-61443 | SRG-APP-000516-DB-999900 |
| V-61445 | SRG-APP-000516-DB-999900 |

# Security Hardening – Case Study – Oracle

- General Information:
  - **Rule Title:** The Oracle Listener must be configured to require administration authentication
  - **STIG ID:** O121-BP-022700
  - **Severity:** CAT I

# Security Hardening – Case Study – Oracle

---

- Discussion:
  - Oracle listener authentication helps prevent unauthorized administration of the Oracle listener. Unauthorized administration of the listener could lead to DoS exploits;



# Security Hardening – Case Study – Oracle

---

- Discussion...:
  - ...loss of connection audit data, unauthorized reconfiguration or other unauthorized access. This is a Category I finding because privileged access to the listener is not restricted to authorized users.



# Security Hardening – Case Study – Oracle

---

- Discussion...:
  - ... Unauthorized access can result in stopping of the listener (DoS) and overwriting of listener audit logs.

# Security Hardening – Case Study – Oracle

---

- Check Content:
  - If a listener is not running on the local database host server, this check is not a finding

# Security Hardening – Case Study – Oracle

- ... Check Content:
  - For Windows hosts, view all Windows services with TNSListener embedded in the service name
  - The service name format is:  
Oracle[ORACLE\_HOME\_NAME]TNSListener

# Security Hardening – Case Study – Oracle

---

- ... Check Content:
  - View the STIGVIEWER for Unix hosts...

# Security Hardening – Case Study – Oracle

---

- Fix Text:
  - By default, Oracle Net Listener permits only local administration for security reasons. As a policy, the listener can be administered only by the user who started it. This is enforced through local operating system authentication.



# Security Hardening – Case Study – Oracle

---

- Fix Text:
  - For example, if user1 starts the listener, then only user1 can administer it. Any other user trying to administer the listener gets an error. The super user is the only exception.

# Security Hardening – Case Study – Oracle

---

- Fix Text:
  - Remote administ. of the listener must not be permitted. If listener administ. from a remote system is required, granting secure remote access to the Oracle DBMS server and performing local administration is preferred.

# Security Hardening – Case Study – Oracle

---

- CCI (Control Correlation Identifier):
  - CCI: CCI-000366  
The organization implements the security configuration settings.

# Security Hardening – Case Study – Oracle

- ... CCI (Control Correlation Identifier):
  - ... NIST SP 800-53 ::  
CM-6 b  
NIST SP 800-53A ::  
CM-6.1 (iv)  
NIST SP 800-53  
Revision 4 :: CM-6 b

**END**

# Case Study Security Hardening – MS SQL

---

- CIS Benchmarks case study (MS SQL Server 2012)



# Case Study Security Hardening – MS SQL

## CIS Microsoft SQL Server 2012 Benchmark

v1.3.0 - 09-30-2016

- September 30, 2016
- 73 pages PDF doc

# Case Study Security Hardening – MS SQL

---

- 2.14 Ensure 'sa' Login Account has been renamed (Scored)
- Profile applicability:
  - Level 1 database engine

# Case Study Security Hardening – MS SQL

---

- 2.14 Ensure 'sa' Login Account has been renamed (Scored)
  - Description: The sa account is a widely known and often widely used SQL Server account with sysadmin privileges.

# Case Study Security Hardening – MS SQL

---

- 2.14 Ensure 'sa' Login Account has been renamed (Scored)
  - Rationale: It is more difficult to launch password-guessing and brute-force attacks against the sa account if the username is not known.

# Case Study Security Hardening – MS SQL

- 2.14 Ensure 'sa' Login Account has been renamed (Scored)
  - Audit: Use the following syntax to determine if the sa account is renamed:

```
SELECT name
FROM
sys.server_principals
WHERE sid = 0x01;
```



# Case Study Security Hardening – MS SQL

---

- 2.14 Ensure 'sa' Login Account has been renamed (Scored)
  - Audit: ... A name of sa indicates the account has not been renamed

# Case Study Security Hardening – MS SQL

- 2.14 Ensure 'sa' Login Account has been renamed (Scored)
  - Remediation: Replace the different\_user value within the below syntax and execute rename the sa login:

```
ALTER LOGIN sa WITH
NAME =
<different_user>;
```

# Case Study Security Hardening – MS SQL

---

- 2.14 Ensure 'sa' Login Account has been renamed (Scored)
  - Impact: It is not a good security practice to code applications or scripts to use the sa account...

# Case Study Security Hardening – MS SQL

---

- 2.14 Ensure 'sa' Login Account has been renamed (Scored)
  - Impact: ... However, if this has been done renaming the sa account will prevent scripts and applications for authenticating to the database server and executing required tasks or functions.

# Case Study Security Hardening – MS SQL

- 2.14 Ensure 'sa' Login Account has been renamed (Scored)
  - Default Value: By default, the 'sa' account name is 'sa'



# Case Study Security Hardening – MS SQL

- 2.14 Ensure 'sa' Login Account has been renamed (Scored)
  - References:  
[https://msdn.microsoft.com/en-us/library/ms144284\(v=sql.110\).aspx](https://msdn.microsoft.com/en-us/library/ms144284(v=sql.110).aspx)  
(Choose An Authentication Mode)

**END**

# Security Hardening – Case Study – Oracle

---

- Oracle database 11.2g
- DISA, Release 11
  - 28 April 2017

# Security Hardening – Case Study – Oracle

## STIGVIEWER WINDOW

The screenshot shows the DISA STIG Viewer 2.5.4 application. The 'STIG Explorer' pane on the left lists various security guides, with 'Oracle Database 11.2g Security Technical Implementation Guide' selected and checked. The 'Filter Panel' at the bottom left shows 'CAT I' selected. The main pane displays a table of rules with columns 'Vul ID' and 'Rule Name'. The right pane shows 'General Information' for the selected rule, including the title 'Oracle Database 11.2g Security Technical Implementation Guide :: Release: 11 Benchmark Date: 28 Apr 2017' and the rule title 'DBA OS accounts must be granted only those host'. The 'Discussion' section explains the requirement to limit exposure by operating from within a privileged account or role. The 'Check Content' section provides instructions to review host system privileges and includes a note to exclude the Oracle software installation account. The 'Fix Text' section states to revoke all host system privileges from the DBA group accounts and DBA user accounts not required for DBMS administration.

| Vul ID  | Rule Name                |
|---------|--------------------------|
| V-52125 | SRG-APP-000063-DB-000021 |
| V-52133 | SRG-APP-000201-DB-000145 |
| V-52135 | SRG-APP-000220-DB-000149 |
| V-52137 | SRG-APP-000221-DB-000150 |
| V-52141 | SRG-APP-000226-DB-000147 |
| V-52143 | SRG-APP-000231-DB-000154 |
| V-52145 | SRG-APP-000232-DB-000155 |
| V-52147 | SRG-APP-000233-DB-000124 |
| V-52149 | SRG-APP-000234-DB-000157 |
| V-52151 | SRG-APP-000100-DB-000201 |
| V-52153 | SRG-APP-000237-DB-000158 |
| V-52155 | SRG-APP-000101-DB-000044 |
| V-52157 | SRG-APP-000243-DB-000128 |
| V-52159 | SRG-APP-000103-DB-000050 |
| V-52161 | SRG-APP-000245-DB-000132 |
| V-52163 | SRG-APP-000104-DB-000051 |
| V-52165 | SRG-APP-000251-DB-000160 |
| V-52167 | SRG-APP-000108-DB-000048 |

**General Information**

**Oracle Database 11.2g Security Technical Implementation Guide :: Release: 11 Benchmark Date: 28 Apr 2017**

**Rule Title:** DBA OS accounts must be granted only those host

**Discussion**

This requirement is intended to limit exposure due to operating from within a privileged account or role. The inclusion of role is intended to address those situations where an access control policy, such as Role Based Access Control (RBAC), is being implemented and where a change of role provides the same degree of assurance in the change of

**Check Content**

Review host system privileges assigned to the Oracle DBA group and all individual Oracle DBA accounts.

**Note:** Do not include the Oracle software installation account in any results for this check.

**Fix Text**

Revoke all host system privileges from the DBA group accounts and DBA user accounts not required for DBMS administration.

# Security Hardening – Case Study – Oracle

---

- General Information:
  - **Rule Title:** The Oracle REMOTE\_OS\_ROLES parameter must be set to FALSE.
  - **STIG ID:** O112-BP-022000
  - **Severity:** CAT I



# Security Hardening – Case Study – Oracle

---

- Discussion:
  - Setting `REMOTE_OS_ROLES` to `TRUE` allows operating system groups to control Oracle roles. The default value of `FALSE` causes roles to be identified and managed by the database...



# Security Hardening – Case Study – Oracle

- Discussion...:
  - ...If `REMOTE_OS_ROLES` is set to `TRUE`, a remote user could impersonate another operating system user over a network connection.

# Security Hardening – Case Study – Oracle

- Check Content:
  - From SQL\*Plus:  
select value from  
v\$parameter where  
**name =**  
**'remote\_os\_roles';**
  - If the returned value  
is not FALSE or not  
documented in the  
System Security Plan  
as required, this is a  
Finding

# Security Hardening – Case Study – Oracle

- Fix Text:
  - Document remote OS roles in the System Security Plan.
  - If not required, disable use of remote OS roles.
  - From SQL\*Plus:  
**alter system set  
remote\_os\_roles =  
FALSE scope = spfile;**

# Security Hardening – Case Study – Oracle

---

- Fix Text:
  - The above SQL\*Plus command will set the parameter to take effect at next system startup

# Security Hardening – Case Study – Oracle

- CCI (Control Correlation Identifier):

- CCI: CCI-000366

The org implements the security configuration settings.

NIST SP 800-53 :: CM-6 b

NIST SP 800-53A :: CM-6.1 (iv)

NIST SP 800-53  
Revision 4 :: CM-6 b

**END**



# Case Study Security Hardening – Windows 8

---

- CIS Benchmarks case study (Windows 8.1)

# Case Study Security Hardening – Windows 8

## CIS Microsoft Windows 8.1 Workstation Benchmark

v2.2.1 - 01-31-2017

- January 31, 2017
- 891 pages PDF doc

# Case Study Security Hardening – Windows 8

- 18.9.70.3 Ensure 'Automatically send memory dumps for OS-generated error reports' is set to 'Disabled' (Scored)
- Profile applicability:
  - Level 1
  - Level 1 + BitLocker

# Case Study Security Hardening – Windows 8

---

- 18.9.70.3 Ensure 'Automatically send memory dumps for OS-generated error reports' is set to 'Disabled' (Scored)
- Description: This policy setting controls whether memory dumps in support of OS-generated error reports can be sent to..

# Case Study Security Hardening – Windows 8

---

- Description...:  
... Microsoft automatically. This policy does not apply to error reports generated by 3rd-party products, or additional data other than memory dumps.
  - The recommended state for this setting is: Disabled.



# Case Study Security Hardening – Windows 8

---

- Rationale: Memory dumps may contain sensitive information and should not be automatically sent to anyone.

# Case Study Security Hardening – Windows 8

---

- Audit: Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

# Case Study Security Hardening – Windows 8

---

– Audit:

**HKEY\_LOCAL\_MACHINE\SOFTWARE\Policies\Microsoft\Windows\Windows Error**

**Reporting:AutoApproveOSDumps**

# Case Study Security Hardening – Windows 8

---

- Remediation: To establish the recommended configuration via GP, set the following UI path to Disabled:

# Case Study Security Hardening – Windows 8

---

- Remediation:  
Computer  
Configuration\Policies\Administrative  
Templates\Windows  
Components\Windows Error  
Reporting\Automatically send memory  
dumps for OS-  
generated error  
reports



# Case Study Security Hardening – Windows 8

---

- Impact: All memory dumps are uploaded according to the default consent and notification settings

# Case Study Security Hardening – Windows 8

---

- Default Value:  
Enabled. (Any  
memory dumps  
generated for error  
reports by Microsoft  
Windows are  
automatically  
uploaded, without  
notification to the  
user.)

# Case Study Security Hardening – Windows 8

- References:
  - CCE-33927-5
  - Critical Controls:  
13 Data Protection

**END**

# Security Hardening – Case Study – Win 10

---

- Windows 10
- DISA, Release 9
  - 28 April 2017



# Security Hardening – Case Study – Win 10

## STIGVIEWER WINDOW

The screenshot shows the DISA STIG Viewer 2.5.4 application. The interface includes a menu bar (File, Export, Checklist, Options, Help) and a toolbar. The main window is divided into three panes:

- STIG Explorer:** A list of STIGs with checkboxes. The 'Windows 10 Security Technical Implementation Guide' is selected.
- Table:** A table listing rules with columns 'Vul ID' and 'Rule Name'.
- General Information:** A pane showing details for the selected rule, including the title, release date, and a discussion.

| Vul ID  | Rule Name      |
|---------|----------------|
| V-63325 | WN10-CC-000315 |
| V-63335 | WN10-CC-000330 |
| V-63337 | WN10-00-000030 |
| V-63347 | WN10-CC-000345 |
| V-63349 | WN10-00-000040 |
| V-63351 | WN10-00-000045 |
| V-63353 | WN10-00-000050 |
| V-63361 | WN10-00-000070 |
| V-63377 | WN10-00-000100 |
| V-63379 | WN10-EM-000005 |
| V-63429 | WN10-AC-000045 |
| V-63651 | WN10-CC-000155 |
| V-63667 | WN10-CC-000180 |
| V-63671 | WN10-CC-000185 |
| V-63673 | WN10-CC-000190 |

**General Information**

**Windows 10 Security Technical Implementation Guide ::**  
**Release: 9 Benchmark Date: 28 Apr 2017**

**Rule Title:** The Windows Installer Always install with elevated privileges must be disabled.

**Discussion**

Standard user accounts must not be granted elevated privileges. Enable Windows Installer to elevate privileges when installing applications can allow malicious persons and applications to gain full control of a system.

**Check Content**

If the following registry value does not exist or is not configured as specified, this is a finding:

Registry Hive: HKEY\_LOCAL\_MACHINE  
Registry Path: \SOFTWARE\Policies\Microsoft\Windows\Installer\



# Security Hardening – Case Study – Win 10

---

- General Information:
  - **Rule Title:** The antivirus program must be configured to update signature files on a daily basis.
  - **STIG ID:** WN10-00-000046
  - **Severity:** CAT I

# Security Hardening – Case Study – Win 10

---

- Discussion:
  - Virus scan programs are a primary line of defense against the introduction of viruses and malicious code that can destroy data and even render a computer inoperable. Using a virus scan program provides the ability to...

# Security Hardening – Case Study – Win 10

---

- Discussion...:
  - ... detect malicious code before extensive damage occurs. Updated virus scan data files help protect a system, as constantly changing malware is identified by the antivirus software vendors

# Security Hardening – Case Study – Win 10

---

- Check Content:
  - This requirement is NA if McAfee VirusScan Enterprise (VSE) is used. It will be addressed with the corresponding McAfee VSE STIG.
  - Configurations will vary depending on the product.

# Security Hardening – Case Study – Win 10

---

- Fix Text:
  - Configure the antivirus program to update signature files at least daily. Ensure the updates are occurring on timely basis and are not more than a week old.



# Security Hardening – Case Study – Win 10

- CCI (Control Correlation Identifier):

- CCI: 000366

The org implements the security config settings.

NIST SP 800-53 :: CM-6 b

NIST SP 800-53A :: CM-6.1 (iv)

NIST SP 800-53  
Revision 4 :: CM-6

**END**

# Case Study Security Hardening – MS Exchange

- CIS Benchmarks case study (MS Exchange Server 2016)

# Case Study Security Hardening – MS Exchange

## CIS Microsoft Exchange Server 2016

v1.0.0 - 11-16-2015

- November 16, 2015
- 66 pages PDF doc

# Case Study Security Hardening – MS Exchange

- 2.5 Set *'Do not permanently delete items until the database has been backed up'* to *'True'* (Scored)
- Profile applicability:
  - Level 1 - Mailbox Services Security

# Case Study Security Hardening – MS Exchange

- 2.5 Set 'Do not permanently delete items until the database has been backed up' to 'True' (Scored)
  - Description: This setting allows you to ensure that items are not permanently deleted until the database has been backed up.



# Case Study Security Hardening – MS Exchange

- 2.5 Set 'Do not permanently delete items until the database has been backed up' to 'True' (Scored)
  - Rationale: To ensure that accidentally deleted items can be recovered, they should not be permanently deleted until the database is backed up.

# Case Study Security Hardening – MS Exchange

- 2.5 Set 'Do not permanently delete items until the database has been backed up' to 'True' (Scored)
  - Audit: Execute the following cmdlet and ensure **RetainDeletedItemsUntilBackup** is set to 'True':

# Case Study Security Hardening – MS Exchange

- 2.5 Set 'Do not permanently delete items until the database has been backed up' to 'True' (Scored)
  - Audit: ... **Get-MailboxDatabase <Mailbox Database Name> | fl -property RetainDeletedItemsUntilBackup**

# Case Study Security Hardening – MS Exchange

- 2.5 Set 'Do not permanently delete items until the database has been backed up' to 'True' (Scored)
  - Remediation: To implement the recommended state, execute the following PowerShell cmdlet:

# Case Study Security Hardening – MS Exchange

- 2.5 Set 'Do not permanently delete items until the database has been backed up' to 'True' (Scored)
  - Remediation: **Set-MailboxDatabase <Mailbox Database Name> - RetainDeletedItems UntilBackup \$true**



# Case Study Security Hardening – MS Exchange

- 2.5 Set 'Do not permanently delete items until the database has been backed up' to 'True' (Scored)
  - Impact: The impact of enabling this setting should be minimal. More storage space will be required until any pending items are permanently deleted.

# Case Study Security Hardening – MS Exchange

- 2.5 Set *'Do not permanently delete items until the database has been backed up'* to *'True'* (Scored)
  - Default Value: False

**END**

# Security Hardening – Case Study – AD

---

- Active Directory Domain
- DISA, Release 8
  - 27 January, 2017

# Security Hardening – Case Study – AD

## STIGVIEWER WINDOW

The screenshot displays the DISA STIG Viewer 2.5.4 application. The interface includes a menu bar (File, Export, Checklist, Options, Help) and a toolbar. The main window is divided into several panes:

- STIG Explorer:** A tree view on the left showing various STIGs. The "Active Directory Domain Security Technical Implementation Guide" is selected and checked.
- Filter Panel:** Located below the STIG Explorer, it includes a "CAT I" dropdown, a "CAT I" label, an "Add" button, and radio buttons for "Inclusive (+) Filter" and "Exclusive (-) Filter". Below these are fields for "Keyword" and "Filter" with a search icon.
- Table:** A central table listing rules with columns "Vul ID" and "Rule Name".
- General Information:** A pane on the right showing details for the selected STIG.

| Vul ID  | Rule Name                                |
|---------|------------------------------------------|
| V-8521  | Object Ownership Delegation              |
| V-8522  | Directory Service Inter-Enclave VPN...   |
| V-8523  | IDS Visibility of Directory VPN Data ... |
| V-8524  | Directory Service Availability           |
| V-8525  | Directory Service Architecture DR D...   |
| V-8526  | Cross-Directory Authentication INF...    |
| V-8530  | Cross-Directory Authentication Doc...    |
| V-8533  | Trusts - document need                   |
| V-8534  | Trust - Classification Levels            |
| V-8536  | Trust - Non-DoD                          |
| V-8538  | Trust - SID Filter Quarantining          |
| V-8540  | Trust - Selective Authentication         |
| V-8547  | Pre-Windows 2000 Compatible Acc...       |
| V-8548  | AD.0240                                  |
| V-8549  | Privileged Group Membership - Cro...     |
| V-8551  | Domain Functional Level                  |
| V-8553  | Replication Schedule                     |
| V-25385 | Directory Data Backup                    |
| V-25840 | DSRM Password Change Policy              |

**General Information**

**Active Directory Domain Security Technical Implementation Guide (STIG) :: Release: 8 Benchr**  
**Date: 27 Jan 2017**

**Discussion**

In AD it is possible to delegate account and other AD object o and administration tasks. (This is commonly done for help des other user support staff.) This is done to avoid the need to assi to Windows groups with more widely ranging privileges. If a u

**Check Content**

1. Interview the IAM or site representative and obtain the list o accounts that have been delegated AD object ownership or up permissions and that are not members of Windows built-in administrative groups.

**Fix Text**

1. Remove user accounts with delegated authority from Windo in administrative groups or remove the delegated authority fro accounts.

**CCI**

CCI: CCI-000366



# Security Hardening – Case Study – AD

---

- General Information:
  - **Rule Title :**  
Membership to the Domain Admins group must be restricted to accounts used only to manage the Active Dir domain and domain controllers



# Security Hardening – Case Study – AD

---

- General Information:
  - **STIG ID:** AD.0002
  - **Severity:** CAT I

# Security Hardening – Case Study – AD

---

- Discussion:
  - The Domain Admins group is a highly privileged group. Personnel who are system administrators must log on to Active Directory systems only using accounts with the level of authority necessary.

# Security Hardening – Case Study – AD

---

- Discussion:
  - ... Only system administrator accounts used exclusively to manage an Active Directory domain and domain controllers may be members of the Domain Admins group. A separation of administrator...

# Security Hardening – Case Study – AD

---

- Discussion:
  - ...responsibilities helps mitigate the risk of privilege escalation resulting from credential theft attacks.

# Security Hardening – Case Study – AD

---

- Check Content:
  - Review the Domain Admins group in Active Directory Users and Computers. Each Domain Administrator must have a separate unique account specifically for...



# Security Hardening – Case Study – AD

---

- ... Check Content:
  - ... managing the Active Directory domain and domain controllers.
  - If any account listed in the Domain Admins group is a member of other administrator groups including the

# Security Hardening – Case Study – AD

---

- ... Check Content:
  - ... Enterprise Admins group, domain member server administrators groups, or domain workstation administrators groups, this is a finding.

# Security Hardening – Case Study – AD

---

- Fix Text:
  - Create the necessary documentation that identifies the members of the Domain Admins group. Ensure that each member has a separate unique account that can only be used to manage the Active Directory...

# Security Hardening – Case Study – AD

---

- Fix Text:
  - ... domain and domain controllers. Remove any Domain Admin accounts from other administrator groups.

# Security Hardening – Case Study – AD

- CCI (Control Correlation Identifier):
  - CCI-000366  
The organization implements the security configuration settings.  
NIST SP 800-53 :: CM-6 b  
NIST SP 800-53A :: CM-6.1 (iv)  
NIST SP 800-53  
Revision 4 :: CM-6 b

END



# Case Study Security Hardening – IE Browser

---

- CIS Benchmarks case study (MS Internet Explorer 11)

# Case Study Security Hardening – IE Browser

## CIS Microsoft Internet Explorer 11

v1.0.0 - 12-01-2014

- January 12, 2014
- 178 pages PDF doc

# Case Study Security Hardening – IE Browser

---

- 1.5 Configure 'Do not allow users to enable or disable add-ons' (Not Scored)
- Profile applicability:
  - Level 1

# Case Study Security Hardening – IE Browser

---

- 1.5 Configure 'Do not allow users to enable or disable add-ons' (Not Scored)
  - Description: This policy setting allows you to manage whether users have the ability to allow or deny add-ons through Add-On Manager.

# Case Study Security Hardening – IE Browser

---

- ... Description: If you enable this policy setting, users cannot enable or disable add-ons through Add-On Manager. The only exception occurs if an add-on has been specifically entered into the 'Add-On List' policy setting in such a way as to allow...



# Case Study Security Hardening – IE Browser

---

- ... Description: users to continue to manage the add-on. In this case, the user can still manage the add-on through the Add-On Manager. If you disable or do not configure this policy setting, the appropriate controls in the Add-On...

# Case Study Security Hardening – IE Browser

---

- ... Description:  
Manager will be available to the user. Configure this setting in a manner that is consistent with security and operational requirements of your organization.

# Case Study Security Hardening – IE Browser

---

- Rationale: Users often choose to install add-ons that are not permitted by an organization's security policy. Such add-ons can pose a significant security and privacy risk to your network.

# Case Study Security Hardening – IE Browser

---

- Audit: Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

# Case Study Security Hardening – IE Browser

---

– Audit:

**HKEY\_LOCAL\_MACHINE\Software\Policies\Microsoft\Internet Explorer\Restrictions\NoExtensionManagement**



# Case Study Security Hardening – IE Browser

---

- Remediation: To establish the recommended configuration via Group Policy, set the following UI path to Not Configured.

# Case Study Security Hardening – IE Browser

---

- Remediation:  
Computer  
Configuration\Admini  
strative  
Templates\Windows  
Components\Internet  
Explorer\Do not  
allow users to enable  
or disable add-ons

# Case Study Security Hardening – IE Browser

---

- Impact: When the Do not allow users to enable or disable add-ons setting is enabled, users will not be able to enable or disable their own Internet Explorer add-ons. If your organization uses add-ons,

# Case Study Security Hardening – IE Browser

---

- Impact: ... this configuration may affect their ability to work.

# Case Study Security Hardening – IE Browser

- 1.5 Configure 'Do not allow users to enable or disable add-ons' (Not Scored)
  - Default Value: Disabled



# Security Hardening – Case Study - Chrome

---

- Google Chrome
- DISA, Release 8
  - 27 April, 2017

# Security Hardening – Case Study - Chrome

## STIGVIEWER WINDOW

The screenshot displays the DISA STIG Viewer 2.5.4 application. The interface is divided into several sections:

- STIG Explorer:** A tree view on the left showing various STIGs. The 'Google Chrome Current Windows Security Technical Implementation Guide' is selected and checked.
- Filter Panel:** Located below the STIG Explorer, it includes a 'CAT I' dropdown, a 'CAT I' label, an 'Add' button, and radio buttons for 'Inclusive (+) Filter' (selected) and 'Exclusive (-) Filter'. Below these are input fields for '+ / -', 'Keyword', and 'Filter'.
- Rule List:** A table in the center showing a list of rules. The columns are 'Vul ID' and 'Rule Name'. The rules listed are:

| Vul ID  | Rule Name                                           |
|---------|-----------------------------------------------------|
| V-44745 | DTBC0015 - Outdated plugins                         |
| V-44749 | DTBC0014 - Plugins requiring authorization          |
| V-44751 | DTBC0015 - Third party cookies                      |
| V-44753 | DTBC0017 - Disable background processing            |
| V-44757 | DTBC0019 - 3D Graphics APIs                         |
| V-44759 | DTBC0020 - Google Data Synchronization              |
| V-44761 | DTBC0021 - URL protocol schemas                     |
| V-44763 | DTBC0022 - AutoComplete for forms                   |
| V-44765 | DTBC0023 - Cloud print sharing                      |
| V-44769 | DTBC0025 - Network prediction                       |
| V-44771 | DTBC0026 - Metrics reporting                        |
| V-44773 | DTBC0027 - Search suggestions                       |
| V-44775 | DTBC0029 - Import of saved passwords                |
| V-44777 | DTBC0030 - Incognito Mode                           |
| V-44781 | DTBC0034 - Plugin blacklist                         |
| V-44783 | DTBC0035 - Approved plugins                         |
| V-44787 | DTBC0036 - Automatic plugin search and installation |
| V-44789 | DTBC0037 - Online revocation checks                 |
- General Information:** A panel on the right showing details for the selected rule. It includes fields for 'ID' (DTBC-0045), 'Rule' (SV-), 'Severity' (57633r4\_rule), 'Class' (Vuln), and 'Vuln' (V-44700).
- Discussion:** A section below General Information containing text about the policy: 'Policy allows you to set a list of URL pa specify sites which are allowed to set s cookies. If this policy is left not set the value will be used for all sites either fro 'DefaultCookieSetting' policy if it is co'.
- Check Content:** A section containing a 'Universal method:' with two steps: '1. In the omnibox(address bar) type ch' and '2. If the policy 'CookiesSessionOnlyFor has any defined values, this is a finding'.
- Fix Text:** A section containing a 'Windows group policy:' with one step: '1. Open the group policy editor tool w'.

# Security Hardening – Case Study - Chrome

---

- General Information:
  - **Rule Title :** Session only based cookies must be disabled.

# Security Hardening – Case Study - Chrome

---

- General Information:
  - **Vuln ID:** V-44799
  - **STIG ID:** DTBC-0045
  - **Severity:** CAT I



# Security Hardening – Case Study - Chrome

---

- **Discussion:**
  - Policy allows you to set a list of URL patterns that specify sites which are allowed to set session only cookies. If this policy is left not set the global default value will be used for all sites...



# Security Hardening – Case Study - Chrome

---

- **Discussion:**
  - ... either from the 'DefaultCookiesSetting' policy if it is set, or the user's personal configuration otherwise. If the 'RestoreOnStartup' policy is set to restore URLs from...

# Security Hardening – Case Study - Chrome

---

- **Discussion:**
  - ... previous sessions this policy will not be respected and cookies will be stored permanently for those sites

# Security Hardening – Case Study - Chrome

---

- **Check Content:**
  - Universal method:
    1. In the omnibox (address bar) type `chrome://policy`
    2. If the policy 'CookiesSessionOnlyForUrls' exists, and has any defined values, this is a finding...

# Security Hardening – Case Study - Chrome

---

- **Check Content:**
  - ... Windows method:
    1. Start regedit
    2. Navigate to HKLM\Software\Policies\Google\Google Chrome\Content Settings\CookieSessionOnlyForUrls
    3. If this key exists and has any defined values, this is a finding

# Security Hardening – Case Study - Chrome

---

- **Fix Text:**
  - Windows group policy:
    1. Open the group policy editor tool with gpedit.msc



# Security Hardening – Case Study - Chrome

- **Fix Text...:**
  - 2. Navigate to Policy  
Path: Computer  
Configuration\Admini  
strative  
Templates\Google\Go  
ogle Chrome\Content  
Settings  
Policy Name: Allow  
session only cookies  
on these sites  
Policy State: Disabled  
Policy Value: N/A...

# Security Hardening – Case Study - Chrome

---

- **CCI (Control Correlation Identifier):**
  - CCI-000166  
The information system protects against an individual (or process acting on behalf of an individual) falsely denying having performed...

# Security Hardening – Case Study - Chrome

- **CCI (Control Correlation Identifier):**
  - ... organization-defined actions to be covered by non-repudiation.  
NIST SP 800-53 :: AU-10  
NIST SP 800-53A :: AU-10.1  
NIST SP 800-53  
Revision 4 :: AU-10

# Case Study Security Hardening – Firefox

---

- CIS Benchmarks case study (Mozilla Firefox)

# Case Study Security Hardening – Firefox

## CIS Mozilla Firefox 38 ESR Benchmark

v1.0.0 - 12-31-2015

- December 31, 2015
- 72 pages PDF doc



# Case Study Security Hardening – Firefox

---

- 3.5 (L2) *Enable IDN Show Punycode (Scored)*
- Profile applicability:
  - Level 2

# Case Study Security Hardening – Firefox

---

- 3.5 (L2) *Enable IDN Show Punycode (Scored)*
  - **Description:** This feature determines whether all Internationalized Domain Names (IDNs) displayed in the browser are displayed as Punycode or as Unicode.

# Case Study Security Hardening – Firefox

---

- 3.5 (L2) *Enable IDN Show Punycode (Scored)*
  - **Rationale:** IDNs displayed in Punycode are easier to identify and therefore help mitigate the risk of accessing spoofed web pages.

# Case Study Security Hardening – Firefox

- 3.5 (L2) *Enable IDN Show Punycode (Scored)*
  - **Audit:** Perform the following procedure:
    1. Type about:config in the address bar
    2. Type network.IDN\_show\_punycode in the filter
    3. Ensure the preferences listed are set to the values specified below:

# Case Study Security Hardening – Firefox

---

- ... Audit:  
`network.IDN_show_punycode=true`



# Case Study Security Hardening – Firefox

- 3.5 (L2) *Enable IDN Show Punycode (Scored)*

- **Remediation:**

- Perform the following procedure:

1. Open the mozilla.cfg file in the installation directory with a text editor
2. Add the following lines to mozilla.cfg:

- ```
lockPref("network.IDN_show_punycode", true);
```

Case Study Security Hardening – Firefox

- 3.5 (L2) *Enable IDN Show Punycode (Scored)*
 - **Default Value:** false

END

Security Hardening – Case Study - FW

- Firewall STIG
- DISA, Release 22
 - 28 April, 2017

Security Hardening – Case Study - FW

STIGVIEWER WINDOW

The screenshot displays the DISA STIG Viewer 2.5.4 application. The interface includes a menu bar (File, Export, Checklist, Options, Help) and a toolbar. The main window is divided into several panes:

- STIG Explorer:** A tree view showing the selected STIG, "Firewall Security Technical Implementation Guide - Cisco".
- Table:** A list of rules with columns for Vul ID and Rule Name. The rules are as follows:

Vul ID	Rule Name
V-3000	Interface ACL deny ...
V-3008	IPSec VPN is not co...
V-3012	Network element is...
V-3013	Login banner is no...
V-3014	Management conn...
V-3020	DNS servers must b...
V-3021	SNMP access is not...
V-3043	SNMP privileged a...
V-3054	Firewall has unnece...
V-3056	Group accounts are...
V-3057	Accounts assigned ...
V-3058	Unauthorized acco...
V-3062	Passwords are view...
V-3069	Management conn...
V-3070	Management conn...
V-3085	HTTP server is not ...
V-3143	Devices exist with s...

- General Information:** Displays the title "Firewall Security Technical Implementation Guide :: Release: 22 Benchmark Da 28 Apr 2017", the rule title "The network device must log all interface access control lists (ACL) deny statement", the STIG ID "NET1020", the rule ID "SV-3000r4 rule", and the severity "CAT III".
- Discussion:** A text block explaining that auditing and logging are key components of any security architecture and that it is essential for security personnel to know what is being done, attempted to be done, and by whom in order to compile accurate risk assessment.
- Check Content:** A text block stating "Review the network device interface ACLs to verify all deny statements are logged." and "If deny statements are not logged, this is a finding."

Security Hardening – Case Study - FW

- General Information:
 - **Rule Title :** The device must be configured to protect the network against denial of service attacks such as Ping of Death, TCP SYN floods, etc.

Security Hardening – Case Study - FW

- General Information:
 - **Vuln ID:** V-3156
 - **STIG ID:** NET0375
 - **Severity:** CAT II

Security Hardening – Case Study - FW

- **Discussion:**
 - A SYN-flood attack is a denial-of-service attack where the attacker sends a huge amount of please-start-a-connection packets and then nothing else. This causes the device being attacked to be overloaded with the..

Security Hardening – Case Study - FW

- **... Discussion:**
 - ... open sessions and eventually crash.
 - A ping sweep (also known as an ICMP sweep) is a basic network scanning technique used to determine which of a range of IP addresses map to live hosts (computers)

Security Hardening – Case Study - FW

- **Check Content:**
 - Review the device configurations to determine if denial of service attacks guarded against.
 - If the device is not configured to mitigate denial of service attacks, this is a finding.

Security Hardening – Case Study - FW

- **Fix Text:**
 - If the firewall support SYN-flood or ping sweep protection then enable these features. If the firewall does not support these features, enable the security features on the router to protect the network from these attacks.

Security Hardening – Case Study - FW

- CCI (Control Correlation Identifier):
 - (Misc info)

END

Security Hardening – Case Study - Switch

- Layer 2 Switch STIG
- DISA, Release 20
 - 28 Oct, 2016

Security Hardening – Case Study - Switch

STIGVIEWER WINDOW

The screenshot displays the DISA STIG Viewer 2.5.4 application. The interface includes a menu bar (File, Export, Checklist, Options, Help) and a toolbar. The main window is divided into several panes:

- STIG Explorer:** A tree view on the left showing the hierarchy of STIGs. The 'Layer 2 Switch Security Technical Implementation Guide' is selected and checked.
- Filter Panel:** A section below the STIG Explorer with a dropdown menu set to 'CAT I' and a search bar. It includes radio buttons for 'Inclusive (+) Filter' (selected) and 'Exclusive (-) Filter'.
- Table:** A central table listing security rules with columns for 'Vul ID' and 'Rule Name'. The rules are as follows:

Vul ID	Rule Name
V-5622	A dedicated VLAN is required for all trunk ports.
V-5623	Ensure trunking is disabled on all access ports.
V-5624	Re-authentication must occur every 60 minutes.
V-5626	NET-NAC-009
V-5628	The VLAN1 is being used for management traffic.
V-5646	Devices not configured to filter and drop half-open connections.
V-7011	The auxiliary port is not disabled.
V-14669	BSDr commands are not disabled.
V-14671	NTP messages are not authenticated.
V-14717	The network element must not allow SSH Version 1.
V-15432	The device is not authenticated using a AAA server.
V-15434	Emergency administration account privilege level is not set.
V-17820	OOBM switch not connected to the NE OOBM interface
V-17821	The OOBM interface not configured correctly.
V-17824	Management interface is assigned to a user VLAN.
V-17825	Management VLAN has invalid addresses
V-17826	Invalid ports with membership to the mgmt VLAN
V-17827	The management VLAN is not pruned from trunk links

- General Information:** A pane on the right showing details for the selected rule. It includes the title 'Layer 2 Switch Security Technical Implementation Guide', the benchmark date '28', and the rule title 'The IAO will ensure that configured using MAC port security receiving a frame with a different I'.
- Discussion:** A section below the general information providing context for the rule. It states: 'The Port Security feature remembers address connected to the switch port address to communicate on that port address tries to communicate through will disable the port.'
- Check Content:** A section at the bottom of the right pane showing the specific configuration requirements for the rule. It states: 'A shutdown action puts the interface state immediately and sends an SNMP receives a frame with a different layer what has been configured or learned following Catalyst IOS interface com'.

Security Hardening – Case Study - Switch

- General Information:
 - **Rule Title :** The IAO to that all switchports configured using MAC port security will shutdown upon receiving a frame with a different layer 2 source address than what has been configured or learned for port security

Security Hardening – Case Study - Switch

- General Information:
 - **Vuln ID:** V-18565
 - **STIG ID:** NET-NAC-032
 - **Severity:** CAT III

Security Hardening – Case Study - Switch

- **Discussion:**
 - The Port Security feature remembers the Ethernet MAC address connected to the switch port and allows only that MAC address to communicate on that port...

Security Hardening – Case Study - Switch

- **... Discussion:**
 - ... If any other MAC address tries to communicate through the port, port security will disable the port.

Security Hardening – Case Study - Switch

- **Check Content:**
 - A shutdown action puts the interface into the error-disabled state immediately and sends an SNMP trap notification if it receives a frame with a different layer 2 source address that what has been...

Security Hardening – Case Study - Switch

- **Check Content:**
 - ... configured or learned for port security. The following Catalyst IOS interface command will shutdown the interface when such an event occurs:
switchport port-security violation shutdown

Security Hardening – Case Study - Switch

- **Fix Text:**
 - Configure the port to shutdown when insecure hosts are connected to the wall jack.

END

Case Study Security Hardening – Cisco IOS 15

- CIS Benchmarks case study (Cisco IOS 15)
- For Cisco routers running IOS 15M

Case Study Security Hardening – Cisco IOS 15

CIS Cisco IOS 15 Benchmark

v4.0.0 - 06-30-2015

- June 30, 2015
- 151 pages PDF doc

Case Study Security Hardening – Cisco IOS 15

- 3.3.2.2 Set 'ip ospf message-digest-key md5' (Scored)
- Profile applicability:
 - Level 2

Case Study Security Hardening – Cisco IOS 15

- 3.3.2.2 Set 'ip ospf message-digest-key md5' (Scored)
 - **Description:** Enable Open Shortest Path First (OSPF) Message Digest 5 (MD5) authentication.

Case Study Security Hardening – Cisco IOS 15

- 3.3.2.2 Set 'ip ospf message-digest-key md5' (Scored)
 - **Rationale:** This is part of the OSPF authentication setup

Case Study Security Hardening – Cisco IOS 15

- 3.3.2.2 Set 'ip ospf message-digest-key md5' (Scored)
 - **Audit:** Verify the appropriate md5 key is defined on the appropriate interface(s)

hostname#sh run int
{interface}

Case Study Security Hardening – Cisco IOS 15

- 3.3.2.2 Set 'ip ospf message-digest-key md5' (Scored)
 - **Remediation:**
Configure the appropriate interface(s) for Message Digest authentication

Case Study Security Hardening – Cisco IOS 15

- 3.3.2.2 Set 'ip ospf message-digest-key md5' (Scored)

– Remediation:...

```
hostname(config)#inte  
rface {interface_name}  
hostname(config-if)#ip  
ospf message-digest-  
key {ospf_md5_key-id}  
md5 {ospf_md5_key}
```

Case Study Security Hardening – Cisco IOS 15

- 3.3.2.2 Set 'ip ospf message-digest-key md5' (Scored)
 - **Impact:**
Organizations should plan and implement enterprise security policies that require rigorous authentication methods for routing protocols...

Case Study Security Hardening – Cisco IOS 15

- 3.3.2.2 Set 'ip ospf message-digest-key md5' (Scored)
 - **Impact:**
... Configuring the proper interface(s) for 'ip ospf message-digest-key md5' enforces these policies by restricting exchanges between network devices.

Case Study Security Hardening – Cisco IOS 15

- 3.3.2.2 Set 'ip ospf message-digest-key md5' (Scored)
 - **Default Value:** Not set

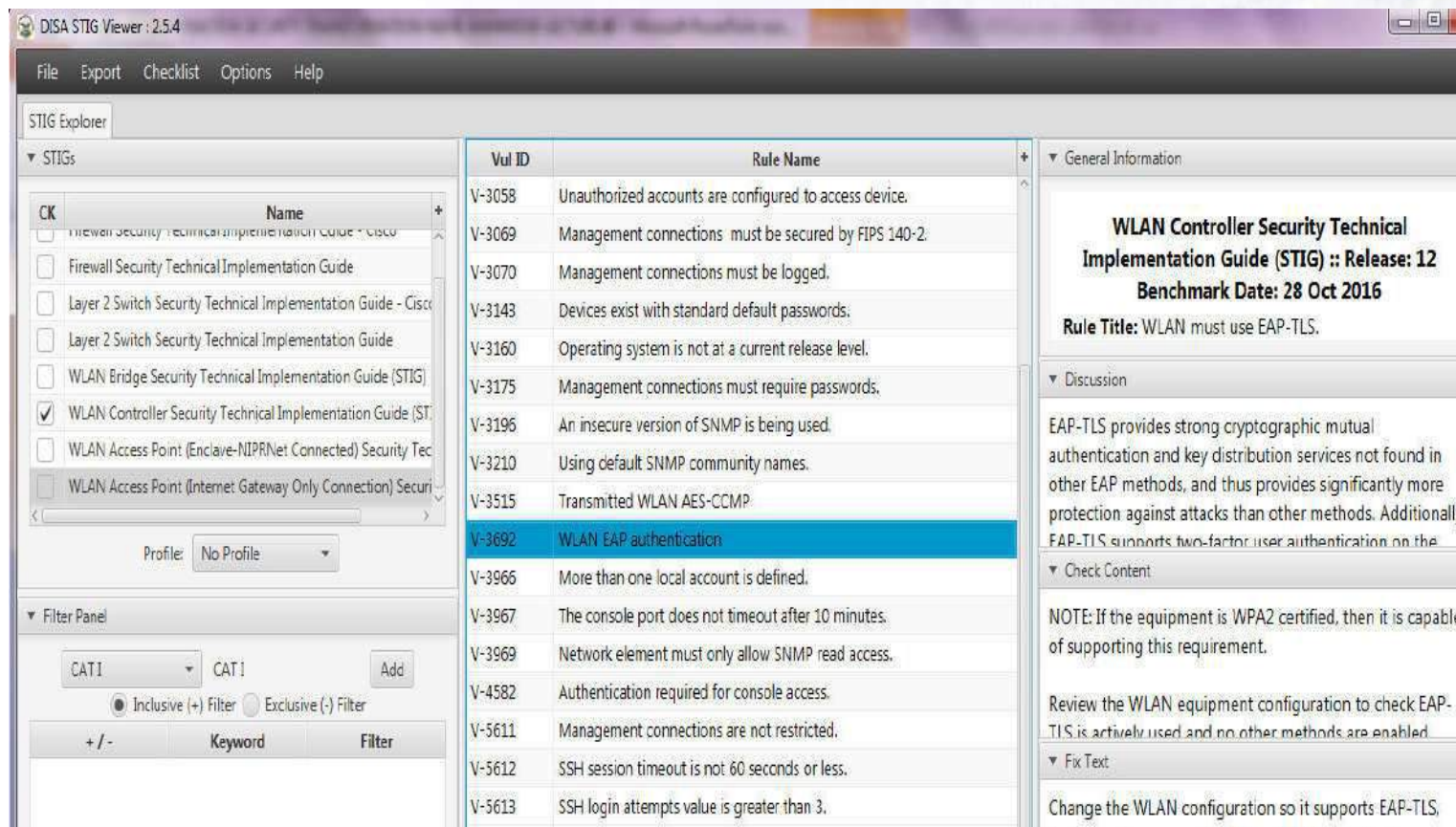
END

Security Hardening – Case Study - WLAN

- WLAN Controller STIG
- DISA, Release 12
 - 28 Oct, 2016

Security Hardening – Case Study - WLAN

STIGVIEWER WINDOW



DISA STIG Viewer : 2.5.4

File Export Checklist Options Help

STIG Explorer

▼ STIGs

CK	Name
☐	Firewall Security Technical Implementation Guide - Cisco
☐	Firewall Security Technical Implementation Guide
☐	Layer 2 Switch Security Technical Implementation Guide - Cisco
☐	Layer 2 Switch Security Technical Implementation Guide
☐	WLAN Bridge Security Technical Implementation Guide (STIG)
☒	WLAN Controller Security Technical Implementation Guide (STIG)
☐	WLAN Access Point (Enclave-NIPRNet Connected) Security Tec
☐	WLAN Access Point (Internet Gateway Only Connection) Securi

Profile: No Profile ▼

▼ Filter Panel

CAT I CAT I Add

☒ Inclusive (+) Filter ☐ Exclusive (-) Filter

+ / - Keyword Filter

Vol ID	Rule Name
V-3058	Unauthorized accounts are configured to access device.
V-3069	Management connections must be secured by FIPS 140-2.
V-3070	Management connections must be logged.
V-3143	Devices exist with standard default passwords.
V-3160	Operating system is not at a current release level.
V-3175	Management connections must require passwords.
V-3196	An insecure version of SNMP is being used.
V-3210	Using default SNMP community names.
V-3515	Transmitted WLAN AES-CCMP.
V-3692	WLAN EAP authentication.
V-3966	More than one local account is defined.
V-3967	The console port does not timeout after 10 minutes.
V-3969	Network element must only allow SNMP read access.
V-4582	Authentication required for console access.
V-5611	Management connections are not restricted.
V-5612	SSH session timeout is not 60 seconds or less.
V-5613	SSH login attempts value is greater than 3.

▼ General Information

WLAN Controller Security Technical Implementation Guide (STIG) :: Release: 12
Benchmark Date: 28 Oct 2016
Rule Title: WLAN must use EAP-TLS.

▼ Discussion

EAP-TLS provides strong cryptographic mutual authentication and key distribution services not found in other EAP methods, and thus provides significantly more protection against attacks than other methods. Additionally, EAP-TLS supports two-factor user authentication on the

▼ Check Content

NOTE: If the equipment is WPA2 certified, then it is capable of supporting this requirement.

Review the WLAN equipment configuration to check EAP-TLS is actively used and no other methods are enabled.

▼ Fix Text

Change the WLAN configuration so it supports EAP-TLS.

Security Hardening – Case Study - WLAN

- General Information:
 - **Rule Title :** WLAN must use EAP-TLS

Security Hardening – Case Study - WLAN

- General Information:
 - **Vuln ID:** V-3692
 - **STIG ID:** WIR0115-01
 - **Severity:** CAT II

Security Hardening – Case Study - WLAN

- **Discussion:**
 - EAP-TLS provides strong cryptographic mutual authentication and key distribution services not found in other EAP methods, and thus provides significantly more protection against attacks than other...

Security Hardening – Case Study - WLAN

- **... Discussion:**
 - ... methods.
Additionally, EAP-TLS supports two-factor user authentication on the WLAN client, which provides significantly more protection than methods that rely on a password or certificate alone.

Security Hardening – Case Study - WLAN

- ... Discussion:
 - ... EAP-TLS also can leverage DoD CAC in its authentication services, providing additional security and convenience.

Security Hardening – Case Study - WLAN

- **Check Content:**
 - NOTE: If the equipment is WPA2 certified, then it is capable of supporting this requirement.
 - Review the WLAN equipment configuration to check EAP-TLS is actively used and no other methods are enabled.

Security Hardening – Case Study - WLAN

- **Check Content:**
 - ... Mark as a finding if either EAP-TLS is not used or if the WLAN system allows users to connect with other methods.

Security Hardening – Case Study - WLAN

- **Fix Text:**
 - Change the WLAN configuration so it supports EAP-TLS, implementing supporting PKI and AAA infrastructure as necessary.

Security Hardening – Case Study - WLAN

- **Fix Text:**
 - If the WLAN equipment is not capable of supporting EAP-TLS, procure new equipment capable of such support.

END

Security Hardening – Case Study – L3 Switch

- Infrastructure Layer 3 Switch STIG
- DISA, Release 22
 - 28 April, 2017

Security Hardening – Case Study - L3 Switch

STIGVIEWER WINDOW

The screenshot displays the DISA STIG Viewer 2.5.4 application. The interface includes a menu bar (File, Export, Checklist, Options, Help), a STIG Explorer pane on the left, a central table of rules, and a right-hand pane for detailed information.

STIG Explorer: A tree view showing various STIGs. The 'Infrastructure L3 Switch Secure Technical Implementation Guide' is selected and checked.

Filter Panel: Shows a filter set named 'CAT I' with 'Inclusive (+) Filter' selected. The 'Add' button is visible.

Rule Table:

Vul ID	Rule Name
V-17832	Mgmt VLAN does not have correct IP address
V-17833	No ingress ACL on management VLAN interface
V-17834	No inbound ACL for mgmt network sub-interface
V-17835	IPSec traffic is not restricted
V-17836	Management traffic is not classified and marked
V-17837	Management traffic doesn't get preferred treatment
V-18522	ACLs must restrict access to server VLANs.
V-18523	ACLs do not protect against compromised servers
V-18544	Restricted VLAN not assigned to non-802.1x device.
V-18545	Upstream access not restricted for non-802.1x VLAN
V-18565	Switchport does not shutdown on a violation
V-18566	NET-NAC-031
V-18790	NET-TUNL-012
V-19188	Control plane protection is not enabled.
V-19189	No Admin-local or Site-local boundary
V-23747	Two NTP servers are not used to synchronize time.

General Information:

- Rule Title:** The administrator must ensure the that all L2TPv3 sessions are authenticated prior to transporting traffic.
- STIG ID:** NET-TUNL-034
- Rule ID:** SV-40556r1_rule
- Severity:** CAT II
- Class:** Unclass
- Vuln ID:** V-20744

Discussion:

L2TPv3 sessions can be used to transport layer-2 protocols across an IP backbone. These protocols were intended for link-local scope only and are therefore less defended and not as well-known. As stated in DoD IPv6 IA Guidance for MO3 (S4-C7-1), the L2TP tunnels can also carry IP packets that are very difficult to filter because of the additional

Check Content:

Review the router or multi-layer switch configuration and determine if L2TPv3 has been configured to provide transport across an IP network. If it has been configured, verify that the L2TPv3 session requires authentication.

Security Hardening – Case Study - L3 Switch

- General Information:
 - **Rule Title :** The administrator must ensure the that all L2TPv3 sessions are authenticated prior to transporting traffic.

Security Hardening – Case Study - L3 Switch

- General Information:
 - **Vuln ID:** V-30744
 - **STIG ID:** NET-TUNL-034
 - **Severity:** CAT II

Security Hardening – Case Study - L3 Switch

- **Discussion:**
 - L2TPv3 sessions can be used to transport layer-2 protocols across an IP backbone. These protocols were intended for link-local scope only and are therefore less defended and not as well-known.

Security Hardening – Case Study - L3 Switch

- **... Discussion:**
 - ... As stated in DoD IPv6 IA Guidance for MO3 (S4-C7-1), the L2TP tunnels can also carry IP packets that are very difficult to filter because of the additional encapsulation.

Security Hardening – Case Study - L3 Switch

- **... Discussion:**
 - ... Hence, it is imperative that L2TP sessions are authenticated prior to transporting traffic

Security Hardening – Case Study - L3 Switch

- **Check Content:**
 - Review the router or multi-layer switch configuration and determine if L2TPv3 has been configured to provide transport across an IP network. If it has been configured, verify that the L2TPv3 session requires authentication.

Security Hardening – Case Study - L3 Switch

- **Check Content:**
 - ... see detailed explanation in Check Content... (configurations)

Security Hardening – Case Study - L3 Switch

- **Fix Text:**
 - Configure L2TPv3 to use authentication for any peering sessions.

END

Case Study Security Hardening – VMware

- CIS Benchmarks case study (Vmware ESXi 5.5)

Case Study Security Hardening – VMware

CIS VMware ESXi 5.5 Benchmark

v1.2.0 - 12-16-2014

- December 16, 2014
- 132 pages PDF doc

Case Study Security Hardening – VMware

- *5.1 Disable DCUI to prevent local administrative control (Scored)*
- Profile applicability:
 - Level 2

Case Study Security Hardening – VMware

- *5.1 Disable DCUI to prevent local administrative control (Scored)*
 - **Description:** The Direct Console User Interface (DCUI) can be disabled to prevent any local administration from the Host;

Case Study Security Hardening – VMware

- *5.1 Disable DCUI to prevent local administrative control (Scored)*
 - **Description:** ... Once the DCUI is disabled any administration of the ESXi host will be done through vCenter.

Case Study Security Hardening – VMware

- **Rationale:**
 - The DCUI allows for low-level host configuration such as configuring IP address, hostname and root password as well as diagnostic capabilities such as enabling the ESXi shell, viewing log files, restarting...

Case Study Security Hardening – VMware

- **Rationale:**
 - ... agents, and resetting configurations. Actions performed from the DCUI are not tracked by vCenter Server. Even if Lockdown Mode is enabled, users who are members of the DCUI.Access list can..

Case Study Security Hardening – VMware

- **Rationale:**
 - ...perform administrative tasks in the DCUI bypassing RBAC and auditing controls provided through vCenter. DCUI access can be disabled. Disabling it prevents all local activity and thus forces actions to be...

Case Study Security Hardening – VMware

- **Rationale:**
 - ...performed in vCenter Server where they can be centrally audited and monitored.

Case Study Security Hardening – VMware

- **Audit:** Perform the following:
 1. From the vSphere web client select the host.
 2. Select "Manage" -> "Settings" -> "System" -> "Security Profile".
 3. Scroll down to "Services".
 4. Click "Edit...".
 5. Select "Direct Console UI".

Case Study Security Hardening – VMware

- **Audit:** ... Perform the following:
 6. Verify the Startup Policy is set to "Start and Stop Manually"

Case Study Security Hardening – VMware

- **Audit:** ... Additionally, the following PowerCLI command may be used:
 - # List DCUI settings for all hosts
Get-VMHost | Get-VMHostService | Where { \$_.key -eq "DCUI" }

Case Study Security Hardening – VMware

- **Remediation:** Perform the following:
 1. From the vSphere web client select the host.
 2. Select "Manage" -> "Settings" -> "System" -> "Security Profile".
 3. Scroll down to "Services".
 4. Click "Edit...".
 5. Select "Direct Console UI".

Case Study Security Hardening – VMware

- **Remediation:...**
 6. Click "Stop".
 7. Change the Startup Policy "Start and Stop Manually".
 8. Click "OK".

Case Study Security Hardening – VMware

- **Impact:**
 - Disabling the DCUI can create a potential "lock out" situation should the host become isolated from vCenter Server. Recovering from a "lock out" scenario requires re-installing ESXi. Consider leaving DCUI enabled and...

Case Study Security Hardening – VMware

- **Impact:**
 - ...instead enable lockdown mode and limit the users allowed to access the DCUI using the DCUI.Access list.

Case Study Security Hardening – VMware

- **Default Value:**
 - The prescribed state is not the default state.

Case Study Security Hardening – VMware

- References:
 - <http://pubs.vmware.com/vsphere-55/topic/com.vmware.vsphere.security.doc/GUID-6779F098-48FE-4E22-B116-A8353D19FF56.html>

END

Case Study Security Hardening – Cloud AWS

- CIS Benchmarks case study (Cloud – Amazon Web Services Foundations)

Case Study Security Hardening – Cloud AWS

CIS Amazon Web Services Foundations

v1.1.0 - 11-29-2016

- November 29, 2016
- 148 pages PDF doc

Case Study Security Hardening – Cloud AWS

- 1.14 *Ensure hardware MFA is enabled for the "root" account (Scored)*
- Profile applicability:
 - Level 2

Case Study Security Hardening – Cloud AWS

- 1.14 *Ensure hardware MFA is enabled for the "root" account (Scored)*
 - **Description:** The root account is the most privileged user in an AWS account. MFA adds an extra layer of protection on top of a user name and password;

Case Study Security Hardening – Cloud AWS

- 1.14 *Ensure hardware MFA is enabled for the "root" account (Scored)*
 - **Description:**... With MFA enabled, when a user signs in to an AWS website, they will be prompted for their user name and password as well as for an authentication...

Case Study Security Hardening – Cloud AWS

- 1.14 *Ensure hardware MFA is enabled for the "root" account (Scored)*
 - **Description:**... code from their AWS MFA device. For Level 2, it is recommended that the root account be protected with a hardware MFA.

Case Study Security Hardening – Cloud AWS

- **Rationale:**
 - A hardware MFA has a smaller attack surface than a virtual MFA. For example, a hardware MFA does not suffer the attack surface introduced by the mobile smartphone on which a virtual MFA resides;

Case Study Security Hardening – Cloud AWS

- **Rationale:**
 - ... **Note:** Using hardware MFA for many, many AWS accounts may create a logistical device management issue. If this is the case, consider implementing this Level 2 recommendation...

Case Study Security Hardening – Cloud AWS

- **Rationale:**
 - ...selectively to the highest security AWS accounts and the Level 1 recommendation applied to the remaining accounts.

Case Study Security Hardening – Cloud AWS

- **Audit:** Perform the following to determine if the root account has a hardware MFA setup:

1. Run the following command to list all virtual MFA devices:

```
aws iam list-virtual-mfa-devices
```


Case Study Security Hardening – Cloud AWS

- **Audit: ...**
 2. If the output contains one MFA with the following Serial Number, it means the MFA is virtual, not hardware and the account is not compliant with this recommendation:

"SerialNumber":

"arn:aws:iam::<aws_account_number>mfa/root-account-mfa-device"

Case Study Security Hardening – Cloud AWS

- **Remediation:** [8 step process... check the benchmark]

Case Study Security Hardening – Cloud AWS

- References:
 - http://docs.aws.amazon.com/IAM/latest/UserGuide/id_credentials_mfa_enable_virtual.html
 - http://docs.aws.amazon.com/IAM/latest/UserGuide/id_credentials_mfa_enable_physical.html#enable-hw-mfa-for-root

END

Software Security Fundamentals-SAMM

- Software Assurance Maturity Model (SAMM) developed by OWASP
 - A guide to building security into software development
 - 96 page PDF

<http://www.opensamm.org/downloads/SAMM-1.0.pdf>

Software Security Fundamentals-SAMM

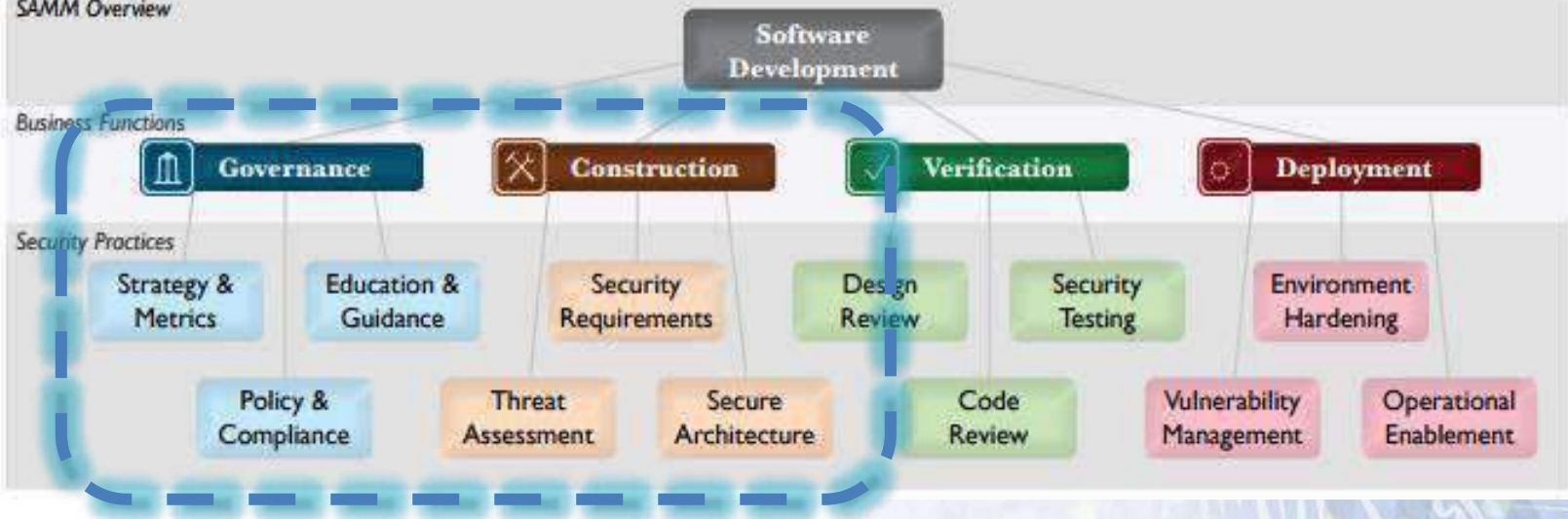
This is an OWASP Project



OWASP

The Open Web Application Security Project

SAMM Overview



Software Security Fundamentals-SAMM



Software Security Fundamentals-SAMM

- OWASP Software Assurance Maturity Model (SAMM)
Governance Phase:
 - Strategy & Metrics
 - Education & Guidance
 - Policy & Compliance

Software Security Fundamentals-SAMM

- **Strategy & Metrics:**
 - Focused on establishing the framework within an organization for a software security assurance program.

Software Security Fundamentals-SAMM

- **Strategy & Metrics:**
 - ... This is the most fundamental step in defining security goals in a way that's both measurable and aligned with the organization's real business risk.

Software Security Fundamentals-SAMM

Strategy & Metrics ...more on page 34			
	 SM 1	 SM 2	 SM 3
OBJECTIVE	Establish unified strategic roadmap for software security within the organization	Measure relative value of data and software assets and choose risk tolerance	Align security expenditure with relevant business indicators and asset value
ACTIVITIES	A. Estimate overall business risk profile B. Build and maintain assurance program roadmap	A. Classify data and applications based on business risk B. Establish and measure per-classification security goals	A. Conduct periodic industry-wide cost comparisons B. Collect metrics for historic security spend

Software Security Fundamentals-SAMM

- **Education & Guidance:**
 - Focused on arming personnel involved in the software lifecycle with knowledge and resources to design, develop, and deploy secure software

Software Security Fundamentals-SAMM

- **Education & Guidance:**
 - ... With improved access to information, project teams will be better able to proactively identify and mitigate the specific security risks that apply to their organization.

Software Security Fundamentals-SAMM

Education & Guidance

...more on page 42



OBJECTIVE

Offer development staff access to resources around the topics of secure programming and deployment

Educate all personnel in the software life-cycle with role-specific guidance on secure development

Mandate comprehensive security training and certify personnel for baseline knowledge

ACTIVITIES

- A. Conduct technical security awareness training
- B. Build and maintain technical guidelines

- A. Conduct role-specific application security training
- B. Utilize security coaches to enhance project teams

- A. Create formal application security support portal
- B. Establish role-based examination/certification

Software Security Fundamentals-SAMM

- **Policy & Compliance:**
 - Focused on understanding and meeting external legal and regulatory requirements while also driving internal security standards to ensure compliance in a way that's aligned with the business purpose of the org.

Software Security Fundamentals-SAMM

- **Policy & Compliance:**
 - A driving theme for improvement within this Practice is focus on project-level audits that gather information about the organization's behavior in order to check that expectations are being met.

Software Security Fundamentals-SAMM

Policy & Compliance

...more on page 38



OBJECTIVE

Understand relevant governance and compliance drivers to the organization

Establish security and compliance baseline and understand per-project risks

Require compliance and measure projects against organization-wide policies and standards

ACTIVITIES

- A. Identify and monitor external compliance drivers
- B. Build and maintain compliance guidelines

- A. Build policies and standards for security and compliance
- B. Establish project audit practice

- A. Create compliance gates for projects
- B. Adopt solution for audit data collection

Software Security Fundamentals-SAMM

- Lets look at SAMM Construction Phase in the next module...

END

Software Security Fundamentals-SAMM-2

- Software Assurance Maturity Model (SAMM) developed by OWASP
 - A guide to building security into software development
 - 96 page PDF

<http://www.opensamm.org/downloads/SAMM-1.0.pdf>

Software Security Fundamentals-SAMM-2

This is an OWASP Project



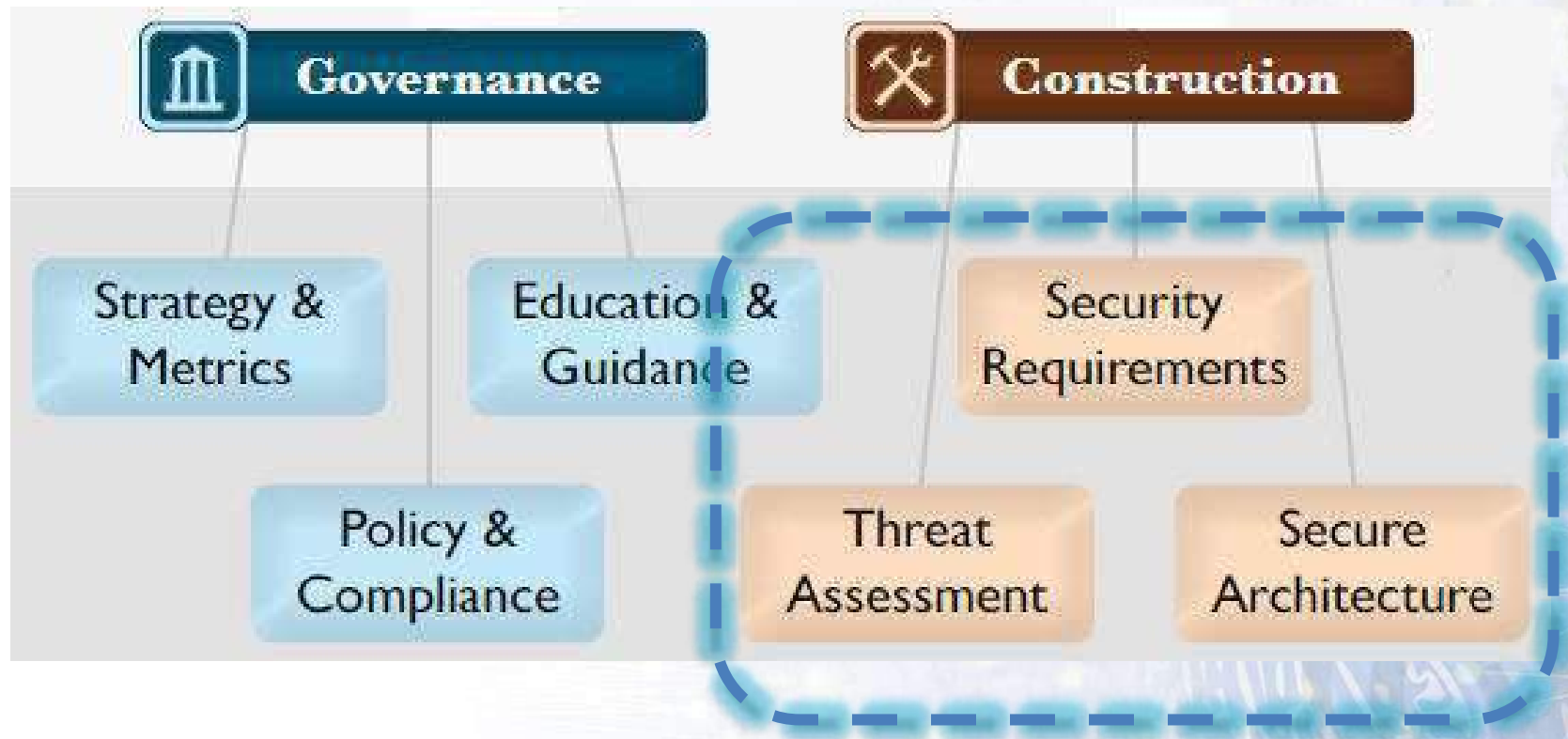
OWASP

The Open Web Application Security Project

SAMM Overview



Software Security Fundamentals-SAMM-2



Software Security Fundamentals-SAMM-2

- OWASP Software Assurance Maturity Model (SAMM)
Construction Phase:
 - Security Requirements
 - Threat Assessment
 - Secure Architecture

Software Security Fundamentals-SAMM-2

- **Security Requirements:**
 - Focused on proactively specifying the expected behavior of software with respect to security

Software Security Fundamentals-SAMM-2

- **Security Requirements:**
 - ... Through addition of analysis activities at the project level, security requirements are initially gathered based on the high-level business purpose of the software

Software Security Fundamentals-SAMM-2

Security Requirements				...more on page 50
	 SR 1	 SR 2	 SR 3	
OBJECTIVE	Consider security explicitly during the software requirements process	Increase granularity of security requirements derived from business logic and known risks	Mandate security requirements process for all software projects and third-party dependencies	
ACTIVITIES	A. Derive security requirements from business functionality B. Evaluate security and compliance guidance for requirements	A. Build an access control matrix for resources and capabilities B. Specify security requirements based on known risks	A. Build security requirements into supplier agreements B. Expand audit program for security requirements	

Software Security Fundamentals-SAMM-2

- **Threat Assessment:**
 - Centered on identification and understanding the project-level risks based on the functionality of the software being developed and characteristics of the runtime environment

Software Security Fundamentals-SAMM-2

- **Threat Assessment:**
 - ... From details about threats and likely attacks against each project, the organization as a whole operates more effectively through better decisions about prioritization of initiatives for security

Software Security Fundamentals-SAMM-2

Threat Assessment

...more on page 46



OBJECTIVE

Identify and understand high-level threats to the organization and individual projects

Increase accuracy of threat assessment and improve granularity of per-project understanding

Concretely tie compensating controls to each threat against internal and third-party software

ACTIVITIES

- A. Build and maintain application-specific threat models
- B. Develop attacker profile from software architecture

- A. Build and maintain abuse-case models per project
- B. Adopt a weighting system for measurement of threats

- A. Explicitly evaluate risk from third-party components
- B. Elaborate threat models with compensating controls

Software Security Fundamentals-SAMM-2

- **Secure Architecture:**
 - Focused on proactive steps for an organization to design and build secure software by default

Software Security Fundamentals-SAMM-2

- **Secure Architecture:**
 - By enhancing the software design process with reusable services and components, the overall security risk from software development can be dramatically reduced.

Software Security Fundamentals-SAMM-2

Secure Architecture				...more on page 54
	 SA 1	 SA 2	 SA 3	
OBJECTIVE	Insert consideration of proactive security guidance into the software design process	Direct the software design process toward known-secure services and secure-by-default designs	Formally control the software design process and validate utilization of secure components	
ACTIVITIES	A. Maintain list of recommended software frameworks B. Explicitly apply security principles to design	A. Identify and promote security services and infrastructure B. Identify security design patterns from architecture	A. Establish formal reference architectures and platforms B. Validate usage of frameworks, patterns, and platforms	

Software Security Fundamentals-SAMM-2

- SAMM is an excellent model for software security and we look at the verification and deployment phases as part of testing and validation (future module)...

END

SECURITY HARDENING – SOFTWARE APPLICATIONS

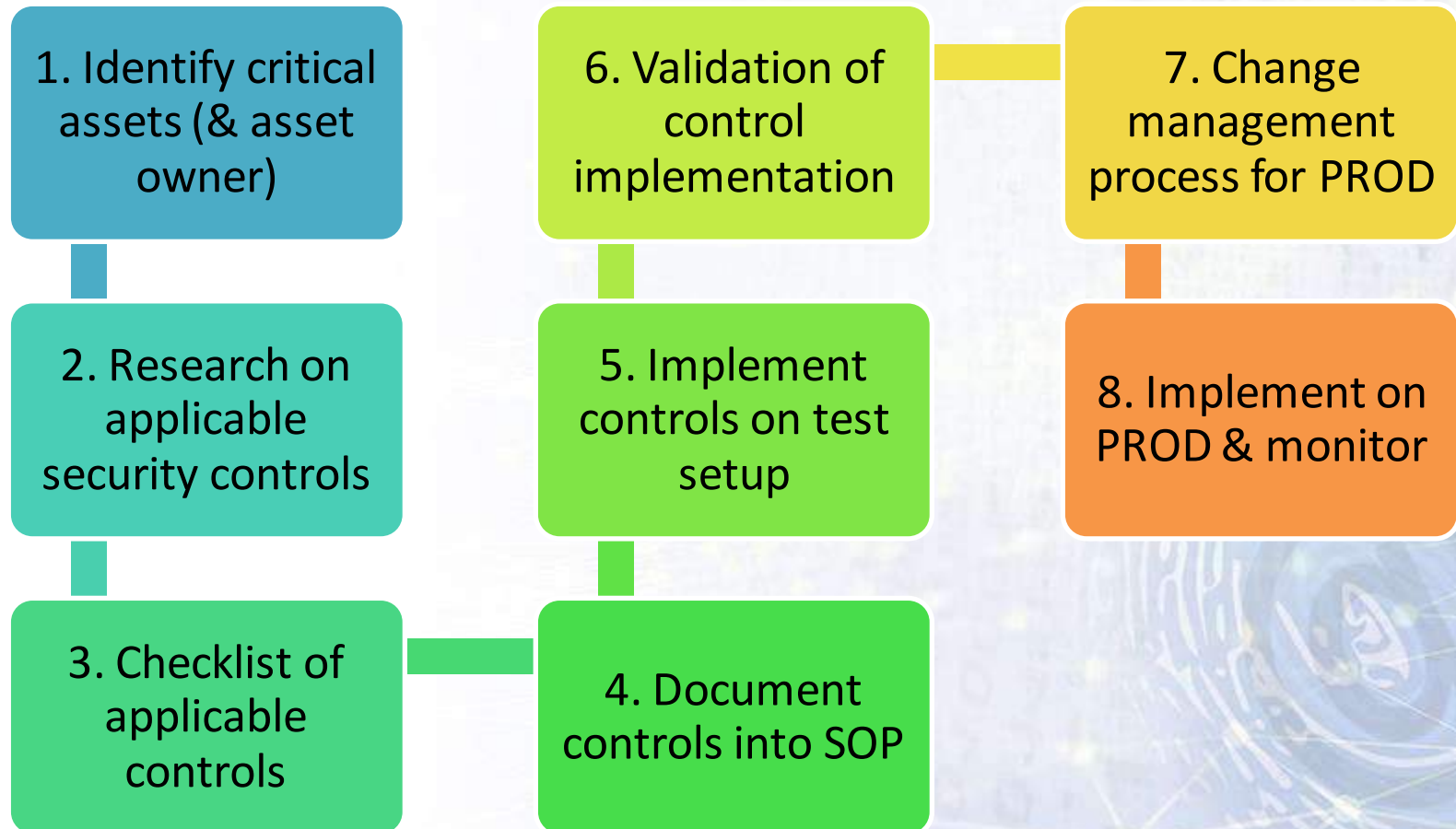
- Two types of security hardening:
 - IT assets (systems, network devices, databases, applications)
 - Software developed internally or by third party

SECURITY HARDENING – SOFTWARE APPLICATIONS

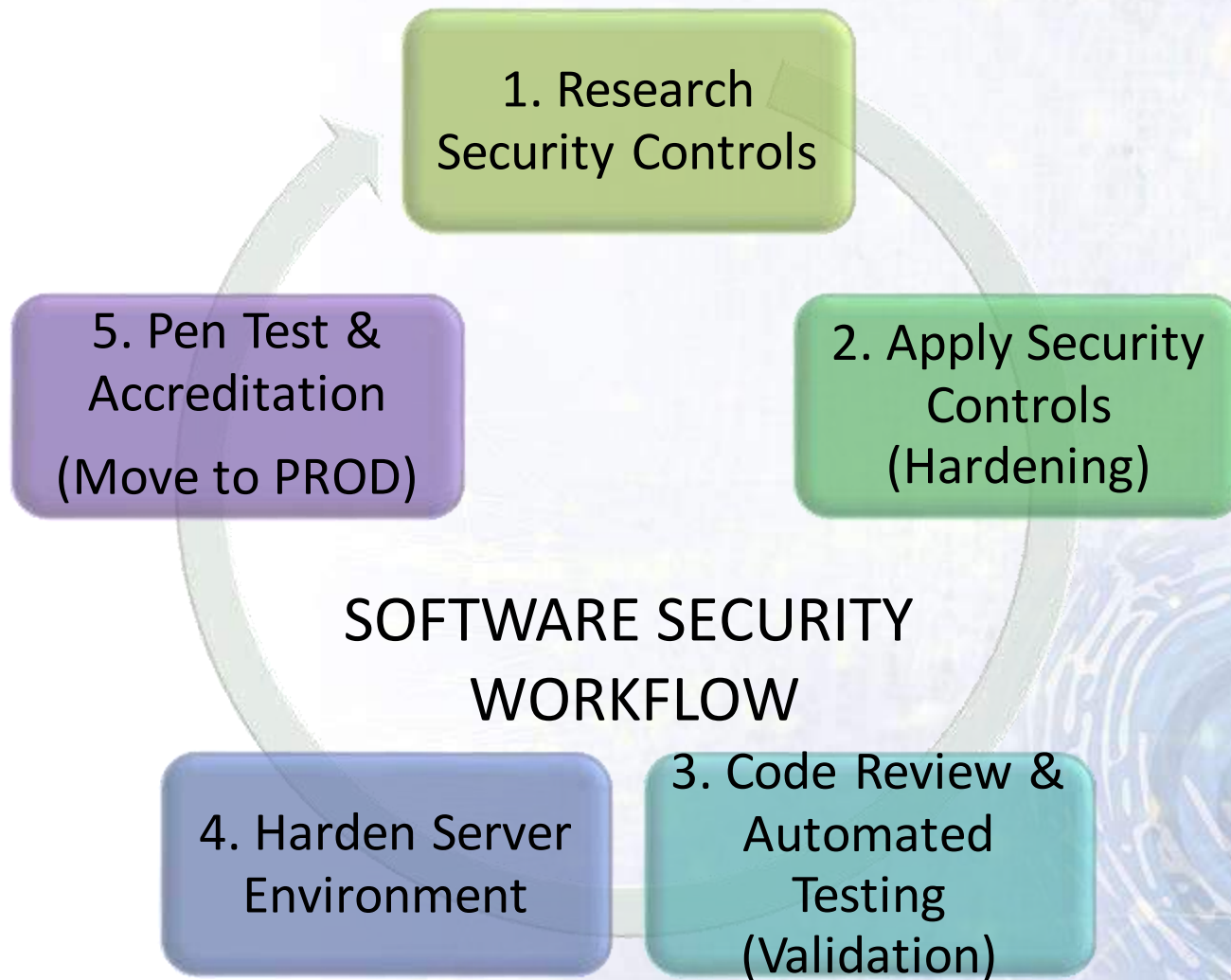
- Typical enterprise software:
 - ERP (Oracle, SAP, IBM, etc)
 - Internally or 3rd party developed software in ASP.NET, PHP, Android/IOS, or other platform

SECURITY HARDENING – SOFTWARE APPLICATIONS

8 STEP SECURITY HARDENING METHODOLOGY



SECURITY HARDENING – SOFTWARE APPLICATIONS



SECURITY HARDENING–SOFTWARE APPLICATIONS

- Useful resources:
 - www.OWASP.org
 - www.cloudsecurityalliance.org
 - MS Technet
 - OWASP Top 10
 - OWASP Secure Coding Practices Quick Reference Guide
 - SAMM

SECURITY HARDENING–SOFTWARE APPLICATIONS



OWASP Secure Coding Practices Quick Reference Guide

Secure Coding Practices Checklist
Input Validation:
Output Encoding:
Authentication and Password Management: ..
Session Management:.....
Access Control:.....
Cryptographic Practices:.....
Error Handling and Logging:
Data Protection:.....
Communication Security:
System Configuration:.....
Database Security:.....
File Management:.....
Memory Management:.....
General Coding Practices:.....

17 pages document

SECURITY HARDENING—SOFTWARE APPLICATIONS



OWASP Top 10 2017

The Ten Most Critical Web Application Security Risks

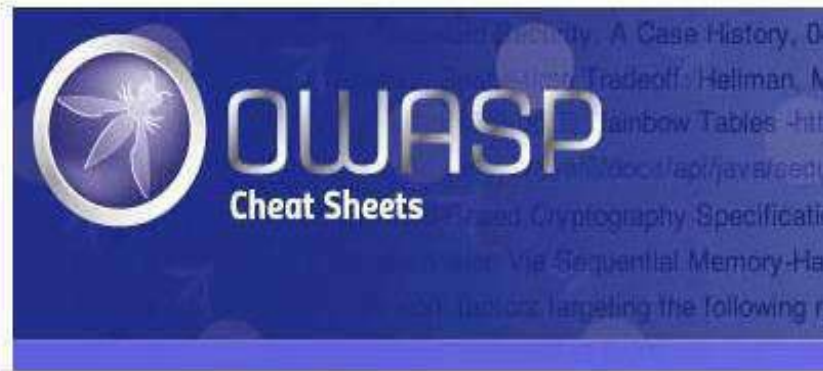
Release Candidate 2

Comments requested per instructions within

Latest version is currently under review

SECURITY HARDENING–SOFTWARE APPLICATIONS

.NET Security Cheat Sheet



Last revision (mm/dd/yy): **09/20/2017**

Latest version 20 SEPT '17

- 1 Introduction
 - 1.1 The .NET Framework
 - 1.2 Updating the Framework
- 2 .NET Framework Guidance
 - 2.1 Data Access
 - 2.2 Encryption
 - 2.3 General
- 3 ASP.NET Web Forms Guidance
 - 3.1 HTTP validation and encoding
 - 3.2 Forms authentication
- 4 ASP.NET MVC Guidance
- 5 XAML Guidance
- 6 Windows Forms Guidance
- 7 WCF Guidance

SECURITY HARDENING–SOFTWARE APPLICATIONS

- Conclusion
 - Software security hardening is a challenging activity
 - Build software security program & integrate with QA
 - Domain specific knowledge required
 - Build capabilities and process following SAMM

END

CASE STUDY – ASP.NET SECURITY HARDENING

- OWASP ASP.NET Cheat Sheet
- https://www.owasp.org/index.php/.NET_Security_Cheat_Sheet

CASE STUDY – ASP.NET SECURITY HARDENING

- .NET Framework Guidance
- ASP.NET Web Forms Guidance
- ASP.NET MVC Framework Guidance

CASE STUDY – ASP.NET SECURITY HARDENING

- .NET Framework Guidance
 - **Data access**
 - Encryption
 - General guidelines

CASE STUDY – ASP.NET SECURITY HARDENING

.NET FRAMEWORK, DATA ACCESS GUIDANCE:

- Use Parameterized SQL commands for all data access, without exception.
- Do not use SqlCommand with a string parameter made up of a concatenated SQL String.
- Whitelist allowable values coming from the user. Use enums, TryParse or lookup values to assure that the data coming from the user is as expected.

CASE STUDY – ASP.NET SECURITY HARDENING

- Apply the principle of least privilege when setting up the Database User in your database of choice. The database user should only be able to access items that make sense for the use case.
- Use of the Entity Framework is a very effective SQL injection prevention mechanism. When using SQL Server, prefer integrated authentication over SQL authentication.
- Use Always Encrypted where possible for sensitive data (SQL Server 2016 and SQL Azure)

CASE STUDY – ASP.NET SECURITY HARDENING

.NET FRAMEWORK, GENERAL GUIDANCE:

- Lock down the config file.
- Remove all aspects of configuration that are not in use.
- Encrypt sensitive parts of the web.config using `aspnet_regiis -pe`
- For Click Once applications the .Net Framework should be upgraded to use version 4.6.2 to ensure TLS 1.1/1.2 support.

CASE STUDY – ASP.NET SECURITY HARDENING

- **ASP.NET Web Forms Guidance**
 - HTTPS & some general configuration
 - HTTP validation & encoding
 - Forms authentication

CASE STUDY – ASP.NET SECURITY HARDENING

- **ASP.NET MVC Guidance**
 - ASP.NET MVC (Model-View-Controller) is a contemporary web application framework that uses more standardized HTTP communication
 - Based on OWASP Top 10

END

CASE STUDY – PHP SECURITY HARDENING

- PHP Security Guidelines
- <https://docs.php.earth/security/intro/>

CASE STUDY – PHP SECURITY HARDENING

1. Cross site scripting (XSS)
2. Injections
 - SQL injection
 - Directory traversal
 - (path injection)
 - Command injection
 - Code injection
3. Cross site request forgery (XSRF/CSRF)
4. Public files

CASE STUDY – PHP SECURITY HARDENING

5. Passwords
6. Uploading files
7. Session hijacking
8. Remote file inclusion
9. PHP configuration
 - Error reporting
 - Exposing PHP version
 - Remote files
 - Open_basedir
 - Session settings

CASE STUDY – PHP SECURITY HARDENING

10. Use HTTPS

11. Things not listed

CASE STUDY – PHP SECURITY HARDENING

9. PHP Configuration

Always keep the installed PHP version updated. You can use [versionscan](#) to check for possible vulnerabilities of your PHP version. Update open source libraries and applications, and keep your web server well maintained.

CASE STUDY – PHP SECURITY HARDENING

9. PHP Configuration...

Here are some of the important settings from php.ini that you should check out. You can also use [iniscan](#) to scan your php.ini files for best security practices.

CASE STUDY – PHP SECURITY HARDENING

9. Error Reporting

In your production environment, you must always turn off displaying errors to the screen. If errors occur in your application and they are visible to the outside world, an attacker could get valuable data for attacking your application.

CASE STUDY – PHP SECURITY HARDENING

```
; Disable displaying errors to screen  
display_errors = off  
; Enable writing errors to server logs  
log_errors = on
```

<https://docs.php.earth/security/intro/#php-configuration>

CASE STUDY – PHP SECURITY HARDENING

- PHP Security Guidelines
- <https://docs.php.earth/security/intro/>

END

CASE STUDY – ASP.NET MVC SECURITY HARDENING

- ASP.NET MVC Security Guidelines
- https://www.owasp.org/index.php/.NET_Security_Cheat_Sheet#ASP.NET_MVC_Guidance

CASE STUDY – ASP.NET MVC SECURITY HARDENING

- ASP.NET MVC (Model-View-Controller) is a contemporary web application framework that uses more standardized HTTP communication than the Web Forms postback model.

CASE STUDY – ASP.NET MVC SECURITY HARDENING

- The OWASP Top 10 lists the most prevalent and dangerous threats to web security in the world today and is reviewed every 3 years.
- After covering the top 10 it is generally advisable to assess for other threats or get a professional Penetration Test.

CASE STUDY – ASP.NET MVC SECURITY HARDENING

- Your approach to securing your web application should be to start at the top threat A1 below and work down, this will ensure that any time spent on security will be spent most effectively and cover the top threats first and lesser threats afterwards.

CASE STUDY – ASP.NET MVC SECURITY HARDENING

A.6 Sensitive data exposure

- DO NOT: Store encrypted passwords.
- DO: Use a strong hash to store password credentials. Use PBKDF2, BCrypt or SCrypt with at least 8000 iterations and a strong key.

CASE STUDY – ASP.NET MVC SECURITY HARDENING

A.6 Sensitive data exposure...

- DO: Enforce passwords with a minimum complexity that will survive a dictionary attack i.e. longer passwords that use the full character set (numbers, symbols and letters) to increase the entropy.

CASE STUDY – ASP.NET MVC SECURITY HARDENING

A.6 Sensitive data exposure...

- DO: Use a strong encryption routine such as AES-512 where personally identifiable data needs to be restored to it's original format. Do not encrypt passwords. Protect encryption keys more than any other asset.

CASE STUDY – ASP.NET MVC SECURITY HARDENING

A.6 Sensitive data exposure...

- Apply the following test:
Would you be happy leaving the data on a spreadsheet on a bus for everyone to read.
Assume the attacker can get direct access to your database and protect it accordingly.

CASE STUDY – ASP.NET MVC SECURITY HARDENING

A.6 Sensitive data exposure...

- DO: Use TLS 1.2 for your entire site. Get a free certificate from [StartSSL.com](https://startssl.com) or [LetsEncrypt.org](https://letsencrypt.org).
- DO NOT: Allow SSL, this is now obsolete

CASE STUDY – ASP.NET MVC SECURITY HARDENING

A.6 Sensitive data exposure...

- DO: Have a strong TLS policy (see [SSL Best Practises](#)), use TLS 1.2 wherever possible. Then check the configuration using [SSL Test](#)
- DO: Ensure headers are not disclosing information about your application.

CASE STUDY – ASP.NET MVC SECURITY HARDENING

A.6 Sensitive data exposure...

- See [HttpHeaders.cs](#) , [Dionach StripHeaders](#) or disable via web.config:

END

Security Hardening – Case Study-SharePoint

- Sharepoint 2013 STIG
- DISA, Release 3
 - 22 April, 2016
- Sharepoint server side configurations

Security Hardening – Case Study-SharePoint

STIGVIEWER WINDOW

The screenshot displays the DISA STIG Viewer 2.5.4 application. The interface includes a menu bar (File, Export, Checklist, Options, Help) and a toolbar. The main window is divided into several sections:

- STIG Explorer:** A tree view on the left showing various STIGs. The "SharePoint 2013 Security Technical Implementation Guide" is selected and highlighted in blue.
- Table:** A central table listing STIGs with columns for "Vul ID" and "Rule Name".
- General Information:** A panel on the right providing details about the selected STIG, including its title, release date, and rule title.
- Discussion:** A panel on the right containing a discussion about session time-out locks.
- Check Content:** A panel on the right providing instructions on how to check the content of the STIG.
- Fix Text:** A panel on the right providing instructions on how to fix the issues identified in the STIG.

Table Data:

Vul ID	Rule Name
V-59919	SRG-APP-000003
V-59935	SRG-APP-000006
V-59937	SRG-APP-000014
V-59939	SRG-APP-000015
V-59941	SRG-APP-000019
V-59943	SRG-APP-000039
V-59945	SRG-APP-000043
V-59947	SRG-APP-000047
V-59949	SRG-APP-000068
V-59953	SRG-APP-000090
V-59955	SRG-APP-000106
V-59957	SRG-APP-000112
V-59961	SRG-APP-000156
V-59963	SRG-APP-000180
V-59965	SRG-APP-000196
V-59967	SRG-APP-000197
V-59969	SRG-APP-000198
V-59971	SRG-APP-000200

General Information:

SharePoint 2013 Security Technical Implementation Guide :: Release: 3 Benchmark
Date: 22 Apr 2016
Rule Title: SharePoint must support the requirement

Discussion:

A session time-out lock is a temporary action taken when user stops work and moves away from the immediate physical vicinity of the information system but does not log out because of the temporary nature of the absence. Rather than relying on the user to manually lock their application...

Check Content:

Review the SharePoint server configuration to ensure a session lock occurs after 15 minutes of inactivity.

Fix Text:

Configure the SharePoint server to lock the session lock after 15 minutes of inactivity.

Security Hardening – Case Study-SharePoint

- General Information:
 - **Rule Title :** For environments requiring an Internet-facing capability, the SharePoint application server upon which Central Administration is installed, must not be installed in the DMZ.

Security Hardening – Case Study-SharePoint

- General Information:
 - **Vuln ID:** V-59995
 - **STIG ID:** SP13-00-000155
 - **Severity:** CAT II

Security Hardening – Case Study-SharePoint

- **Discussion:**
 - Information flow control regulates where information is allowed to travel within an information system and between information systems (as opposed to who is allowed to access the information) and without explicit...

Security Hardening – Case Study-SharePoint

- **... Discussion:**
 - ...regard to subsequent accesses to the information.
 - SharePoint installed Central Administrator is a powerful management tool used to administer the farm. This server should be installed on a trusted network...

Security Hardening – Case Study-SharePoint

- **... Discussion:**
 - ... segment. This server should also be used to run services rather than user-oriented web applications.

Security Hardening – Case Study-SharePoint

- **Check Content:**
 - For environments requiring an Internet-facing capability, ensure the SharePoint Central Administration application server is not in the DMZ.
 - Inspect the logical location of the server farm web front end...

Security Hardening – Case Study-SharePoint

- **Check Content:**
 - ... servers.
 - Verify the Central Administration site is not installed on a server located in a DMZ or other publicly accessible segment of the network.
 - If Central Administrator is...

Security Hardening – Case Study-SharePoint

- **Check Content:**
 - installed on a publicly facing SharePoint server, this is a finding.

Security Hardening – Case Study-SharePoint

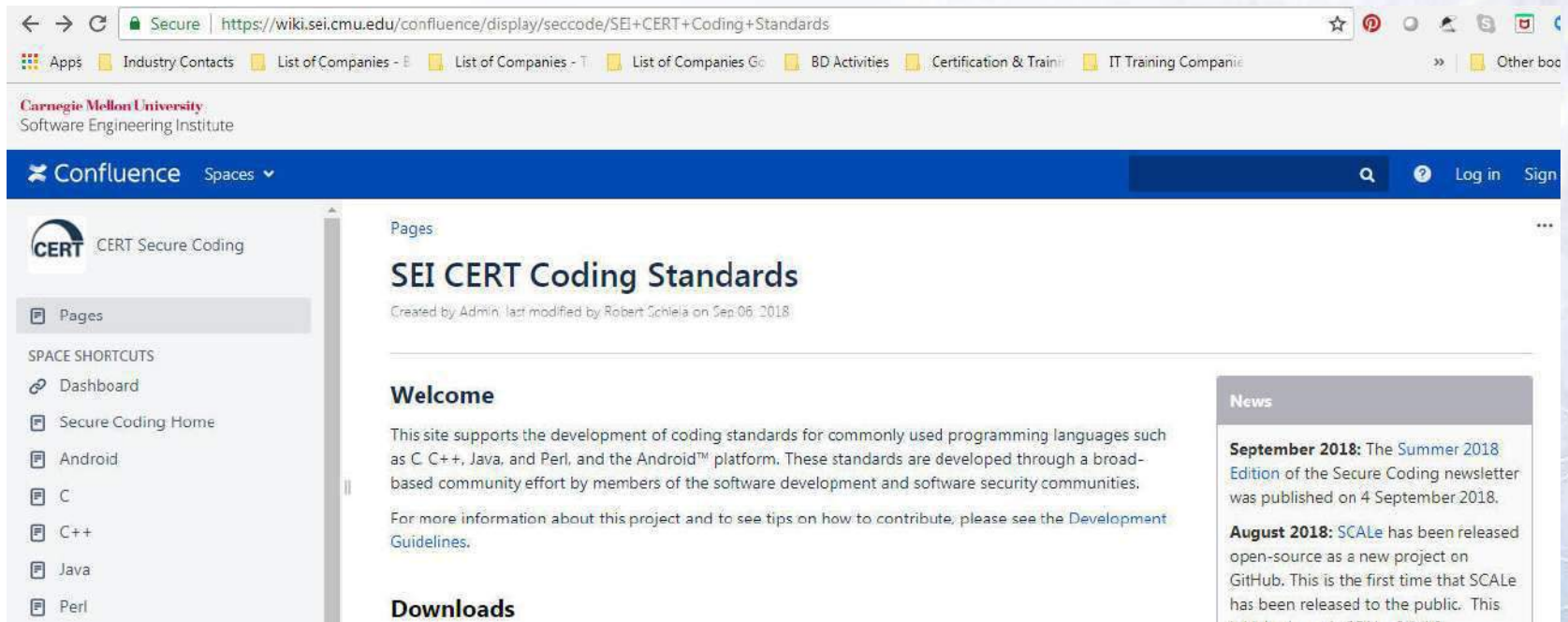
- **Fix Text:**
 - For environments requiring an Internet-facing capability, remove the SharePoint Central Administration application server upon which Central Administration is installed from the DMZ.

END

CASE STUDY – C APPLICATIONS SECURITY HARDENING

- Carnegie Mellon
Software Engineering
Institute
- <https://wiki.sei.cmu.edu/confluence/display/seccode/SEI+CERT+Coding+Standards>
- <https://wiki.sei.cmu.edu/confluence/display/c/SEI+CERT+C+Coding+Standard>

CASE STUDY – C APPLICATIONS SECURITY HARDENING



The screenshot shows a web browser displaying the SEI CERT Coding Standards page on Confluence. The browser's address bar shows the URL: <https://wiki.sei.cmu.edu/confluence/display/seccode/SEI+CERT+Coding+Standards>. The page header includes the Carnegie Mellon University Software Engineering Institute logo and the Confluence navigation bar. The main content area is titled "SEI CERT Coding Standards" and includes a "Welcome" section with text about the site's purpose and a "Downloads" section. A "News" sidebar on the right lists recent updates, including the September 2018 newsletter and the August 2018 release of SCALE.

Pages

SEI CERT Coding Standards

Created by Admin, last modified by Robert Schielea on Sep 06, 2018

Welcome

This site supports the development of coding standards for commonly used programming languages such as C, C++, Java, and Perl, and the Android™ platform. These standards are developed through a broad-based community effort by members of the software development and software security communities.

For more information about this project and to see tips on how to contribute, please see the [Development Guidelines](#).

Downloads

News

September 2018: The Summer 2018 Edition of the Secure Coding newsletter was published on 4 September 2018.

August 2018: SCALE has been released open-source as a new project on GitHub. This is the first time that SCALE has been released to the public. This initial release is SCALE 2.1.0.

<https://wiki.sei.cmu.edu/confluence/display/seccode/SEI+CERT+Coding+Standards>

CASE STUDY – C APPLICATIONS SECURITY HARDENING

- There are existing compiler [implementations](#) that allow const-qualified objects to be modified without generating a warning message.

CASE STUDY – C APPLICATIONS SECURITY HARDENING

- Avoid casting away const qualification because doing so makes it possible to modify const-qualified objects without issuing diagnostics.

CASE STUDY – C APPLICATIONS SECURITY HARDENING

Noncompliant Code Example

This noncompliant code example allows a constant object to be modified:

```
const int **ipp;
int *ip;
const int i = 42;

void func(void) {
    ipp = &ip; /* Constraint violation */
    *ipp = &i; /* Valid */
    *ip = 0;   /* Modifies constant i (was 42) */
}
```

CASE STUDY – C APPLICATIONS SECURITY HARDENING

- The first assignment is unsafe because it allows the code that follows it to attempt to change the value of the const object i.

CASE STUDY – C APPLICATIONS SECURITY HARDENING

```
int **ipp;  
int *ip;  
int i = 42;  
  
void func(void) {  
    ipp = &ip; /* Valid */  
    *ipp = &i; /* Valid */  
    *ip = 0; /* Valid */  
}
```

CASE STUDY – C APPLICATIONS SECURITY HARDENING

- The compliant solution depends on the intent of the programmer. If the intent is that the value of *i* is modifiable, then it should not be declared as a constant, as in this compliant solution:

CASE STUDY – C APPLICATIONS SECURITY HARDENING

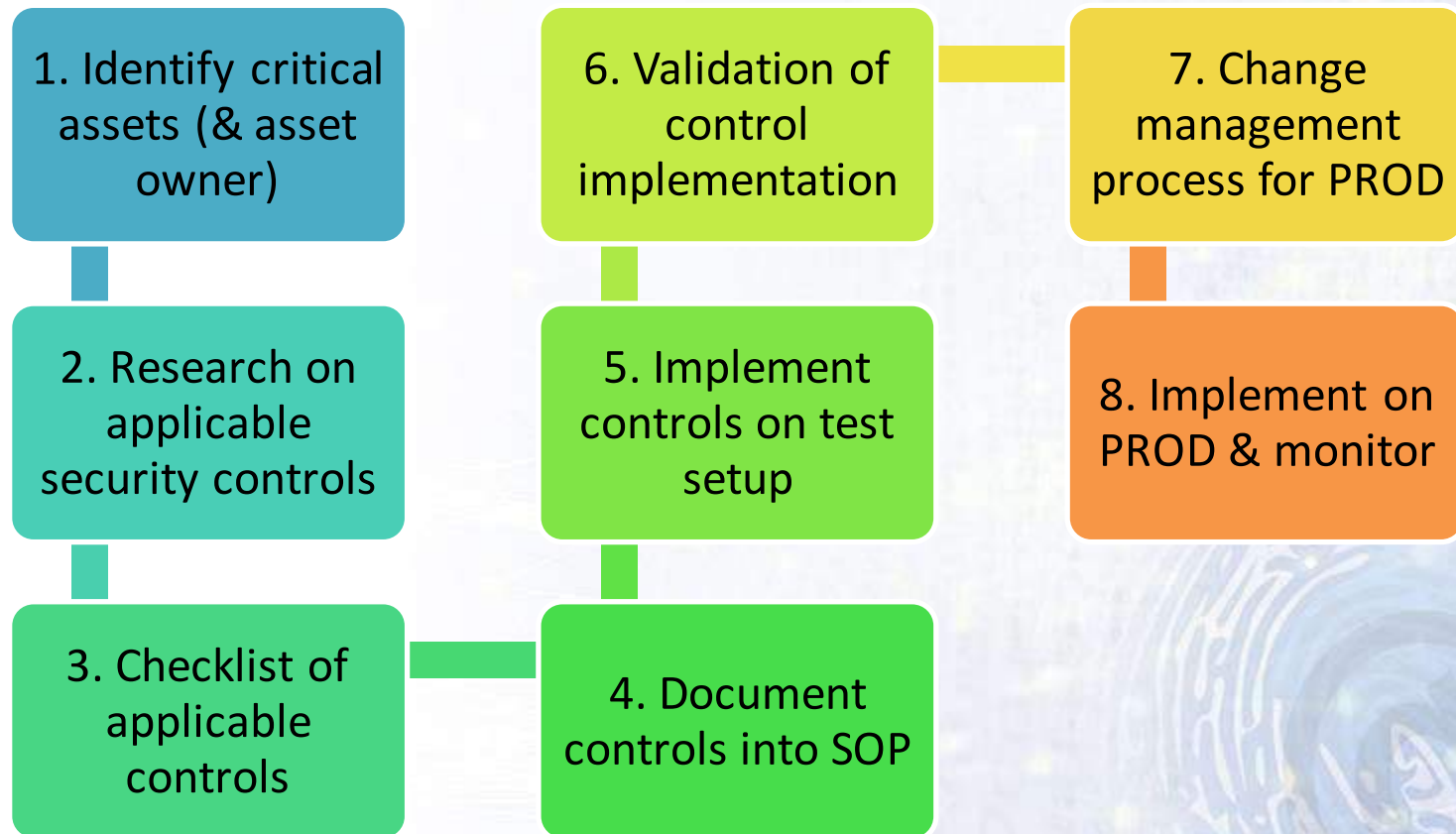
- If the intent is that the value of *i* is not meant to change, then do not write noncompliant code that attempts to modify it.
- Risk Assessment
- Automated detection
- Related vulnerabilities

END

CASE STUDY – C++ APPLICATIONS SECURITY HARDENING

- Carnegie Mellon
Software Engineering
Institute
- <https://wiki.sei.cmu.edu/confluence/pages/viewpage.action?pageId=88046682>

CASE STUDY – C++ APPLICATIONS SECURITY HARDENING



CASE STUDY – C++ APPLICATIONS SECURITY HARDENING

- Rule 01. Declarations and Initialization (DCL)
- Rule 02. Expressions (EXP)
- Rule 03. Integers (INT)
- Rule 04. Containers (CTR)
- Rule 05. Characters and Strings (STR)

CASE STUDY – C++ APPLICATIONS SECURITY HARDENING

- Rule 06. Memory Management (MEM)
- Rule 07. Input Output (FIO)
- Rule 08. Exceptions and Error Handling (ERR)Page:
- Rule 09. Object Oriented Programming (OOP)
- Rule 10. Concurrency (CON)

CASE STUDY – C++ APPLICATIONS SECURITY HARDENING

- Rule 10. Concurrency (CON)
- [CON50-CPP. Do not destroy a mutex while it is locked](#)

CASE STUDY – C++ APPLICATIONS SECURITY HARDENING

- Mutex objects are used to protect shared data from being concurrently accessed. If a mutex object is destroyed while a thread is blocked waiting for the lock, critical sections and shared data are no longer protected.

CASE STUDY – C++ APPLICATIONS SECURITY HARDENING

- The C++ Standard, [thread.mutex.class], paragraph 5 [[ISO/IEC 14882-2014](#)], states the following:
- The behavior of a program is undefined if it destroys a mutex object owned by any thread or a thread terminates while owning a mutex object.

CASE STUDY – C++ APPLICATIONS SECURITY HARDENING

```
#include <mutex>
#include <thread>

const size_t maxThreads = 10;

void do_work(size_t i, std::mutex *pm) {
    std::lock_guard<std::mutex> lk(*pm);

    // Access data protected by the lock.
}

void start_threads() {
    std::thread threads[maxThreads];
    std::mutex m;

    for (size_t i = 0; i < maxThreads; ++i) {
        threads[i] = std::thread(do_work, i, &m);
    }
}
```

CASE STUDY – C++ APPLICATIONS SECURITY HARDENING

- **Non-Compliant Code Example:**
- This noncompliant code example creates several threads that each invoke the `do_work()` function, passing a unique number as an ID.
- Unfortunately, this code contains a race condition, allowing the mutex to be destroyed

CASE STUDY – C++ APPLICATIONS SECURITY HARDENING

- ... while it is still owned, because `start_threads()` may invoke the mutex's destructor before all of the threads have exited.

CASE STUDY – C++ APPLICATIONS SECURITY HARDENING

```
#include <mutex>
#include <thread>

const size_t maxThreads = 10;

void do_work(size_t i, std::mutex *pm) {
    std::lock_guard<std::mutex> lk(*pm);

    // Access data protected by the lock.
}

std::mutex m;

void start_threads() {
    std::thread threads[maxThreads];

    for (size_t i = 0; i < maxThreads; ++i) {
        threads[i] = std::thread(do_work, i, &m);
    }
}
```

CASE STUDY – C++ APPLICATIONS SECURITY HARDENING

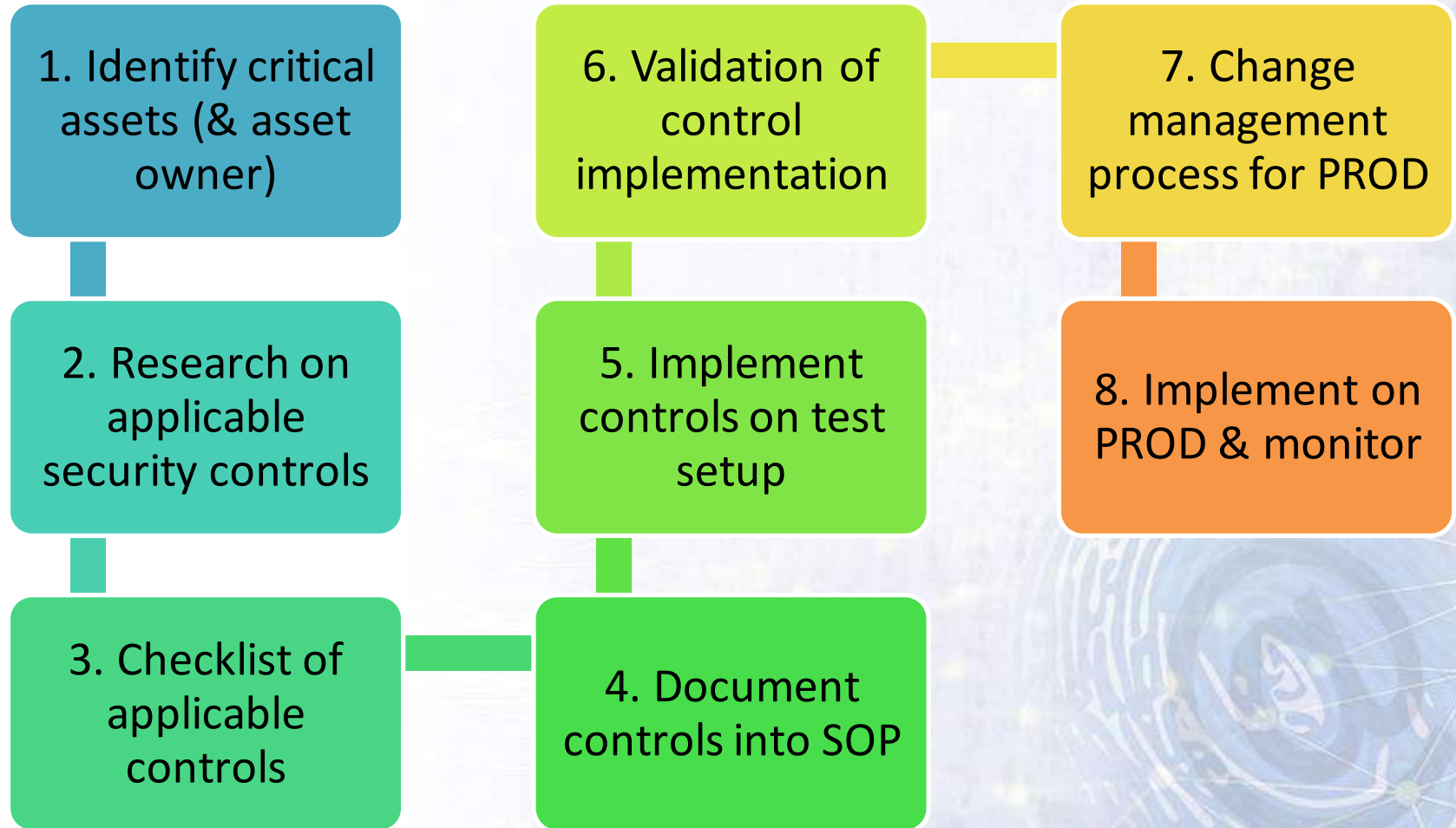
- **Compliant Code Example:**
- This compliant solution eliminates the race condition by extending the lifetime of the mutex.

END

CASE STUDY – JAVA APPLICATIONS SECURITY HARDENING

- Carnegie Mellon
Software Engineering
Institute
- <https://wiki.sei.cmu.edu/confluence/display/java/SEI+CERT+Oracle+Coding+Standard+for+Java>

CASE STUDY – JAVA APPLICATIONS SECURITY HARDENING



CASE STUDY – JAVA APPLICATIONS SECURITY HARDENING

- ☐ Rule 00. Input Validation and Data Sanitization (IDS)
- ☐ Rule 01. Declarations and Initialization (DCL)
- ☐ Rule 02. Expressions (EXP)
- ☐ Rule 03. Numeric Types and Operations (NUM)
- ☐ Rule 04. Characters and Strings (STR)
- ☐ Rule 05. Object Orientation (OBJ)
- ☐ Rule 06. Methods (MET)
- ☐ Rule 07. Exceptional Behavior (ERR)
- ☐ Rule 08. Visibility and Atomicity (VNA)
- ☐ Rule 09. Locking (LCK)
- ☐ Rule 10. Thread APIs (THI)
- ☐ Rule 11. Thread Pools (TPS)
- ☐ Rule 12. Thread-Safety Miscellaneous (TSM)
- ☐ Rule 13. Input Output (FIO)
- ☐ Rule 14. Serialization (SER)
- ☐ Rule 15. Platform Security (SEC)
- ☐ Rule 16. Runtime Environment (ENV)
- ☐ Rule 17. Java Native Interface (JNI)
- ☐ Rule 49. Miscellaneous (MSC)
- ☐ Rule 50. Android (DRD)

Recommendations

- ☐ Rec. 00. Input Validation and Data Sanitization (IDS)
- ☐ Rec. 01. Declarations and Initialization (DCL)
- ☐ Rec. 02. Expressions (EXP)
- ☐ Rec. 03. Numeric Types and Operations (NUM)
- ☐ Rec. 04. Characters and Strings (STR)
- ☐ Rec. 05. Object Orientation (OBJ)
- ☐ Rec. 06. Methods (MET)
- ☐ Rec. 07. Exceptional Behavior (ERR)
- ☐ Rec. 13. Input Output (FIO)
- ☐ Rec. 15. Platform Security (SEC)
- ☐ Rec. 18. Concurrency (CON)
- ☐ Rec. 49. Miscellaneous (MSC)

CASE STUDY – JAVA APPLICATIONS SECURITY HARDENING

- Rule 7
- [ERR02-J. Prevent exceptions while logging data](#)
- Exceptions that are thrown while logging is in progress can prevent successful logging unless special care is taken. Failure to account for exceptions during the logging process can

CASE STUDY – JAVA APPLICATIONS SECURITY HARDENING

- ... cause security [vulnerabilities](#), such as allowing an attacker to conceal critical security exceptions by preventing them from being logged. Hence, programs must ensure that data logging continues to operate correctly even when exceptions are thrown

CASE STUDY – JAVA APPLICATIONS SECURITY HARDENING

- ... during the logging process.

CASE STUDY – JAVA APPLICATIONS SECURITY HARDENING

```
try {  
    // ...  
} catch (SecurityException se) {  
    System.err.println(se);  
    // Recover from exception  
}
```

CASE STUDY – JAVA APPLICATIONS SECURITY HARDENING

- **Non-compliant Code Example:**
- This noncompliant code example writes a critical security exception to the standard error stream:

CASE STUDY – JAVA APPLICATIONS SECURITY HARDENING

- Writing such exceptions to the standard error stream is inadequate for logging purposes. First, the standard error stream may be exhausted or closed, preventing recording of subsequent exceptions. Second, the trust level of the standard error stream may be

CASE STUDY – JAVA APPLICATIONS SECURITY HARDENING

- ...insufficient for recording certain security-critical exceptions or errors without leaking sensitive information. If an I/O error were to occur while writing the security exception, the catch block would throw an IOException and the

CASE STUDY – JAVA APPLICATIONS SECURITY HARDENING

- ... critical security exception would be lost. Finally, an attacker may disguise the exception so that it occurs with several other innocuous exceptions.

CASE STUDY – JAVA APPLICATIONS SECURITY HARDENING

```
try {  
    // ...  
} catch(SecurityException se) {  
    logger.log(Level.SEVERE, se);  
    // Recover from exception  
}
```

CASE STUDY – JAVA APPLICATIONS SECURITY HARDENING

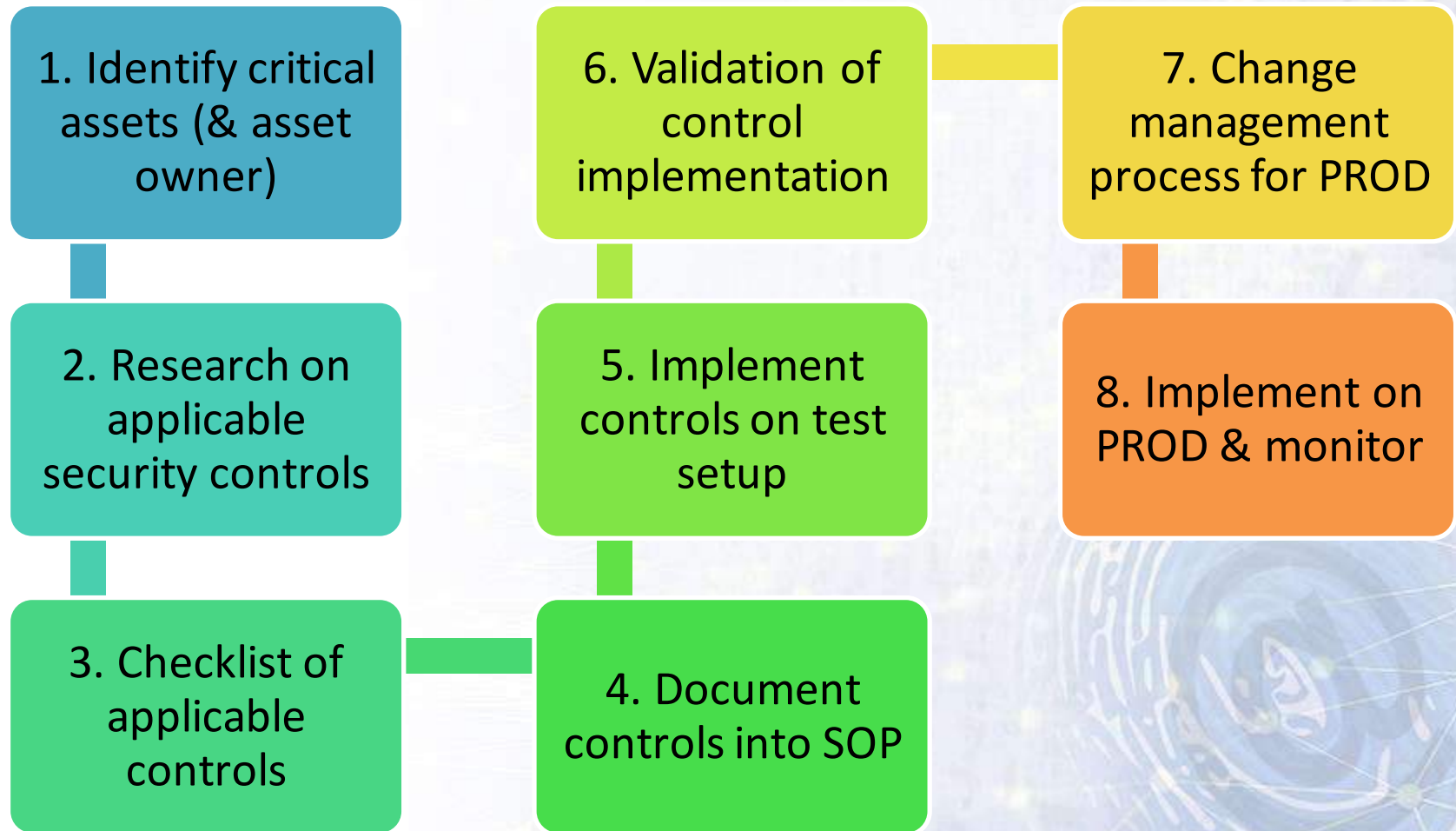
- **Compliant Solution:**
- This compliant solution uses `java.util.logging.Logger`, the default logging API provided by JDK 1.4 and later. Use of other compliant logging mechanisms, such as `log4j`, is also permitted.
- Typically, only one logger is required for the entire program.

END

CASE STUDY – PERL APPLICATIONS SECURITY HARDENING

- Carnegie Mellon
Software Engineering
Institute
- <https://wiki.sei.cmu.edu/confluence/display/perl/SEI+CERT+Perl+Coding+Standard>

CASE STUDY – PERL APPLICATIONS SECURITY HARDENING



CASE STUDY – PERL APPLICATIONS SECURITY HARDENING

Rules

- ≡ Rule 01. Input Validation and Data Sanitization (IDS)
- ≡ Rule 02. Declarations and Initialization (DCL)
- ≡ Rule 03. Expressions (EXP)
- ≡ Rule 04. Integers (INT)
- ≡ Rule 05. Strings (STR)
- ≡ Rule 06. Object-Oriented Programming (OOP)
- ≡ Rule 07. File Input and Output (FIO)
- ≡ Rule 50. Miscellaneous (MSC)

Recommendations

- ≡ Rec. 01. Input Validation and Data Sanitization (IDS)
- ≡ Rec. 02. Declarations and Initialization (DCL)
- ≡ Rec. 03. Expressions (EXP)
- ≡ Rec. 04. Integers (INT)
- ≡ Rec. 05. Strings (STR)
- ≡ Rec. 06. Object-Oriented Programming (OOP)
- ≡ Rec. 07. File Input and Output (FIO)
- ≡ Rec. 50. Miscellaneous (MSC)

CASE STUDY – PERL APPLICATIONS SECURITY HARDENING

- [Rule 1](#)
- [IDS30-PL. Exclude user input from format strings](#)

CASE STUDY – PERL APPLICATIONS SECURITY HARDENING

- Never call any formatted I/O function with a format string containing user input.
- An attacker who can fully or partially control the contents of a format string can crash the Perl interpreter or cause a denial of service. She can also modify values, perhaps by using

CASE STUDY – PERL APPLICATIONS SECURITY HARDENING

- ... the %n|| conversion specifier, and use these values to divert control flow. Their capabilities are not as strong as in C [[Seacord 2005](#)]; nonetheless the danger is sufficiently great that the formatted output functions {sprintf() and printf()} should never be passed unsanitized format strings.

CASE STUDY – PERL APPLICATIONS SECURITY HARDENING

```
my $host = `hostname`;
chop($host);
my $prompt = "$ENV{USER}@$host";

sub validate_password {
    my ($password) = @_ ;
    my $is_ok = ($password eq "goodpass");
    printf "$prompt: Password ok? %d\n", $is_ok;
    return $is_ok;
};

if (validate_password( $ARGV[0])) {
    print "$prompt: access granted\n";
} else {
    print "$prompt: access denied\n";
};
```


CASE STUDY – PERL APPLICATIONS SECURITY HARDENING

- This **noncompliant code example** tries to authenticate a user by having the user supply a password and granting access only if the password is correct.

CASE STUDY – PERL APPLICATIONS SECURITY HARDENING

```
sub validate_password {  
    my ($password) = @_;  
    my $is_ok = ($password eq "goodpass");  
    print "$prompt: Password ok? $is_ok\n";  
    return $is_ok;  
};  
  
# ...
```

CASE STUDY – PERL APPLICATIONS SECURITY HARDENING

- This **compliant code example** avoids the use of `printf()`, since `print()` provides sufficient functionality.

END

Case Study Security Hardening – Android

- CIS Benchmarks case study (Google Android 7)

Case Study Security Hardening – Android

CIS Google Android 7 Benchmark

v1.0.0 - 01-24-2017

- January 24, 2017
- 87 pages PDF doc

Case Study Security Hardening – Android

- 1.15 Ensure Android Device Manager is set to Enabled (Not Scored)
- Profile applicability:
 - Level 2

Case Study Security Hardening – Android

- 1.15 *Ensure Android Device Manager is set to Enabled (Not Scored)*
 - **Description:** Setup **Android Device Manager** as a Device Administrator.

Case Study Security Hardening – Android

- **Rationale:**
 - If you lose your Android device, you could use Android Device Manager to find your device and also ring, lock, or erase your device data remotely.

Case Study Security Hardening – Android

- **Audit:** Follow the below steps to verify that Android Device Manager is enabled:
 1. Tap the System Settings Gear Icon.
 2. Scroll to Personal.
 3. Tap Security.
 4. Scroll to Device administration;

Case Study Security Hardening – Android

- **Audit: ...**
 5. Tap Device administrators.
 6. Verify that Android Device Manager is enabled.

Case Study Security Hardening – Android

- **Remediation:** Follow the below steps to enable Android Device Manager:
 1. Tap the System Settings Gear Icon.
 2. Scroll to Personal.
 3. Tap Security.
 4. Scroll to Device administration;

Case Study Security Hardening – Android

- **Remediation:...**

5. Tap Device administrators.

6. Tap Android Device Manager.

7. Tap Activate this device administrator.

Case Study Security Hardening – Android

- **Impact:**
 - Google may track your device location anytime.

Case Study Security Hardening – Android

- **Default Value:**
 - By default, Android Device Manager is not enabled.

Case Study Security Hardening – Android

- References:
 - <https://support.google.com/pixelphone/answer/3265955>

END

Case Study Security Hardening – Apple IOS 10

- CIS Benchmarks case study (Apple IOS 10)

Case Study Security Hardening – Apple iOS 10

CIS Apple iOS 10 Benchmark

v2.0.0 - 05-15-2017

- May 15, 2017
- 138 pages PDF doc

Case Study Security Hardening – Apple IOS 10

- 3.2.1.12 (L2) Ensure 'Allow modifying cellular data app settings' is set to 'Disabled' (Not Scored)
- Profile applicability:
 - Level 2 -
Institutionally Owned
Devices

Case Study Security Hardening – Apple IOS 10

- 3.2.1.12 (L2) Ensure 'Allow modifying cellular data app settings' is set to 'Disabled' (Not Scored)
 - **Description:** This recommendation pertains to modifying the use of cellular data by apps.

Case Study Security Hardening – Apple IOS 10

- **Rationale:**
 - It is appropriate for an institution to have remote locating and erasure capability with their devices. Forcing cellular data to remain active is a means of supporting this goal.

Case Study Security Hardening – Apple iOS 10

- **Audit:**
 - From the Configuration Profile:
 1. Open Apple Configurator
 2. Open the Configuration Profile
 3. In the left windowpane, click on the Restrictions tab.
 4. In the right windowpane, verify that under the tab...

Case Study Security Hardening – Apple IOS 10

- **Audit: ...**
 - ... Functionality, that the checkbox for Allow modifying cellular data app settings is unchecked.

Case Study Security Hardening – Apple iOS 10

- **Audit: ...**

... Or, from the device:

1. Tap Settings.
2. Tap General.
3. Tap Profile.
4. Tap <_Profile Name_>.
5. Tap Restrictions.
6. Confirm Changing app cellular data usage not allowed is displayed.

Case Study Security Hardening – Apple IOS 10

- **Remediation:**

1. Open Apple Configurator.
2. Open the Configuration Profile.
3. In the left windowpane, click on the Restrictions tab;

Case Study Security Hardening – Apple IOS 10

- **Remediation...:**

4. In the right windowpane, under the tab Functionality, uncheck the checkbox for **Allow modifying cellular data app settings**.
5. Deploy the Configuration Profile.

Case Study Security Hardening – Apple IOS 10

- **CIS Controls:**
 - 5.1 Minimize And Sparingly Use Administrative Privileges Minimize administrative privileges and only use administrative accounts when they are required;

Case Study Security Hardening – Apple IOS 10

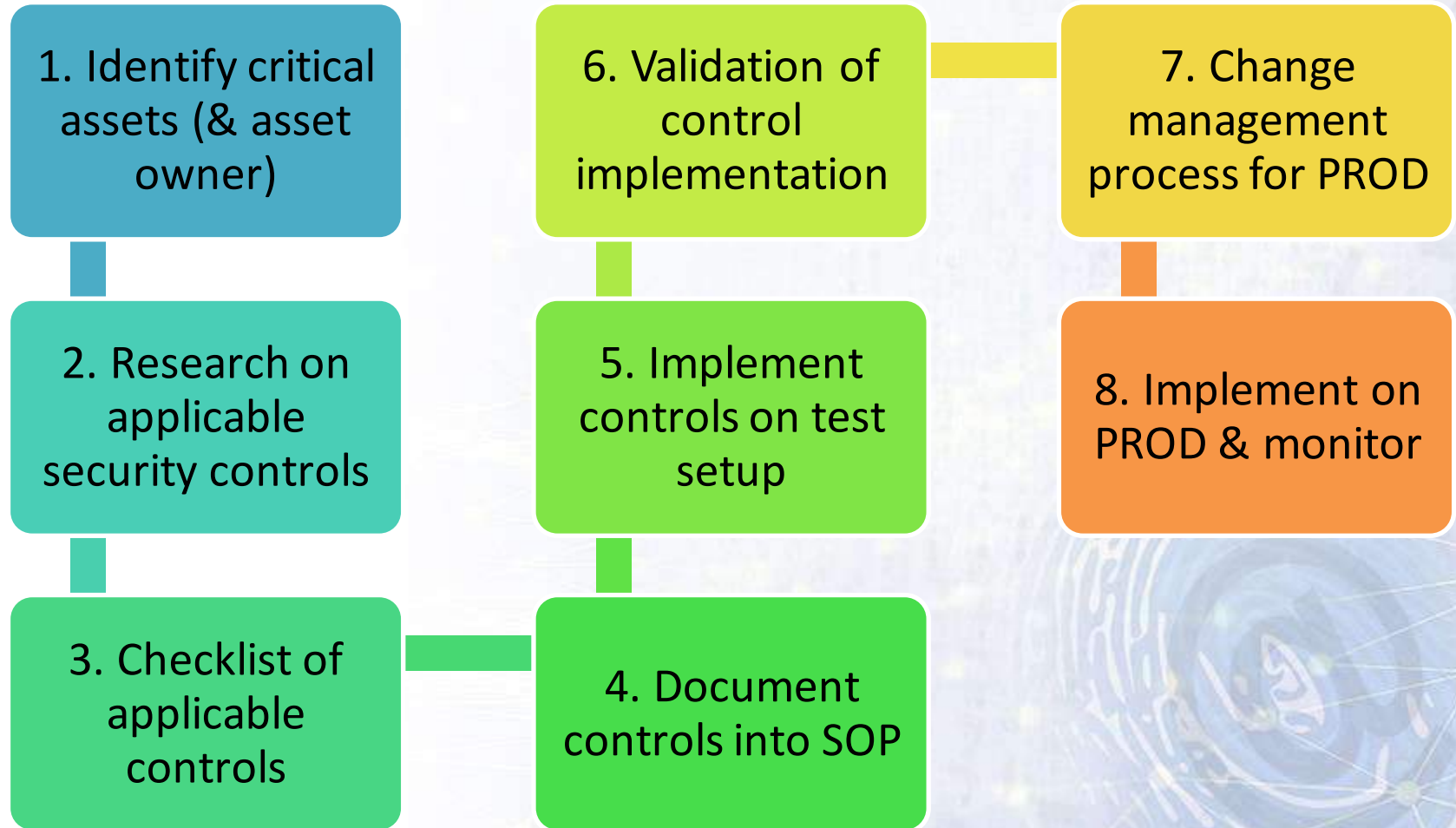
- **CIS Controls:**
 - ... Implement focused auditing on the use of administrative privileged functions and monitor for anomalous behavior

END

CASE STUDY – ASTERISK VOIP SECURITY HARDENING

- <http://www.ipcomms.net/asteriskblog/1-11-steps-to-secure-your-asterisk-pbx>

CASE STUDY – PERL APPLICATIONS SECURITY HARDENING



CASE STUDY – ASTERISK VOIP SECURITY HARDENING

1. Physically secure your IP PBX and network hardware
 - The first step to security of your system

CASE STUDY – ASTERISK VOIP SECURITY HARDENING

2. Never, Never, Never use the default passwords on any system. (Use Strong Passwords)

- This will stop most of the attacks as hackers use weak passwords to break in

CASE STUDY – ASTERISK VOIP SECURITY HARDENING

3. Never use the same Username and password on your extensions

- **“This is another VERY common issue, especially within the Asterisk community. Using password 101 for extension 101 is asking for big trouble. DON’T DO IT!”**

CASE STUDY – ASTERISK VOIP SECURITY HARDENING

3. Never use the same Username and password on your extensions

- **“This is another VERY common issue, especially within the Asterisk community. Using password 101 for extension 101 is asking for big trouble. DON’T DO IT!”**

CASE STUDY – ASTERISK VOIP SECURITY HARDENING

4. Place your PBX behind a Firewall

- **Use VPNs for remote access and limit to specific IP addresses**
- **Allow access on ports which are absolutely necessary**
- **Disable anonymous WAN requests (ICMP or PING) access to your IP PBX**

CASE STUDY – ASTERISK VOIP SECURITY HARDENING

5. Use the “permit=” and “deny=” lines in sip.conf
 - “Use the “permit=” and “deny=” lines in sip.conf to only allow a small range of IP addresses access to extension/user in your sip.conf file. This is true even if you decide to allow inbound calls from “anywhere” (default),

CASE STUDY – ASTERISK VOIP SECURITY HARDENING

5. ...it won't let those users reach any authenticated elements!”

CASE STUDY – ASTERISK VOIP SECURITY HARDENING

6. Keep inbound and outbound routing separate (asterisk)

- This is probably the biggest cause and source of toll fraud. By keeping your inbound call routing in a different context than your outbound routing, if an intruder does happen to...

CASE STUDY – ASTERISK VOIP SECURITY HARDENING

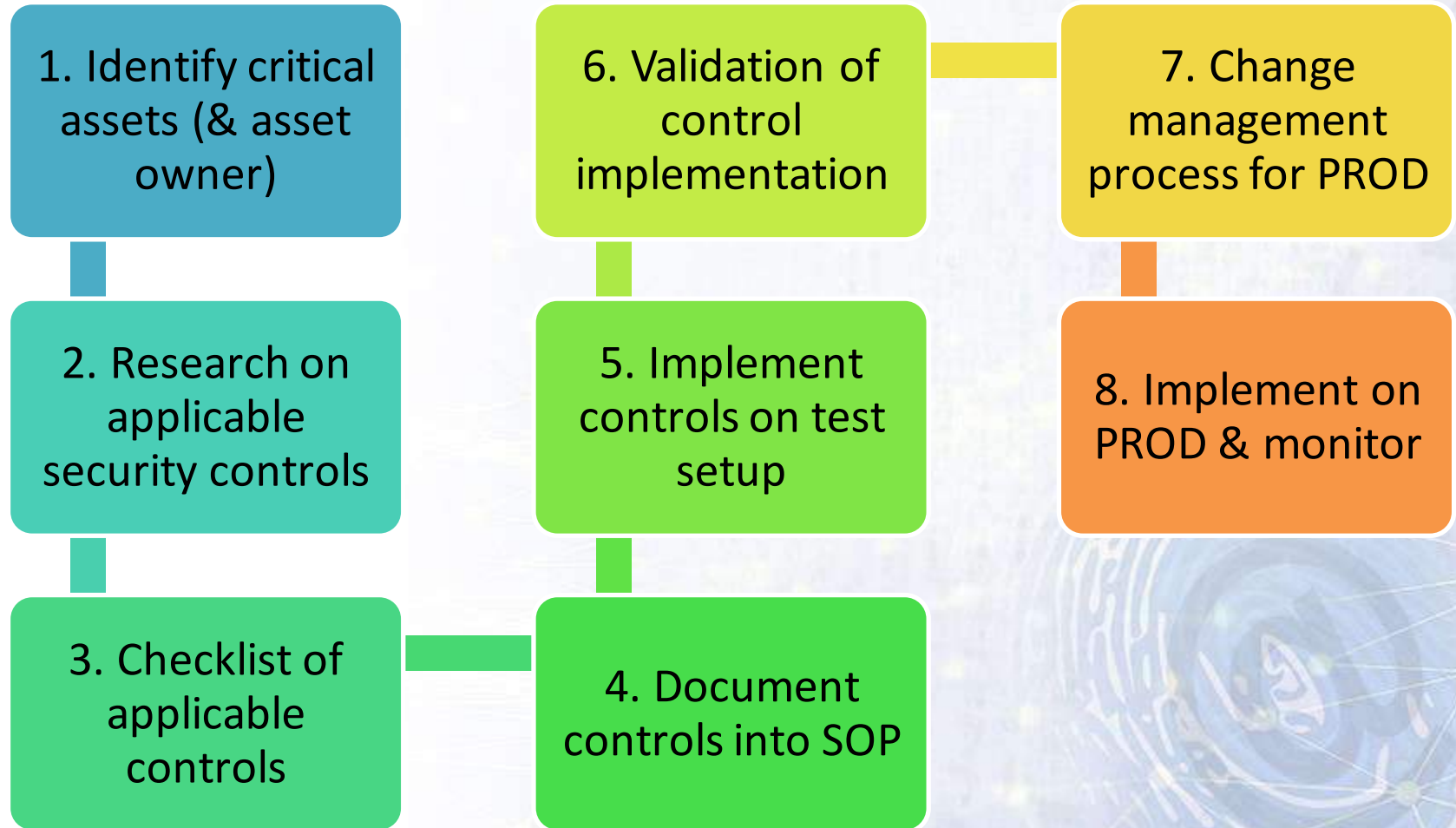
6. ... make it into your system, he can't get back out again.

END

CASE STUDY – ASTERISK VOIP SECURITY HARDENING (2)

- <http://www.ipcomms.net/asteriskblog/1-11-steps-to-secure-your-asterisk-pbx>

CASE STUDY – ASTERISK VOIP SECURITY HARDENING (2)



CASE STUDY – ASTERISK VOIP SECURITY HARDENING (2)

7. Limit registration by extensions to your local subnet.

- Restrict the IP addresses your extensions can register onto the local subnet. Asterisk PBXs can use the ACL (permit/deny) in SIP.conf to block IP addresses. This can fend off brute force registration attempts.

CASE STUDY – ASTERISK VOIP SECURITY HARDENING (2)

8. Disable channels and services that are not in use
 - Disable channels that you aren't using like skinny and MGCP. For Asterisk PBXs, you can “unload” these modules in the `/etc/modules.conf` file

CASE STUDY – ASTERISK VOIP SECURITY HARDENING (2)

9. Make it harder for sip scanners (Set “alwaysauthreject=yes”)
- Set “alwaysauthreject=yes” in your sip configuration file. What this does is prevent Asterisk from telling a sip scanner which extensions are valid by rejecting authentication requests

CASE STUDY – ASTERISK VOIP SECURITY HARDENING (2)

- ... on existing usernames with the same rejection details as with nonexistent usernames. If they can't find you they can't hack you!
- Another way to make it hard for SIP scanners is to install a SIP port firewall. This will block

CASE STUDY – ASTERISK VOIP SECURITY HARDENING (2)

- ...“scanning” of port 5060 and 5061 and can disable the attempting endpoint for a specific time when it detects a violation.

CASE STUDY – ASTERISK VOIP SECURITY HARDENING (2)

10. Limit and restrict routing and phone number dial plans

- Restrict calling to high-cost calling destination and don't allow calling to 0900 + Premium numbers)

CASE STUDY – ASTERISK VOIP SECURITY HARDENING (2)

11. Audit your system security regularly

END

Version Control For IT Assets

- Benefits of version control
- Security implications

Version Control For IT Assets

- Benefits of version control
 - http://its.unl.edu/best_practices/version-management

Version Control For IT Assets

- Benefits of version control
 - 1. Organized, coordinated management of changes to software assets by one or many individuals, some of whom may be geographically dispersed

<http://its.unl.edu/bestpractices/version-management>

Version Control For IT Assets

- Benefits of version control
 - 2. Organized, coordinated management of changes to software assets for emergency hot-fixes, routine maintenance, upgrades...

<http://its.unl.edu/bestpractices/version-management>

Version Control For IT Assets

- Benefits of version control
 - 2. ... & new features with potentially overlapping dev timeframes (e.g., work on new features occurs simultaneously with work on routine maintenance and/or hot-fixes)

<http://its.unl.edu/bestpractices/version-management>

Version Control For IT Assets

- Benefits of version control
 - 3. An auditable change history (e.g., what changed, when, and by whom)

<http://its.unl.edu/bestpractices/version-management>

Version Control For IT Assets

- Benefits of version control
 - 4. A reliable master copy of what assets are currently in production

<http://its.unl.edu/bestpractices/version-management>

Version Control For IT Assets

- Benefits of version control
 - 5. A reliable master copy of assets from which to build and/or configure the production environment

<http://its.unl.edu/bestpractices/version-management>

Version Control For IT Assets

- Benefits of version control
 - 6. Reliable copies of previous production versions of assets

<http://its.unl.edu/bestpractices/version-management>

Version Control For IT Assets

- Benefits of version control
 - 7. Ability to see the specific differences between distinct versions of a given asset

<http://its.unl.edu/bestpractices/version-management>

Version Control For IT Assets

- Security controls:
 - Access control measures
 - Privileged management
 - Backups

END

Version Control Best Practices

- Version control best practices
 - <https://intland.com/blog/source-control-management-best-practices/>

Version Control Best Practices

1. Starting with the basics, choose a source control system.
2. Keep your source code in source control (but not files generated / compiled from it).
3. Ensure the working file is from the latest version of the source file.

<https://intland.com/blog/sdlc/source-control-management-best-practices/>

Version Control Best Practices

4. Only Check-out the file being worked upon.
5. Check in immediately after alterations are completed.
6. Review every change before committing, utilize the diff function!
7. Commit often, – every commit provides a rollback position.

<https://intland.com/blog/sdlc/source-control-management-best-practices/>

Version Control Best Practices

8. Make extensive, – detailed notes in the check-in comments about why the changes were made.
9. Developers must commit their own changes (only).

<https://intland.com/blog/sdlc/source-control-management-best-practices/>

Version Control Best Practices

10. Use the ignore button for files that should not be committed, consider adding pre-commit filters to prevent the wrong kinds of file (such as accidental check-in of personal user settings docs) from entering the source control

<https://intland.com/blog/sdlc/source-control-management-best-practices/>

Version Control Best Practices

END

11. Ensure external dependencies are added to the source control, a common problem where everything works great on the contributing developers system but not elsewhere because they forgot to add dependent files to the system.

<https://intland.com/blog/sdlc/source-control-management-best-practices/>

SECURITY HARDENING - SECURE SOFTWARE IMAGES

- CIS 20 CRITICAL SECURITY CONTROLS
- CONTROL 5, VERSION 7
- **Secure Configuration for Hardware and Software on Mobile Devices, Laptops, Workstations and Servers**

SECURITY HARDENING - SECURE SOFTWARE IMAGES

5.1 Establish Secure Configurations

- Maintain documented, standard security configuration standards for all authorized operating systems and software.

5.2 Maintain Secure Images

- Maintain secure images or templates for all systems in the enterprise based on the organization's approved configuration standards. Any new system deployment or existing system that becomes compromised should be

5.2 Maintain Secure Images

- ...imaged using one of those images or templates.

5.3 Securely Store Master Images

- Store the master images and templates on securely configured servers, validated with integrity monitoring tools, to ensure that only authorized changes to the images are possible.

5.4 Deploy System Configuration Management Tools

- Deploy system configuration management tools that will automatically enforce and redeploy configuration settings to systems at regularly scheduled intervals.

5.5 Implement Automated Configuration Monitoring Systems

- Utilize a Security Content Automation Protocol (SCAP) compliant configuration monitoring system to verify all security configuration elements, catalog approved exceptions, and alert..

5.5 Implement Automated Configuration Monitoring Systems

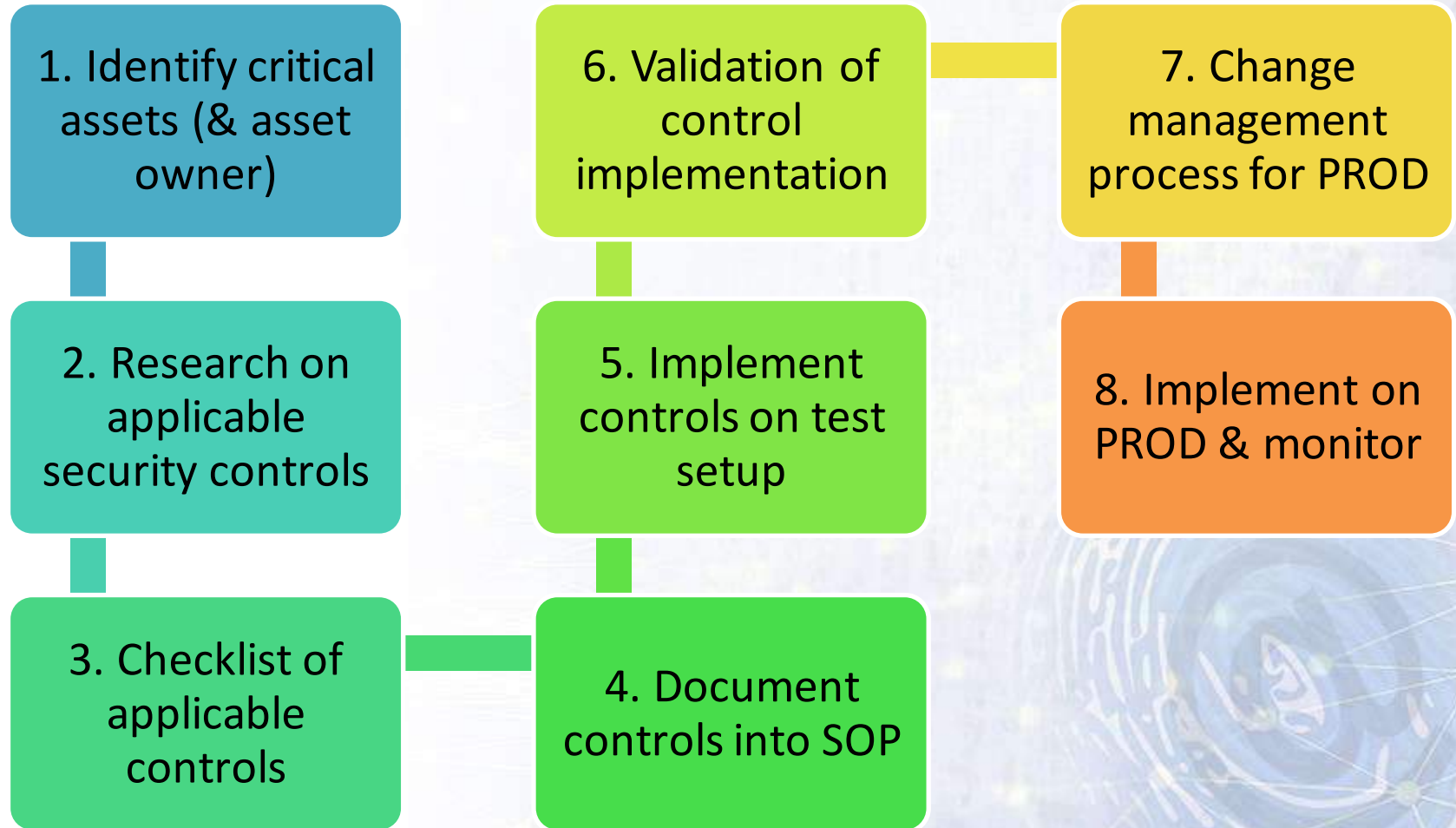
- ...when unauthorized changes occur.

END

SECURITY HARDENING – MANUAL & AUTOMATED WORK

- **Manual & Automated mechanisms for security hardening & validation**

CASE STUDY – PERL APPLICATIONS SECURITY HARDENING



SECURITY HARDENING – MANUAL & AUTOMATED WORK

- **Step 1: Scan an IT asset using Qualys compliance scan, NISSUS compliance scan, or CIS CAT PRO Tool**
- **Acquire report of failed controls**

SECURITY HARDENING – MANUAL & AUTOMATED WORK

- **Step 2: Apply the failed controls using AD (for Windows) or manually for other systems & devices**

SECURITY HARDENING – MANUAL & AUTOMATED WORK

- **Step 3: Use the automated feature of Qualys compliance scan, Nessus compliance scan or CIS CAT Pro Tool to verify that the applied controls are in place**
- **Compare the ‘before’ and ‘after’ report**

SECURITY HARDENING – MANUAL & AUTOMATED WORK

- **Step 4: manually verify if any discrepancy is found (control should be in place but not being validated by the tool)**

SECURITY HARDENING – MANUAL & AUTOMATED WORK

- **Step 5: For any system or device for which the Qualys compliance scan, Nessus compliance scan, or CIS CAT Pro Tool scan cannot be performed, conduct the validation of control implementation manually**

SECURITY HARDENING – MANUAL & AUTOMATED WORK

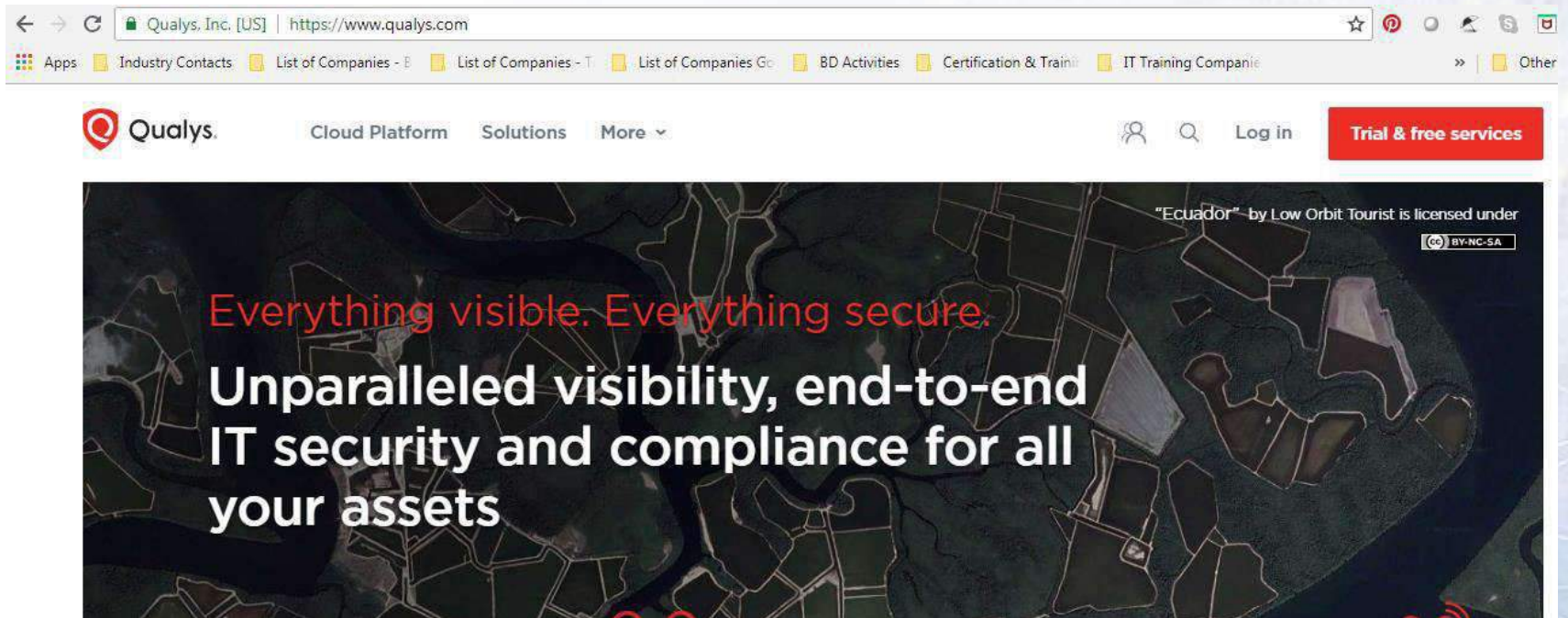
- Use sampling where necessary during manual validation work to reduce workload
- For example, 15-20 % of assets may be checked at random
- Or 15-20% of controls may be checked on an asset

END

QUALYS DEMO – SECURITY HARDENING

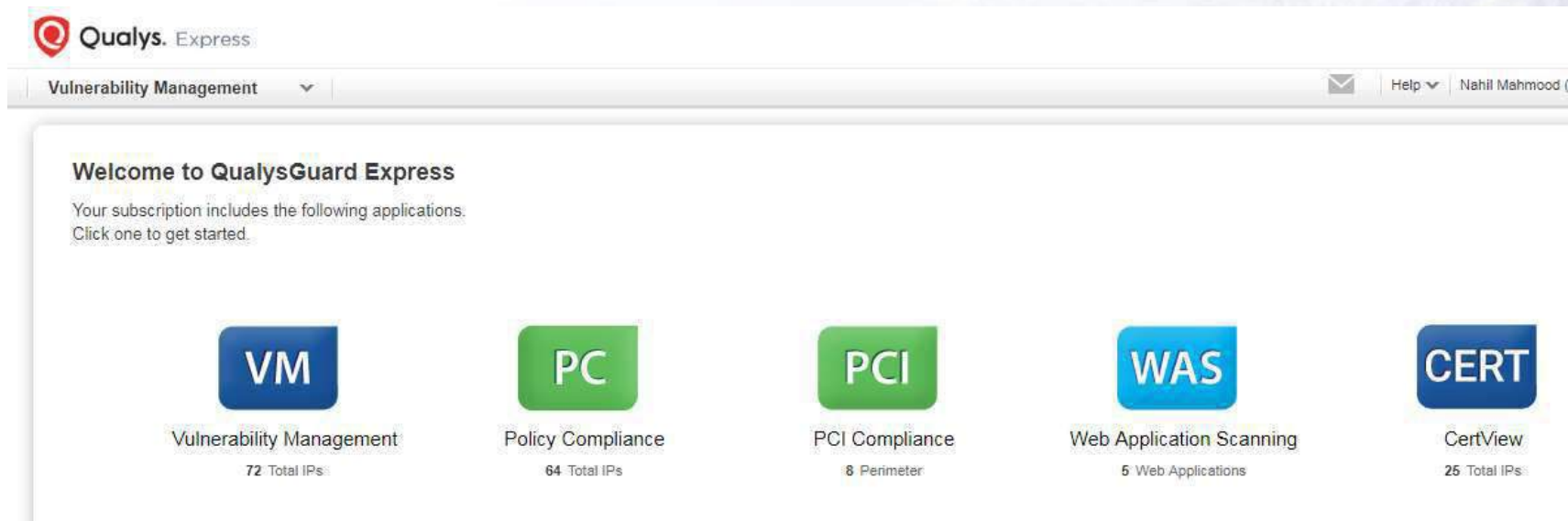
- Lets have a look at how Qualys can aid in the security hardening process

QUALYS DEMO – SECURITY HARDENING



QUALYS WEBSITE – FREE TRIAL

QUALYS DEMO – SECURITY HARDENING



QUALYS GUARD – HOME SCREEN

QUALYS DEMO – SECURITY HARDENING



Policy Compliance ▾

[Dashboard](#) [Policies](#) [Scans](#) [Reports](#) [Exceptions](#) [Assets](#) [Users](#)

Welcome to Qualys® Policy Compliance

Thank you for signing up for our cloud based security service for policy compliance. You'll find helpful information below to get started with your scans.

Steps for a successful scan

[Skip to Dashboard >](#)



1 Add IP addresses to scan >

Add the IPs/ranges that you want to scan for compliance.



2 Configure scan settings >

Customize the various scanning options required to run a scan. These can be saved as profiles for reuse. [View compliance profiles](#) provided by Qualys or [create a new profile](#).



3 Configure authentication >

Set up authentication records to use the authentication feature (Windows, Linux, Oracle, etc) in order to perform an in-depth assessment of your assets.

POLICY COMPLIANCE – HOME SCREEN

QUALYS DEMO – SECURITY HARDENING

Welcome to Qualys® Policy Compliance

Thank you for signing up for our cloud based security service for policy compliance. You'll find helpful information below to get started with your scans.

Steps for a successful scan

[Skip to Dashboard >](#)



3 [Configure authentication >](#)

Set up authentication records to use the authentication feature (Windows, Linux, Oracle, etc) in order to perform an in-depth assessment of your assets.



4 [Start your scan >](#)

You're now ready to start scanning! [Launch a new compliance scan](#) or [schedule your scan](#) to run automatically or on a recurring basis.

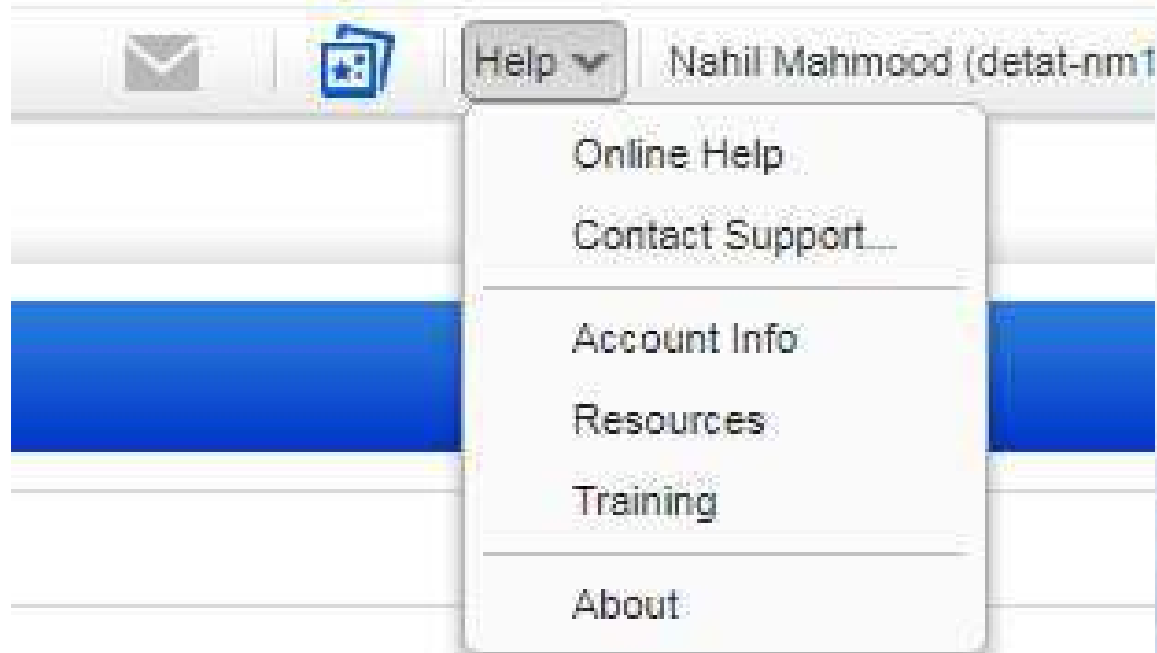


5 [Build a policy >](#)

Quickly create a new policy based on a scanned host. The service builds the policy for you using the host as a Golden Image. Or [import a policy](#) from the Library. Once you have a policy, go to the [Policy Summary](#) to check your compliance status and run reports.

POLICY COMPLIANCE – 5 STEPS

QUALYS DEMO – SECURITY HARDENING



HELP OPTIONS

QUALYS DEMO – SECURITY HARDENING

[Contents](#) [Search](#) [Back](#) [Print](#)

VM - Vulnerability Management
PC - Policy Compliance
Start Here
Policies
Scans
Reports
PC - SCAP Compliance
SCA - Security Configuration Assessment
Assets
Users
Resources

Scanning - The Basics (for PC Scans)

Good to Know

Recommendation for your first scan
What you can scan
How often you should scan
Scan complete email notification

What to Scan

How do I identify hosts to scan?
Can I exclude hosts from the scan?
Can I scan my IPv6 addresses?
Will the scan impact my hosts?
What are asset groups?
What are asset tags?

Recommendation for your first scan

We recommend you start small, maybe one or two IPs. Review the results, fix the compliance issues found, and re-scan the IPs to verify. Once you're comfortable, scan larger sets of IPs. When you're done, you'll feel more comfortable scanning larger sets of IPs.

What you can scan

The simple answer to what to scan is this: pretty much anything that's connected to your organization's network. Here's a list: all routers and switches, servers (operating systems), workstations, databases, desktop computers, printers, and wireless access devices.

How often you should scan

How to Scan

Which option profile should I use?
How can I customize my scan?
Why should I use authentication?

Which Scanner to Use

Are you scanning internally or externally?
Options when scanning asset groups
Do I need to whitelist Qualys scanners?
Scanning through a firewall
Don't see the scanner appliance option
How do I get a scanner appliance?

ONLINE HELP – POLICY COMPLIANCE

QUALYS DEMO – SECURITY HARDENING

Resources

Look to these resources to help you with our cloud security and compliance solutions.

Get Started

[Quick Tour](#)
[Evaluator's Guide](#)
[Community Edition](#)
[Securing Amazon Web Services with Qualys](#)

Watch Videos

[VM | PC | WAS | WAF | AWS EC2 | Express Lite | More Videos](#)

Get started with your applications

[CloudView](#)
[Container Security](#)
[Indication of Compromise](#)
[Web Application Scanning](#)
- [Crawling REST services using WAS](#)
- [Jenkins Plugin for WAS: user guide | download](#)
- [Qualys Browser Recorder: user guide | download](#)
[Web Application Firewall](#)
[Policy Compliance](#)
[SCAP Compliance](#)
[Security Configuration Assessment](#)
[PCI Compliance](#)
[File Integrity Monitoring](#)

Scan Authentication

Get system and account requirements for supported technologies below.
[Monitor scan authentication & status](#)

Cloud Agents

[Cloud Agent Getting Started Guide](#)
[Windows Installation Guide](#)
[Linux Installation Guide](#)
[Unix Installation Guide](#)
[Mac Installation Guide](#)

Using a scanner appliance?

[Scanner Appliance User Guide](#)
[Scanner Appliance Quick Start \(prior version\)](#)
[Virtual Scanner Appliance User Guide](#)
[Offline Scanner Appliance User Guide](#)
[Consultant Scanner Personal Edition User Guide](#)
[Cloud Platforms: AWS | Azure | GCE | OpenStack](#)
[Qualys Scanner - Static Route Configuration](#)
[Qualys Scanner - VLAN Scanning Guide](#)
[Scanner Appliance FAQs](#)

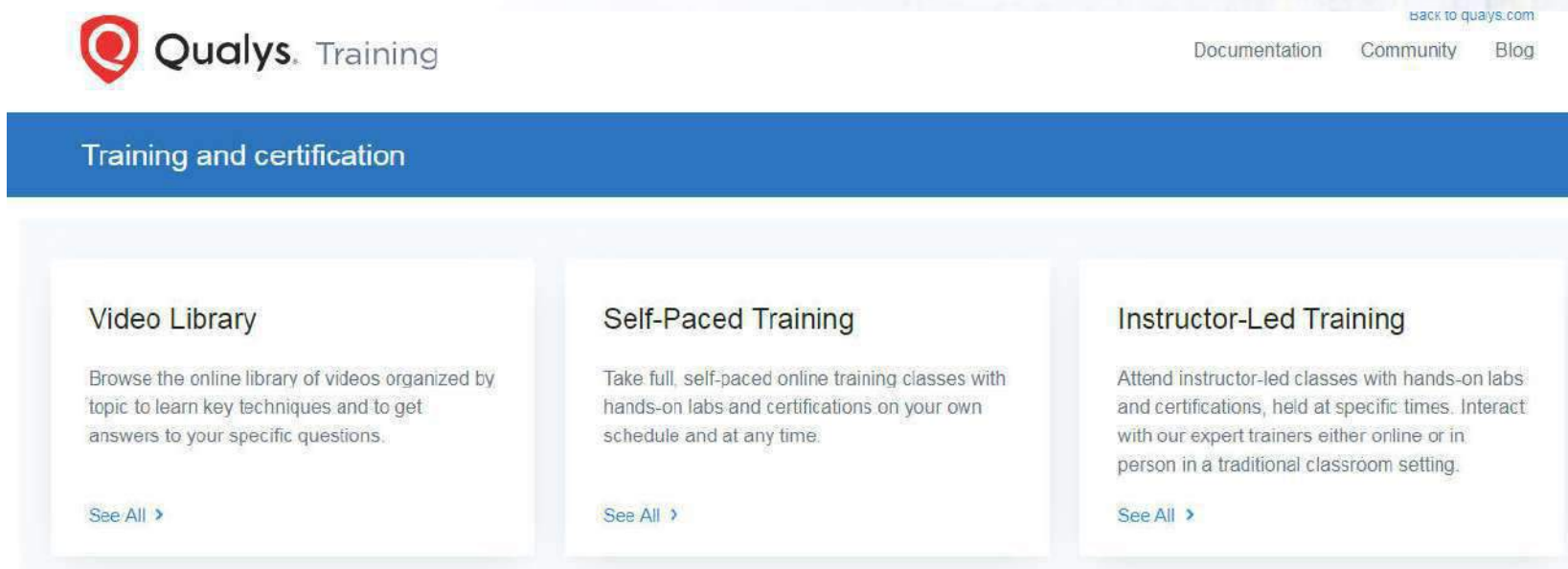
API Documentation

[Qualys API Quick Reference for all APIs](#)
[Qualys API \(VM, SCA, PC\)](#)

[Cloud Agent \(CA\) API](#)
[Web Application Scanning \(WAS\) API](#)
[Web Application Firewall \(WAF\) API](#)
[Malware Detection \(MD\) API](#)

RESOURCES

QUALYS DEMO – SECURITY HARDENING

A screenshot of the Qualys Training website. The header features the Qualys logo and 'Training' text on the left, and links for 'Documentation', 'Community', and 'Blog' on the right. A blue banner below the header reads 'Training and certification'. The main content area has three white boxes: 'Video Library' with a description and a 'See All' link, 'Self-Paced Training' with a description and a 'See All' link, and 'Instructor-Led Training' with a description and a 'See All' link. The background of the website has a light blue and white abstract pattern.

 **Qualys**. Training

[Back to qualys.com](#)

[Documentation](#) [Community](#) [Blog](#)

Training and certification

Video Library

Browse the online library of videos organized by topic to learn key techniques and to get answers to your specific questions.

[See All >](#)

Self-Paced Training

Take full, self-paced online training classes with hands-on labs and certifications on your own schedule and at any time.

[See All >](#)

Instructor-Led Training

Attend instructor-led classes with hands-on labs and certifications, held at specific times. Interact with our expert trainers either online or in person in a traditional classroom setting.

[See All >](#)

QUALYS WEBSITE - TRAINING

QUALYS DEMO – SECURITY HARDENING

The screenshot displays the Vimeo interface for a video playlist. At the top, the Vimeo logo is on the left, and navigation links for 'Join', 'Log in', 'Host videos', 'Sell', 'Watch', and 'Stock' are in the center. A search bar on the right contains the text 'Search videos, people, and more'. Below the navigation bar, the playlist title 'Self-Paced Class: Policy Compliance' is shown, along with '6 Videos' and a 'Share' button. The creator 'Qualys, Inc.' is listed below the title. Two video thumbnails are visible: 'Policy Compliance Overview' with a duration of 16:47, and 'Policies' with a duration of 17:26. Both thumbnails show the Qualys logo and a blue video player interface.

TRAINING VIDEOS - VIMEO

QUALYS DEMO – SECURITY HARDENING

- Qualys is an excellent tool with detailed online help, training, and resources to aid the new user

END

QUALYS DEMO – SECURITY HARDENING II

- Lets have a detailed look at Qualys interface for Policy Compliance

QUALYS DEMO – SECURITY HARDENING II



Policy Compliance ▾

[Dashboard](#) [Policies](#) [Scans](#) [Reports](#) [Exceptions](#) [Assets](#) [Users](#)

Welcome to Qualys® Policy Compliance

Thank you for signing up for our cloud based security service for policy compliance. You'll find helpful information below to get started with your scans.

Steps for a successful scan

[Skip to Dashboard >](#)



1 Add IP addresses to scan >

Add the IPs/ranges that you want to scan for compliance.



2 Configure scan settings >

Customize the various scanning options required to run a scan. These can be saved as profiles for reuse. [View compliance profiles](#) provided by Qualys or [create a new profile](#).



3 Configure authentication >

Set up authentication records to use the authentication feature (Windows, Linux, Oracle, etc) in order to perform an in-depth assessment of your assets.

1. ADD IP ADDRESSES TO SCAN

QUALYS DEMO – SECURITY HARDENING

New HostsLaunch Help✕

General Information: >

Host IPs >

Host Attributes >

Host IPs

Enter IPs and ranges in the field below. See the [Help](#) for proper formatting.

IPs: *

192.168.0.6

☐ Add to CertView Module

☐ Add to VM Module

(ex: 192.168.0.200,192.168.0.87-192.168.0.92)

Validate IPs through [Whois](#)

Cancel

Add

1. ADD IP ADDRESSES TO SCAN

QUALYS DEMO – SECURITY HARDENING



Policy Compliance ▾

[Dashboard](#) [Policies](#) [Scans](#) [Reports](#) [Exceptions](#) [Assets](#) [Users](#)

Welcome to Qualys® Policy Compliance

Thank you for signing up for our cloud based security service for policy compliance. You'll find helpful information below to get started with your scans.

Steps for a successful scan

[Skip to Dashboard >](#)



1 Add IP addresses to scan >

Add the IPs/ranges that you want to scan for compliance.



2 Configure scan settings >

Customize the various scanning options required to run a scan. These can be saved as profiles for reuse. [View compliance profiles](#) provided by Qualys or create a new profile.



3 Configure authentication >

Set up authentication records to use the authentication feature (Windows, Linux, Oracle, etc) in order to perform an in-depth assessment of your assets.

2. CONFIGURE SCAN SETTINGS

QUALYS DEMO – SECURITY HARDENING

Compliance Profile Information

General Information >

Scan Settings >

Additional Settings >

Scan restriction by Policy

Status: Disabled

Auto Update Expected Value

Status:: Disabled

Control Types

File Integrity Monitoring Controls: Disabled

Custom WMI Query Checks: Disabled

Dissolvable Agent

Dissolvable Agent (for this profile): Disabled

Password Auditing Controls: Disabled

Windows Share Enumeration: Disabled

Windows Directory Search: Disabled

Lite OS Discovery: Disabled

Ports

Scanned Ports: Targeted Scan

Hosts to Scan in Parallel

Use Appliance Parallel ML Scaling: Off

External Scanners: 15

Scanner Appliances: 30

Processes to Run in Parallel

Total: 10

HTTP: 10

2. CONFIGURE SCAN SETTINGS

QUALYS DEMO – SECURITY HARDENING

The screenshot displays the Qualys Express web interface. At the top, the 'Policy Compliance' dropdown is visible. Below it, a navigation bar includes 'Dashboard', 'Policies', 'Scans' (which is highlighted), 'Reports', 'Exceptions', 'Assets', and 'Users'. The 'Scans' section is further divided into sub-tabs: 'Scans', 'PC Scans', 'Schedules', 'Appliances', 'Option Profiles', 'Authentication', and 'Setup'. The 'Scans' sub-tab is active, showing a table of scan profiles. A dashed blue box highlights the 'New' dropdown menu, which has opened to show 'Compliance Profile...' and 'Download...'. The table lists several profiles, with 'CIS SCAN TEST PROFILE' highlighted in yellow.

Type	Name
Compliance	Initial PC Options
Compliance	CIS SCAN TEST PROFILE
Compliance	Initial PC Options
Compliance	windows-7 scan

NEW COMPLIANCE PROFILE

QUALYS DEMO – SECURITY HARDENING

New Compliance Profile

Compliance Profile Title >

Scan >

Additional >

Compliance Profile Title

Title: * CIS SCAN TEST PROFILE

Owner Nahil Mahmood (Manager: detat-nm1) ▼

☐ Make this a globally available option profile

‘CIS SCAN TEST PROFILE’ CREATED

QUALYS DEMO – SECURITY HARDENING

Welcome to Qualys® Policy Compliance

Thank you for signing up for our cloud based security service for policy compliance. You'll find helpful information below to get started with your scans.

Steps for a successful scan

[Skip to Dashboard >](#)



3 Configure authentication >

Set up authentication records to use the authentication feature (Windows, Linux, Oracle, etc) in order to perform an in-depth assessment of your assets.



4 Start your scan >

You're now ready to start scanning! Launch a new compliance scan or schedule your scan to run automatically or on a recurring basis.



5 Build a policy >

Quickly create a new policy based on a scanned host. The service builds the policy for you using the host as a Golden Image. Or import a policy from the Library. Once you have a policy, go to the [Policy Summary](#) to check your compliance status and run reports.

3. CONFIGURE AUTHENTICATION

QUALYS DEMO – SECURITY HARDENING

The screenshot displays the Qualys Express web interface. The top navigation bar includes the Qualys logo and the text "Qualys Express". Below this, the "Policy Compliance" section is active, with a dropdown menu open showing a list of records: Windows Record..., Unix Record..., Oracle Record..., Oracle Listener Record..., SNMP Record..., MS SQL Record..., Cisco Record..., IBM DB2 Record..., VMware ESXi Record..., MySQL Record..., MariaDB Record..., Sybase Record..., Checkpoint Firewall..., PostgreSQL Record..., Palo Alto Networks Firewall Record..., MongoDB Record..., Application Records..., and Authentication Vaults. The "Download..." option is at the bottom of the list. The left sidebar contains a "Scans" section with a search bar and an "Overview" section with a "Credentials Breach" link. The main content area shows a dashboard with tabs for "Appliances", "Option Profiles", "Authentication", and "Setup". Below these tabs, there are four status boxes: "Passing 0", "Failing 0", "Problematic 0", and "In Vault 0". At the bottom left, there is an "Actions (0)" dropdown and a "New" button.

Qualys Express

Policy Compliance

Dashboard

Scans

Search...

Overview

Credentials Breach

0

Actions (0)

New

Windows Record...

Unix Record...

Oracle Record...

Oracle Listener Record...

SNMP Record...

MS SQL Record...

Cisco Record...

IBM DB2 Record...

VMware ESXi Record...

MySQL Record...

MariaDB Record...

Sybase Record...

Checkpoint Firewall...

PostgreSQL Record...

Palo Alto Networks Firewall Record...

MongoDB Record...

Application Records...

Authentication Vaults

Download...

Appliances

Option Profiles

Authentication

Setup

Passing 0

Failing 0

Problematic 0

In Vault 0

QUALYS DEMO – SECURITY HARDENING

New Windows Record

Record Title >

Login Credentials >

IPs >

Comments >

Login Credentials

Windows Authentication

☐ Local

☒ Domain

Domain type:

NetBIOS, User-Selected IPs ▼

Domain name: *

syntax: DOMAIN1

Login

For compliance scans, trusted scanning is required. Trusted scanning allows the service to conduct assessment.

Use the basic login credential or choose to use authentication vault for authenticated scanning.

☒ Basic authentication

☐ Authentication Vault

User Name: *

Password:

QUALYS DEMO – SECURITY HARDENING

Welcome to Qualys® Policy Compliance

Thank you for signing up for our cloud based security service for policy compliance. You'll find helpful information below to get started with your scans.

Steps for a successful scan

[Skip to Dashboard >](#)



3 Configure authentication >

Set up authentication records to use the authentication feature (Windows, Linux, Oracle, etc) in order to perform an in-depth assessment of your assets.



4 Start your scan >

You're now ready to start scanning! Launch a new compliance scan or schedule your scan to run automatically or on a recurring basis.



5 Build a policy >

Quickly create a new policy based on a scanned host. The service builds the policy for you using the host as a Golden Image. Or import a policy from the Library. Once you have a policy, go to the [Policy Summary](#) to check your compliance status and run reports.

3. CONFIGURE AUTHENTICATION

QUALYS DEMO – SECURITY HARDENING

Create a New Policy



Policy from Library: Choose from one of the policies in our library.

Find the policy that best suits your needs. Our Compliance Policy Library contains several sample policies based on popular compliance frameworks, including SOX, HIPAA, CoBIT and more. Click on one of the policies below, and then click Next to import it.

Labels	Technologies	Policies (6)
All	☐ Oracle 11g	 HITRUST Cyber Security Framework (CSF) for Linux, Version 8.1 Version 3.0 07/24/2018 View Description View Policy
New	☐ Oracle 12c	
Updated	☐ Oracle Enterprise Linux 6.x	
CIS	☐ Oracle Enterprise Linux 7.x	
Qualys	☐ Oracle WebLogic Server 11g	 DISA Security Technical Implementation Guide (STIG) for Red Hat Enterprise Linux 7, V1R4 Version 4.0 08/02/2018 View Description View Policy
Mandate	☐ Oracle WebLogic Server 12c	
DISA STIG	☐ PaloAlto Networks PAN-OS	
Vendor	☐ Pivotal tc Server 3.x	
	☐ PostgreSQL 9.x	
	☐ Red Hat Enterprise Linux 5.x	 CIS Benchmark for Red Hat Enterprise Linux 7, v2.2.0 [Scored, Level 1] Version 1.0 06/20/2018 View Description View Policy
	☐ Red Hat Enterprise Linux 6.x	
	☒ Red Hat Enterprise Linux 7.x	
	☐ SAP Adaptive Server Enterprise 16	 CIS Benchmark for Red Hat Enterprise Linux 7, v2.2.0 [Scored, Level 1 and Level 2]

Back

Choose Source

Next

COMPLIANCE LIBRARY: CIS RED HAT ENT. LINUX 7

QUALYS DEMO – SECURITY HARDENING

Policy Editor

This policy is locked so it can be used for certification.
Click 'Save As...' to create an editable version of this policy for purposes other than certification.

Overview

CIS Benchmark for Red Hat Enterprise Linux 7, v2.2.0 [Scored, Level 1] v.1.0

Policy Information

Sections

6

Technologies

1

Controls

295

Status:

 Active | Deactivate

Locking:

 Block other users ☐ OFF

Last Evaluated:

09/20/2018 at 20:25:44 (GMT+0500)

Created By:

Nahil Mahmood (detat-nm1)

Assigned Technologies (1)

Red Hat Enterprise Linux 7.x

assigned to 295 controls

POLICY EDITOR

QUALYS DEMO – SECURITY HARDENING

Launch Compliance Scan

General Information

Give your scan a name, select a scan profile (a default is selected for you with recommended settings), and choose a scanner from

Title:

SCAN 1

Compliance Profile:

CIS SCAN TEST PROFILE

[View](#)

Scanner Appliance:

External

[View](#)

Choose Target Hosts from

Tell us which hosts (IP addresses) you want to scan.

☒ Assets

☐ Tags

Asset Groups

Select items...



[Select](#)

IPs/Ranges

192.168.0.1

[Select](#)

Example: 192.168.0.87-192.168.0.92, 192.168.0.200

Exclude IPs/Ranges

[Select](#)

LAUNCH COMPLIANCE SCAN

QUALYS DEMO – SECURITY HARDENING II

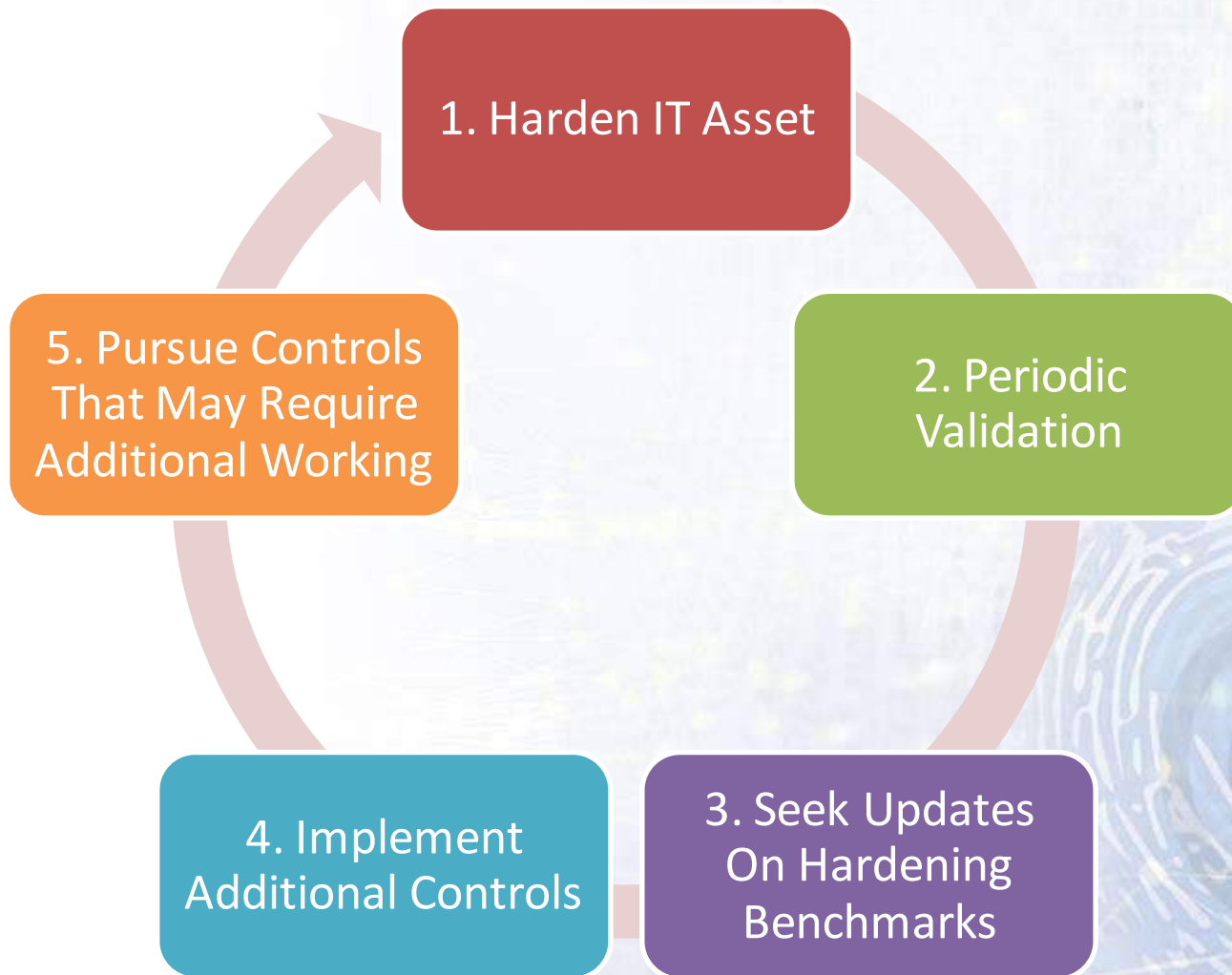
- The scan features may also be adjusted from the main Qualys dashboard

END

SECURITY HARDENING – LIFECYCLE

- **Security Hardening Lifecycle: Maintaining An Integrated & Current Program**

SECURITY HARDENING – LIFECYCLE

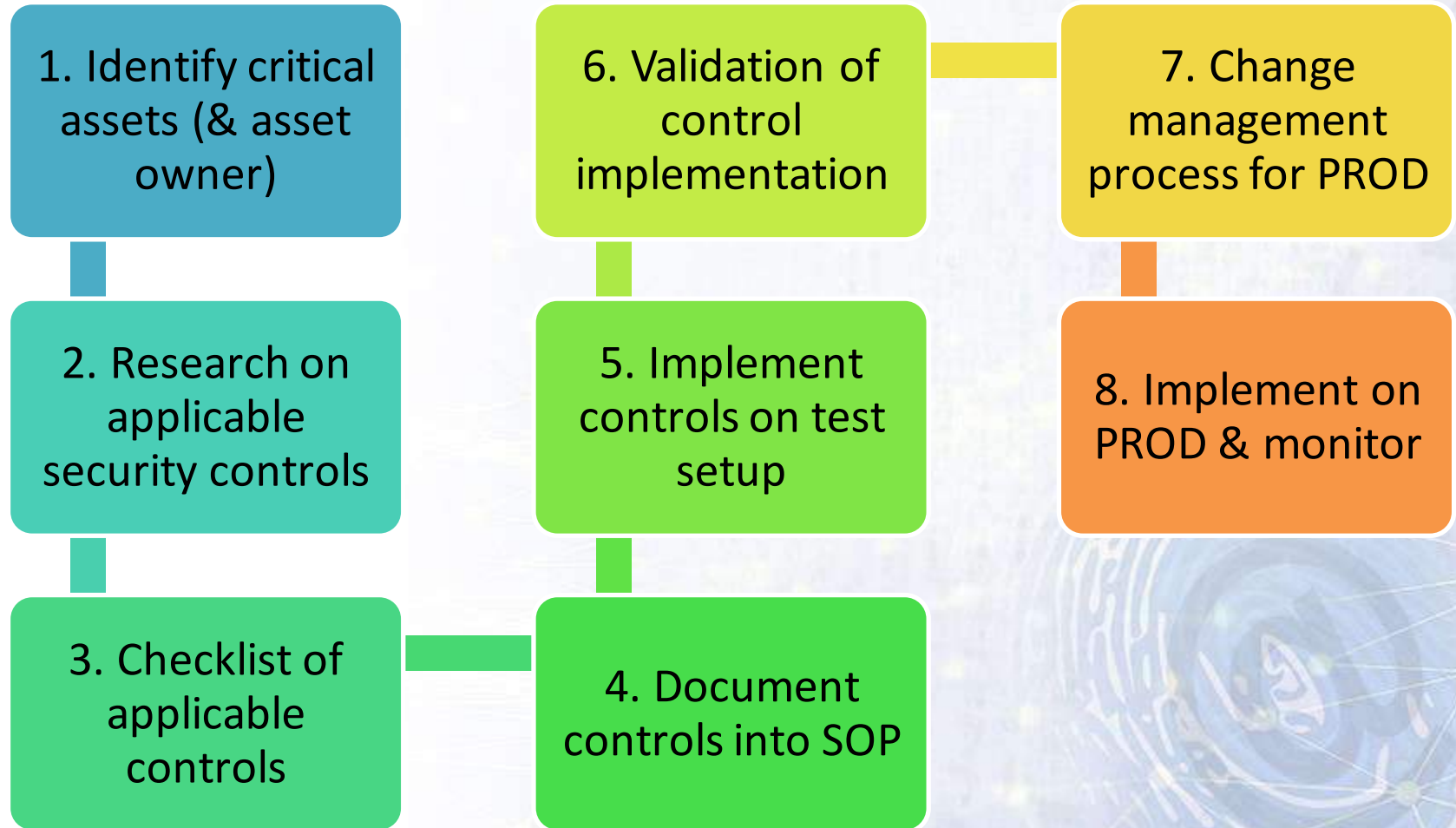


SECURITY HARDENING – LIFECYCLE

1: Harden IT Asset

Pursue the 8 step
hardening methodology

SECURITY HARDENING – LIFECYCLE



SECURITY HARDENING – LIFECYCLE

2: Periodic Validation

Check periodically (every quarter) for changes to the established standard or baseline

SECURITY HARDENING – LIFECYCLE

3: Seek Updated On Hardening Benchmarks

- Benchmarks are periodically updated
- Subscribe to feeds from CIS, DISA, NIST NCP (National Checklist Program) Repository

SECURITY HARDENING – LIFECYCLE

4: Implement Additional Controls

- Update the security controls by studying the changes

SECURITY HARDENING – LIFECYCLE

5: Pursue & Implement Controls That May Require Additional Working

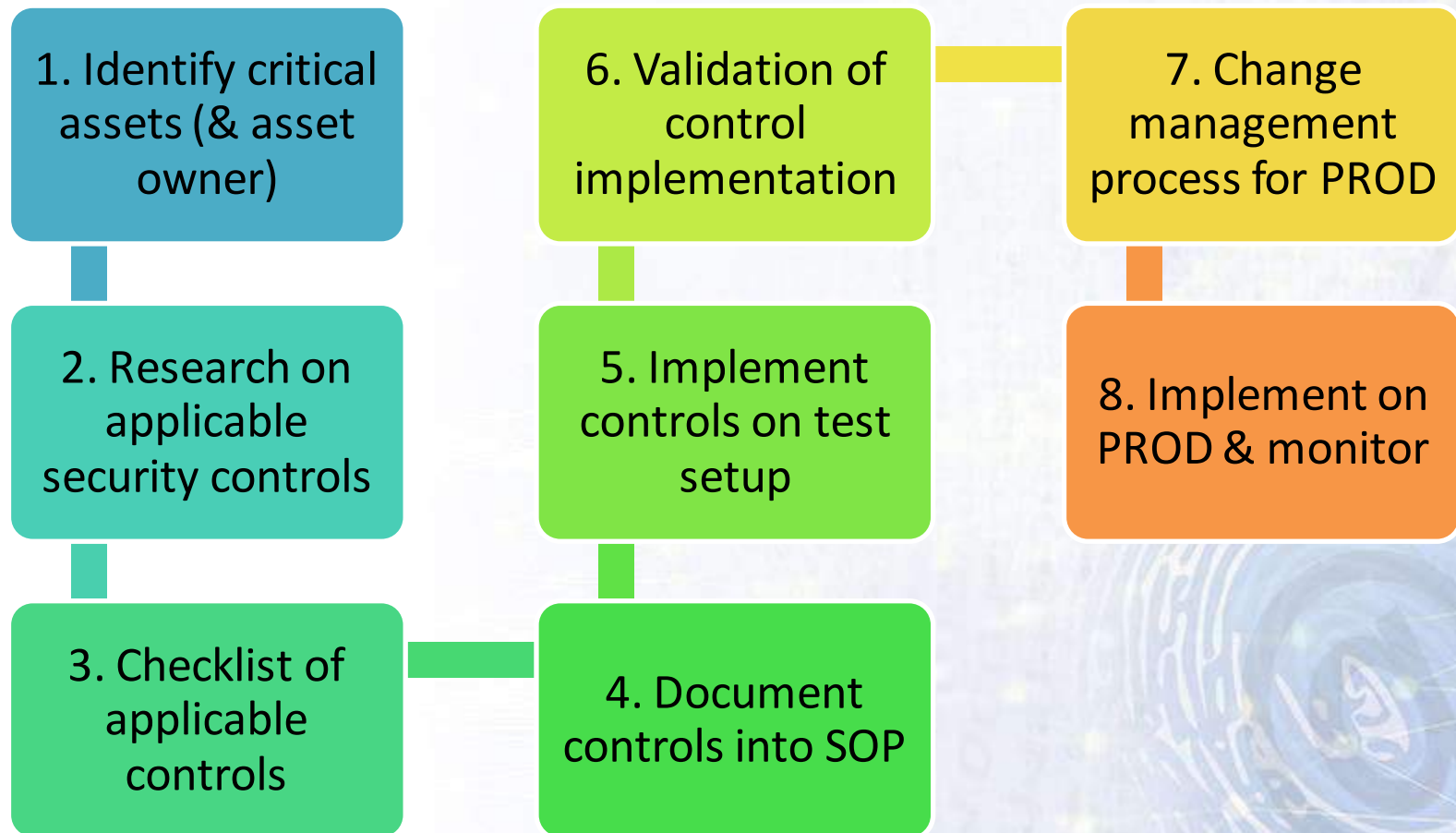
- Some controls may have caused a crash or malfunction
- Some controls may have not been possible due to dependencies or missing utilities
- Enhance the % of implemented controls

END

Hardening When CIS/DISA STIG Not Available

- What type of IT assets do not have a CIS/DISA STIG ?
 - Software applications (ASP.NET, PHP, Other)
 - Other applications such as asterisk deployments

Hardening When CIS/DISA STIG Not Available



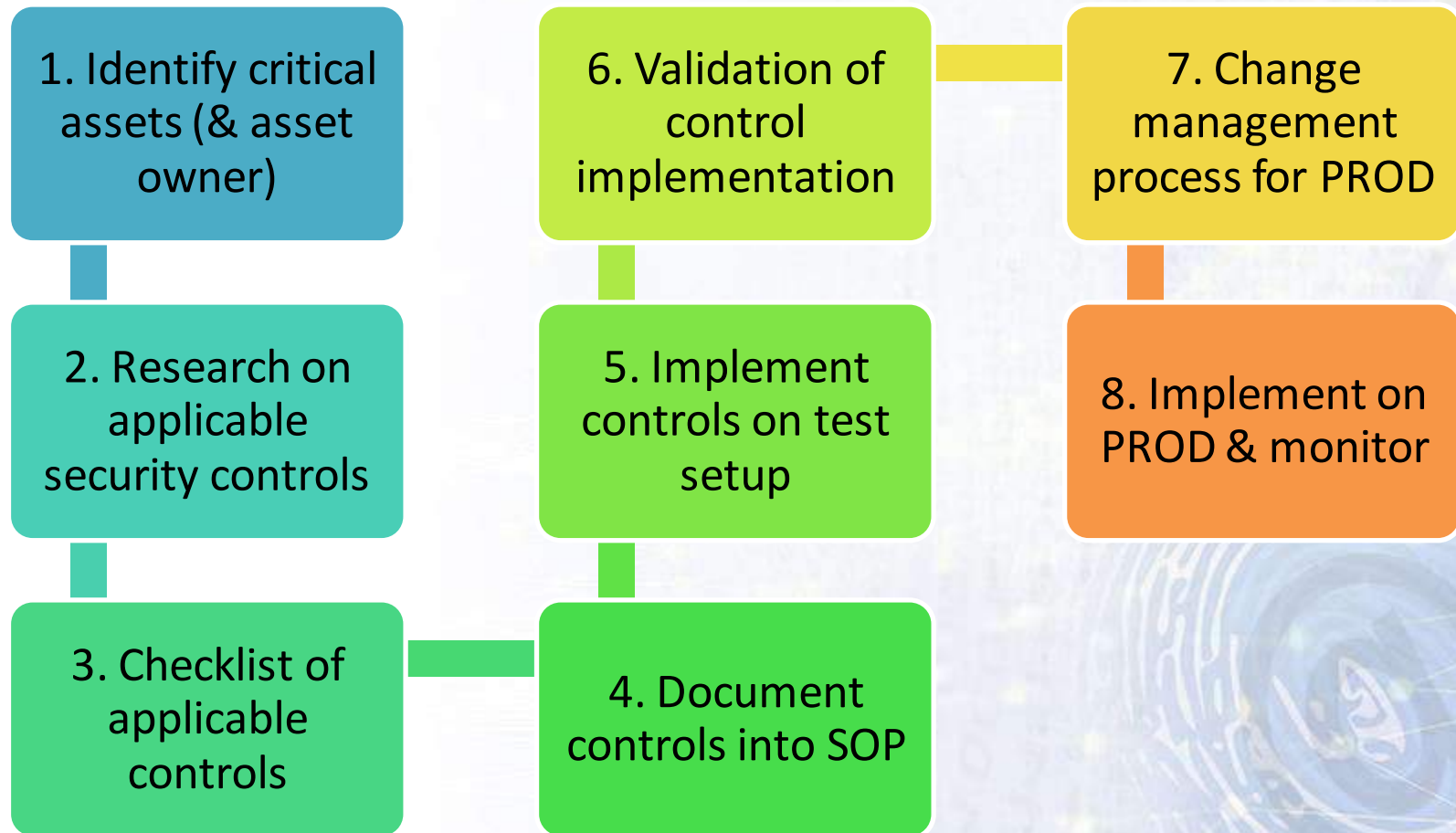
Hardening When CIS/DISA STIG Not Available

- Step 2: Research:
 - Look up google
 - Look for case studies and whitepapers

Hardening When CIS/DISA STIG Not Available

- Other considerations:
 - Implement on test setup
 - Test the controls
 - Security testing tools
 - Perform third-party security testing (penetration testing)
 - Vendor best-practices for application security hardening

Hardening When CIS/DISA STIG Not Available



Hardening When CIS/DISA STIG Not Available

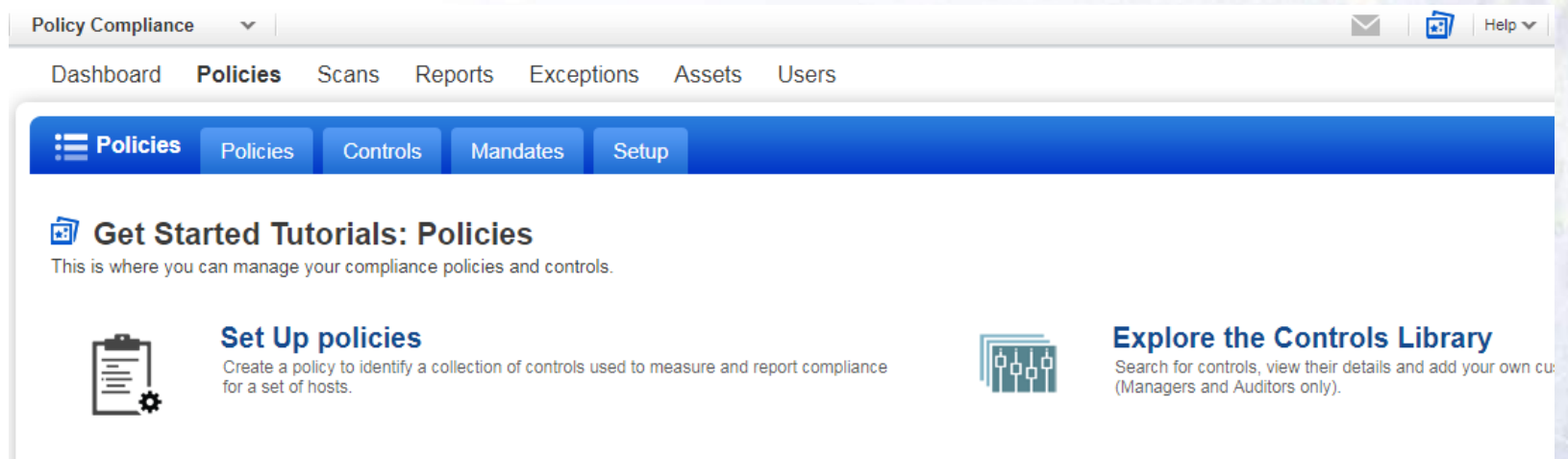
- With efforts and by following the 8-step methodology, all types of assets can be hardened

END

QUALYS POLICY LIBRARIES

- Lets have a detailed look at Qualys built-in libraries for creating scanning policies
- CIS
- QUALYS
- MANDATE
- DISA
- VENDOR

QUALYS POLICY LIBRARIES



The screenshot displays the Qualys Policy Compliance web interface. At the top, there is a navigation bar with 'Policy Compliance' on the left and a 'Help' dropdown on the right. Below this is a secondary navigation bar with links for 'Dashboard', 'Policies', 'Scans', 'Reports', 'Exceptions', 'Assets', and 'Users'. The 'Policies' section is active, indicated by a blue bar with sub-tabs for 'Policies', 'Controls', 'Mandates', and 'Setup'. The main content area features a 'Get Started Tutorials: Policies' section with the text 'This is where you can manage your compliance policies and controls.' Below this, there are two prominent cards. The first card, 'Set Up policies', includes a clipboard icon and describes creating a policy to identify controls for a set of hosts. The second card, 'Explore the Controls Library', includes a server rack icon and describes searching for controls and adding custom ones for managers and auditors.

Policy Compliance

Dashboard **Policies** Scans Reports Exceptions Assets Users

Policies Policies Controls Mandates Setup

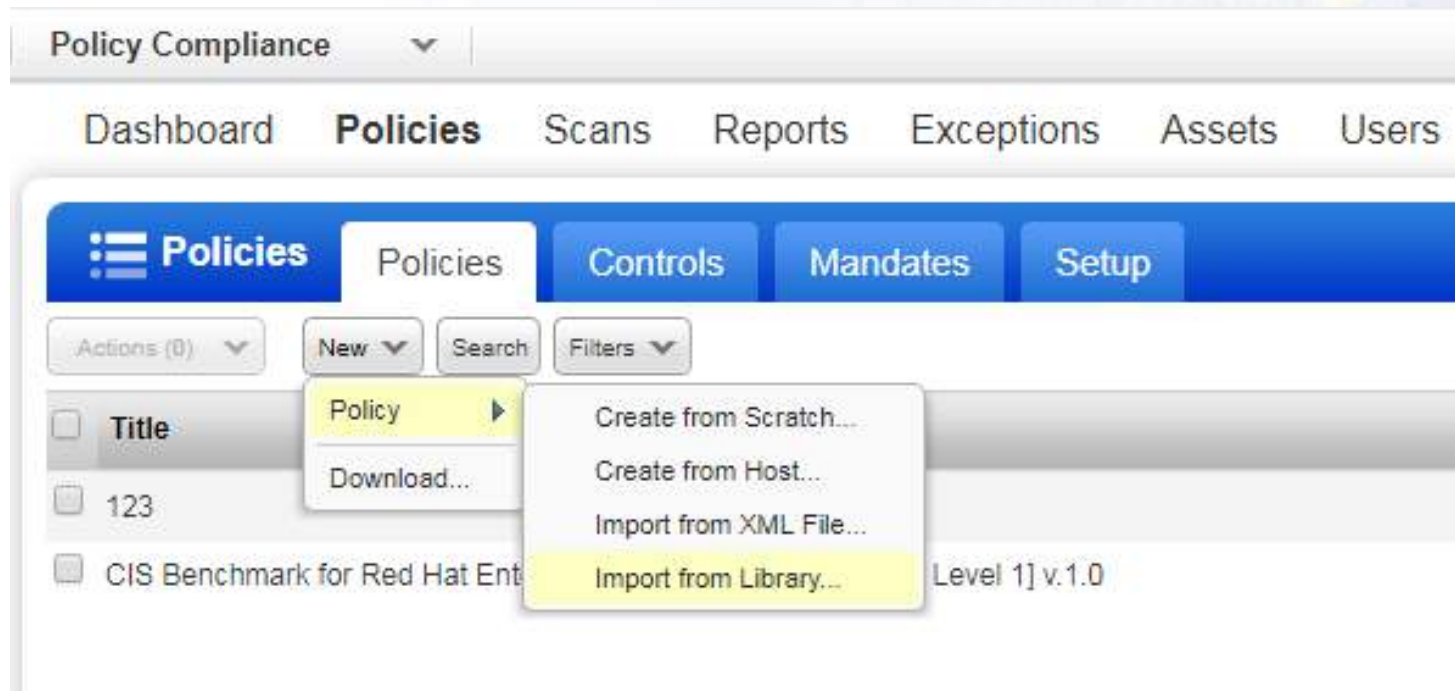
 **Get Started Tutorials: Policies**
This is where you can manage your compliance policies and controls.

 **Set Up policies**
Create a policy to identify a collection of controls used to measure and report compliance for a set of hosts.

 **Explore the Controls Library**
Search for controls, view their details and add your own controls (Managers and Auditors only).

EXPLORE THE CONTROLS LIBRARY

QUALYS POLICY LIBRARIES



CREATE NEW POLICY > IMPORT FROM LIBRARY

QUALYS POLICY LIBRARIES

Create a New Policy



Policy from Library: Choose from one of the policies in our library.

Find the policy that best suits your needs. Our Compliance Policy Library contains several sample policies based on popular compliance frameworks, including SOX, HIPAA, CoBIT and more. Click on one of the policies below, and then click Next to import it.

Labels

All

New

Updated

CIS

Qualys

Mandate

DISA STIG

Vendor

Technologies

☐ AIX 6.x

☐ AIX 7.x

☐ Amazon Linux 2 AMI

☐ Amazon Linux AMI

☐ Apache HTTP Server 2.2.x

☐ Apache HTTP Server 2.4.x

☐ Apache Tomcat 6.x

☐ Apache Tomcat 7.x

☐ Apache Tomcat 8.x

☐ CentOS 6.x

☐ CentOS 7.x

☐ Checkpoint Firewall

☐ Cisco ASA 8.x

☐ Cisco ASA 9.x

Policies (260)



CIS Benchmark for SuSE Enterprise Linux Server 10.x v2.0 [Scored]



Version 2.0 02/10/2016 [View Description](#) | [View Policy](#)



CIS Benchmark for Apache Tomcat 6.0 v1.0.0 [Scored and Not Scored, Level 1]



Version 2.0 12/01/2017 [View Description](#) | [View Policy](#)



CIS Benchmark for Apache Tomcat 6.0 v1.0.0 [Scored and Not Scored, Level 1 and Level 2]



Version 2.0 12/01/2017 [View Description](#) | [View Policy](#)



CIS Benchmark for Apache Tomcat 6.0 v1.0.0 [Scored, Level 1 and Level 2]

Back

Choose Source

Next

CREATE A NEW POLICY

QUALYS POLICY LIBRARIES

The screenshot displays the Qualys Policy Libraries interface. On the left, under the 'Labels' section, 'CIS' is selected. Under the 'Technologies' section, 'Red Hat Enterprise Linux 7.x' is checked. The main area, titled 'Policies (3)', lists three policies, all of which are CIS Benchmarks for Red Hat Enterprise Linux 7, v2.2.0. Each policy entry includes a document icon, a title, a lock icon, the version (1.0), the date (06/20/2018), and links to 'View Description' and 'View Policy'. A Red Hat logo is visible in the bottom right corner of each policy entry. The entire policy list is enclosed in a blue dashed border.

Labels	Technologies	Policies (3)
All	☐ MS IIS 7.x	CIS Benchmark for Red Hat Enterprise Linux 7, v2.2.0 [Scored, Level 1] Version 1.0 06/20/2018 View Description View Policy
New	☐ MS IIS 8.x	CIS Benchmark for Red Hat Enterprise Linux 7, v2.2.0 [Scored, Level 1 and Level 2] Version 1.0 06/20/2018 View Description View Policy
Updated	☐ MySQL 5.x	CIS Benchmark for Red Hat Enterprise Linux 7, v2.2.0 [Scored, Level 2] Version 1.0 06/20/2018 View Description View Policy
CIS	☐ Oracle 11g	
Qualys	☐ Oracle 12c	
Mandate	☐ Oracle Enterprise Linux 6.x	
DISA STIG	☐ Oracle Enterprise Linux 7.x	
Vendor	☐ PaloAlto Networks PAN-OS	
	☐ Red Hat Enterprise Linux 5.x	
	☐ Red Hat Enterprise Linux 6.x	
	☒ Red Hat Enterprise Linux 7.x	
	☐ Solaris 10.x	
	☐ Solaris 11.x	

CIS > RED HAT ENT. LINUX 7.X

QUALYS POLICY LIBRARIES

The screenshot displays the Qualys Policy Compliance dashboard. At the top, there's a navigation bar with tabs: Dashboard, Policies (selected), Scans, Reports, Exceptions, Assets, and Users. Below this, a sub-navigation bar includes Policies (selected), Controls, Mandates, and Setup. A toolbar shows 'Actions (1)', 'New', 'Search', and 'Filters'. A table lists policies, with the first one highlighted in yellow and enclosed in a dashed blue box. The details pane on the right shows information for the selected policy.

Title
120
☒ CIS Benchmark for Red Hat Enterprise Linux 7, v2.2.0 [Scored, Level 1 and Level 2] v.1.0
☐ CIS Benchmark for Red Hat Enterprise Linux 7, v2.2.0 [Scored, Level 1] v.1.0

CIS Benchmark for Red Hat Enterprise Linux 7, v2.2.0 [Scored, Level 1 and Level 2] v.1.0

ID:	372295
Policy Title:	CIS Benchmark for Red Hat Enterprise Linux 7, v2.2.0 [Scored, Level 1 and Level 2] v.1.0
Lock Status:	Locked at Import
Active:	Active
Evaluate Now:	No
Created By:	Nahil Mahmood (detat-nm1)

POLICIES DASHBOARD

QUALYS POLICY LIBRARIES

Create a New Policy



Policy from Library: Choose from one of the policies in our library.

Find the policy that best suits your needs. Our Compliance Policy Library contains several sample policies based on popular compliance frameworks, including SOX, HIPAA, CoBIT and more. Click on one of the policies below, and then click Next to import it.

Labels

All

New

Updated

CIS

Qualys

Mandate

DISA STIG

Vendor

Technologies

☐ MS IIS 10.x

☐ MS IIS 7.x

☐ MS IIS 8.x

☐ Red Hat Enterprise Linux 5.x

☐ Red Hat Enterprise Linux 6.x

☐ Red Hat Enterprise Linux 7.x

☐ Windows 10

☐ Windows 2008 Active Directory

☐ Windows 2008 Server

☐ Windows 2012 R1/R2 Active Directory

☐ Windows 2012 Server

☐ Windows 2016 Active Directory

Policies (18)



DISA Security Technical Implementation Guide (STIG) for Internet Explorer 10, V1R15

Version 4.0 07/24/2018 [View Description](#) | [View Policy](#)



DISA Security Technical Implementation Guide (STIG) for Windows 8.1, V1R20

Version 1.0 08/02/2018 [View Description](#) | [View Policy](#)



DISA Security Technical Implementation Guide (STIG) for Windows Server 2008 (non-R2) DC, V6R39

Version 1.0 08/02/2018 [View Description](#) | [View Policy](#)



DISA Security Technical Implementation Guide (STIG) for Windows Server 2012 (non-R2)

[Back](#)

[Choose Source](#)

[Next](#)

DISA STIG

QUALYS POLICY LIBRARIES

Create a New Policy



Policy from Library: Choose from one of the policies in our library.

Find the policy that best suits your needs. Our Compliance Policy Library contains several sample policies based on popular compliance frameworks, including SOX, HIPAA, CoBIT and more. Click on one of the policies below, and then click Next to import it.

Labels

All

New

Updated

CIS

Qualys

Mandate

DISA STIG

Vendor

Technologies

- ☐ Oracle Enterprise Linux 6.x
- ☐ Oracle Enterprise Linux 7.x
- ☐ Oracle WebLogic Server 11g
- ☐ Oracle WebLogic Server 12c
- ☐ Pivotal tc Server 3.x
- ☐ PostgreSQL 9.x
- ☐ Red Hat Enterprise Linux 6.x
- ☐ Red Hat Enterprise Linux 7.x
- ☒ SAP Adaptive Server Enterprise 16
- ☐ vFabric tc Server 2.9.x
- ☐ Windows 10
- ☐ Windows 2000
- ☐ Windows 2000 Active Directory

Policies (1)



Qualys - Security Configuration and Compliance Policy for SAP Adaptive Server Enterprise 16.0



Version 2.0 07/24/2018 [Hide Description](#) | [View Policy](#)

This policy for 'Security Configuration and Compliance Policy for SAP Adaptive Server Enterprise 16.0' is based on the 'CIS benchmark for Sybase ASE 15.0, v.1.1.0'. The Policy contains Level 1 and Level 2 'Scored' types of checks from the benchmark. The controls within the policy are configured on the basis of values specified by CIS benchmark.

[Back](#)

[Choose Source](#)

[Next](#)

QUALYS SAP ADAPTIVE SERVER ENT 16

QUALYS POLICY LIBRARIES

Create a New Policy

 **Policy from Library:** Choose from one of the policies in our library.

Find the policy that best suits your needs. Our Compliance Policy Library contains several sample policies based on popular compliance frameworks, including SOX, HIPAA, CoBIT and more. Click on one of the policies below, and then click Next to import it.

Labels

- All
- New
- Updated
- CIS
- Qualys
- Mandate
- DISA STIG
- Vendor**

Technologies

- ☐ VMware ESX/ESXi 4.x
- ☐ VMware ESXi 5.x
- ☐ VMware ESXi 6.x
- ☐ Windows 10
- ☐ Windows 2008 Active Directory
- ☐ Windows 2008 Server
- ☐ Windows 2012 Server
- ☐ Windows 2016 Server
- ☐ Windows 7
- ☐ Windows 8
- ☐ Windows 8.1
- ☐ Windows Server 2012 R2

Policies (17)



VMWare vSphere Security Hardening Guide for ESXi 6.x

 Version 3.0 03/01/2018 [View Description](#) | [View Policy](#)

VMware



Microsoft Security Compliance Manager (SCM) Baseline for Windows Server 2012 R2 [Member Server]

 Version 2.0 09/20/2016 [View Description](#) | [View Policy](#)





Microsoft Security Compliance Manager (SCM) Baseline for Windows 8.1

 Version 3.0 09/20/2016 [View Description](#) | [View Policy](#)





Microsoft Security Compliance Manager (SCM) Baseline for Windows 10 version 1511

Back

Choose Source

Next

VENDOR POLICIES

QUALYS POLICY LIBRARIES

- Qualys has a vast number of options for Compliance Scans, and these should be fully explored through the Qualys trial

END

Security Hardening For Outsourced IT Assets

- IT Outsourcing
- Mechanism to harden outsourced IT assets
- Important considerations

Security Hardening For Outsourced IT Assets

- IT Outsourcing examples:
 - Call centers
 - Hosted servers
 - Software development
 - Workstation helpdesk functions
 - Network services
 - Any other arrangement

Security Hardening For Outsourced IT Assets

- Mechanism:
 - Information Security Policy
 - Vendor contract (right-to-audit clause)
 - Set up security project with security project manager
 - Periodic reviews
 - Penalties for non-compliance

Security Hardening For Outsourced IT Assets

- Important considerations:
 - Enter security requirements into RFP
 - Part of vendor evaluation
 - Proceed with contract including InfoSec clauses
 - Awareness training

Security Hardening For Outsourced IT Assets

END

- Security evaluations:
 - Include outsourced scope in periodic internal audit
 - Ask for third-party security review
 - Vulnerability assessment and penetration test (if applicable)
 - Spot security checks

What is Vulnerability Management?

- What is a vulnerability ?
 - Vulnerability is a cyber-security term that refers to a flaw in a system that can leave it open to attack. A vulnerability may also refer to any type of weakness in a computer system itself, in a set of procedures...

What is Vulnerability Management?

- What is a vulnerability ?
 - ... or in anything that leaves information security exposed to a threat.

<https://www.techopedia.com/definition/13484/vulnerability>

What is Vulnerability Management?

- How do you fix vulnerabilities?
 - Computer users and network personnel can protect computer systems from vulnerabilities by keeping software security patches up to date. These patches can remedy flaws or security holes that were...

What is Vulnerability Management?

- How do you fix vulnerabilities?
 - ... found in the initial release. Computer and network personnel should also stay informed about current vulnerabilities in the software they use and seek out ways to protect against them.

<https://www.techopedia.com/definition/13484/vulnerability>

What is Vulnerability Management?

- What is vulnerability management?
 - Vulnerability management is the "cyclical practice of identifying, classifying, remediating, and mitigating vulnerabilities"

Foreman, P: *Vulnerability Management*, page 1.

What is Vulnerability Management?

- What is vulnerability assessment (VA)?
 - A process that defines, identifies, and classifies the security holes (vulnerabilities) in a computer, network, or communications infrastructure.

<http://searchmidmarketsecurity.techtarget.com/definition/vulnerability-analysis>

What is Vulnerability Management?

- What are some of the common vulnerability scanners?
 - OpenVAS
 - Nessus
 - Qualys
 - Rapid7

END

What Are The Steps In VM Lifecycle ?

VM Steps:

1. Analyze assets
2. Prepare scanner
3. Run vulnerability scan
4. Assess results
5. Patch systems
6. Verify (re-scan)

What Are The Steps In VM Lifecycle ?

1. Analyze Assets
 - Examine assets to scan
 - Gather details on IP subnet
 - Look at potential issues with network traffic
 - Inform asset owners and relevant department heads

What Are The Steps In VM Lifecycle ?

2. Prepare Scanner

- Set scanner parameters
- Select type of scan
- Look at credentials-based scan
- Explore and research plug-ins
- Do a test run
- Coordinate with asset owner

What Are The Steps In VM Lifecycle ?

3. Run Vulnerability Scanner

- Run the automated scan
- Monitor network performance degradation issues
- Generate report

What Are The Steps In VM Lifecycle ?

4. Assess Results:
 - Evaluate results
 - Prioritize according to the risk level
 - Collate results for asset owners
 - Communicate the results and remediation timelines

What Are The Steps In VM Lifecycle ?

5. Patch Systems:

- Research vulnerabilities
- Evaluate fixes and remediation method
- Test the patches and fixes
- Apply patches/fixes
- Monitor results

What Are The Steps In VM Lifecycle ?

6. Verify (Re-scan)

- Re-scan to confirm that the vulnerability scanner gives a positive report
- Collate results of vulnerability scan
- Report findings

END

Why Is Software Insecure ?

- Software is everywhere in IT
- Software is being developed in a manner which leaves many defects which may be exploited by attackers
- Race to meet software deadlines with little emphasis on security
- Result: insecure software

Why Is Software Insecure ?

- Gary McGraw, “trinity of trouble” for software security:
 - **Connectivity**; ever-increasing computer connectivity & to the internet enhances exposure to attacks

<https://newrepublic.com/article/115145/us-cybersecurity-why-software-so-insecure>

Why Is Software Insecure ?

- **Extensibility:** “Second, an extensible system is one that supports updates and extensions and thereby allows functionality to evolve incrementally.
- Web browsers, for example, support plug-ins that enable users to install extensions for new document types.

Why Is Software Insecure ?

- **Extensibility:**
... Extensibility is attractive for purposes of increasing functionality, but also makes it difficult to keep the constantly-adapting system free of software vulnerabilities.”

<https://newrepublic.com/article/115145/us-cybersecurity-why-software-so-insecure>

Why Is Software Insecure ?

- **Complexity:** Software systems are growing exponentially in size and complexity, which makes vulnerabilities unavoidable.

<https://newrepublic.com/article/115145/us-cybersecurity-why-software-so-insecure>

Why Is Software Insecure ?

- Carnegie Mellon University's CyLab Sustainable Computing Consortium estimates that [commercial software contains 20 to 30 bugs for every 1,000 lines of code...](#)

<https://newrepublic.com/article/115145/us-cybersecurity-why-software-so-insecure>

Why Is Software Insecure ?

- —and Windows XP contains at least 40 million lines of code
- That's 1 million bugs in Windows XP !

<https://newrepublic.com/article/115145/us-cybersecurity-why-software-so-insecure>

Why Is Software Insecure ?

- **Monoculture: Dan Greer:** “The security situation is deteriorating, and that deterioration compounds when nearly all computers in the hands of end users rely on a single operating system subject to the same vulnerabilities the world over.”

<https://newrepublic.com/article/115145/us-cybersecurity-why-software-so-insecure>

END

Why Is A VM Program Required ?

- What is a patch ?
 - “A **patch** is a piece of software designed to update a computer program or its supporting data, to fix or improve it. This includes fixing **security vulnerabilities** and **other bugs**”

[https://en.wikipedia.org/wiki/Patch_\(computing\)](https://en.wikipedia.org/wiki/Patch_(computing))

Why Is A VM Program Required ?

- What is patch management?
 - Patch management is an area of systems management that involves acquiring, testing, and installing multiple patches (code changes) to an administered computer system.

<http://searchenterprisedesktop.techtarget.com/definition/patch-management>

Why Is A VM Program Required ?

- Patch management tasks :
 - Maintaining current knowledge of available patches, deciding what patches are appropriate for particular systems, ensuring that patches are installed...

<http://searchenterprisedesktop.techtarget.com/definition/patch-management>

Why Is A VM Program Required ?

- Patch management tasks:
 - properly, testing systems after installation, and documenting all associated procedures, such as specific configs required.

Why Is A VM Program Required ?

Risk of not patching:

- By not applying a patch you might be leaving the door open for a malware attack
- Malware exploits flaws in a system in order to do its work. In addition, the timeframe between an exploit and when a patch is released is getting shorter

Why Is A VM Program Required ?

Risk of not patching... :

- Defects in clients like web browsers, email programs, image viewers, instant messaging software, and media players may allow malicious websites, etc. to infect or compromise your computer with no action on your part other than

Why Is A VM Program Required ?

Risk of not patching...:

- ...viewing or listening to the website, message, or media

<https://ist.mit.edu/security/patches>

Why Is A VM Program Required ?

A VM program addresses timely management of patching to ensure that vulnerabilities are not present for hackers to exploit...

END

What Is CVE & Vulnerability Database ?

- What is CVE ?
 - CVE is a list of information security vulnerabilities and exposures that aims to provide common names for publicly known cyber security issues. The goal of CVE is to make it easier to share data...

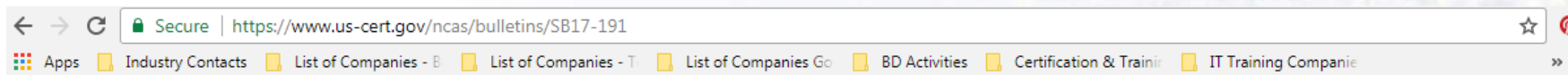
What Is CVE & Vulnerability Database ?

- What is CVE ?
 - ... across separate vulnerability capabilities (tools, repositories, and services) with this "common enumeration."

https://cve.mitre.org/about/faqs.html#cve_identifier_descriptions_created

What Is CVE & Vulnerability Database ?

SNAPSHOT OF US-CERT VULNERABILITY BULLETINS



High Vulnerabilities				
Primary Vendor – Product	Description	Published	CVSS Score	Source & Patch Info
cisco -- elastic_services_controller	A vulnerability in certain commands of Cisco Elastic Services Controller could allow an authenticated, remote attacker to elevate privileges to root and run dangerous commands on the server. The vulnerability occurs because a "tomcat" user on the system can run certain shell commands, allowing the user to overwrite any file on the filesystem and elevate privileges to root. This vulnerability affects Cisco Elastic Services Controller prior to releases 2.3.1.434 and 2.3.2. Cisco Bug IDs: CSCvc76634.	2017-07-05	9.0	CVE-2017-6712 BID CONFIRM
cisco -- elastic_services_controller	A vulnerability in the Play Framework of Cisco Elastic Services Controller (ESC) could allow an unauthenticated, remote attacker to gain full access to the affected system. The vulnerability is due to static, default credentials for the Cisco ESC UI that are shared between installations. An attacker who can extract the static credentials from an existing installation of Cisco ESC could generate an admin session token that allows access to all instances of the ESC web UI. This vulnerability affects Cisco Elastic Services Controller prior to releases 2.3.1.434 and 2.3.2. Cisco Bug IDs: CSCvc76627.	2017-07-05	10.0	CVE-2017-6713 BID CONFIRM
cisco -- ios_xr	A vulnerability in the CLI of Cisco IOS XR Software could allow an authenticated, local attacker to elevate privileges to the root level. More	2017-07-03	7.2	CVE-2017-6718

What Is CVE & Vulnerability Database ?

national vulnerability database

What is NVD ?

- The NVD is the CVE dictionary augmented with additional analysis, a database, and a fine-grained search engine. The NVD is a superset of CVE. The NVD is synchronized with CVE such that any updates to CVE appear immediately on the NVD.

<https://nvd.nist.gov/general/faq>

What Is CVE & Vulnerability Database ?

SNAPSHOT OF NATIONAL VULNERABILITY DATABASE - NVD

The screenshot shows the NVD website interface. At the top, the browser address bar displays the URL <https://nvd.nist.gov/vuln/detail/CVE-2017-10788>. The page header includes the NVD logo, the text "Computer Security Resource Center National Vulnerability Database", and the NIST logo with "National Institute of Standards and Technology U.S. Department of Commerce". A navigation bar contains links for General, Vulnerabilities, Vulnerability Metrics, Products, Configurations (CCE), Info, Other Sites, and a Search icon. Below the navigation bar, a breadcrumb trail shows "Vulnerabilities > Detail". The main heading is "CVE-2017-10788 Detail". Under the "Current Description" section, the text states: "The DBD::mysql module through 4.043 for Perl allows remote attackers to cause a denial of service (use-after-free and application crash) or possibly have unspecified other impact by triggering (1) certain error responses from a MySQL server or (2) a loss of a network connection to a MySQL server. The use-after-free defect was introduced by relying on incorrect Oracle mysql_stmt_close documentation and code examples." Below this, it lists "Source: MITRE" and "Last Modified: 07/01/2017" with a link to "View Analysis Description". On the right, a "Quick Info" box contains: "CVE Dictionary Entry: CVE-2017-10788", "Original release date: 07/01/2017", "Last revised: 07/12/2017", and "Source: US-CERT/NIST". The "Impact" section is partially visible at the bottom.

NVD Computer Security Resource Center
National Vulnerability Database

NIST
National Institute of Standards and Technology
U.S. Department of Commerce

General Vulnerabilities Vulnerability Metrics Products Configurations (CCE) Info Other Sites Search

Vulnerabilities > Detail

CVE-2017-10788 Detail

Current Description

The DBD::mysql module through 4.043 for Perl allows remote attackers to cause a denial of service (use-after-free and application crash) or possibly have unspecified other impact by triggering (1) certain error responses from a MySQL server or (2) a loss of a network connection to a MySQL server. The use-after-free defect was introduced by relying on incorrect Oracle mysql_stmt_close documentation and code examples.

Source: MITRE **Last Modified:** 07/01/2017 [View Analysis Description](#)

Impact

Quick Info

CVE Dictionary Entry: CVE-2017-10788

Original release date: 07/01/2017

Last revised: 07/12/2017

Source: US-CERT/NIST

What Is CVE & Vulnerability Database ?

What is the NVD severity score ?

- The NVD uses the Common Vulnerability Scoring System (CVSS) Version 2, which is an open standard for assigning vulnerability impacts that is used by a variety of organizations

<https://nvd.nist.gov/general/faq>

What Is CVE & Vulnerability Database ?

What is the NVD severity score ?

- [NISTIR 7946 - CVSS Implementation Guidance](#) describes methodologies developed by the NVD for using CVSS, and along with Appendix B describes the NVD's entire vulnerability assessment process.

<https://nvd.nist.gov/general/faq>

What Is CVE & Vulnerability Database ?

SNAPSHOT OF CVE-2017-10788

CVE-2017-10788 Detail

Current Description

The DBD::mysql module through 4.043 for Perl allows remote attackers to cause a denial of service (use-after-free and application crash) or possibly have unspecified other impact by triggering (1) certain error responses from a MySQL server or (2) a loss of a network connection to a MySQL server. The use-after-free defect was introduced by relying on incorrect Oracle mysql_stmt_close documentation and code examples.

Source: MITRE **Last Modified:** 07/01/2017 [- Hide Analysis Description](#)

Analysis Description

The DBD::mysql module through 4.043 for Perl allows remote attackers to cause a denial of service (use-after-free and application crash) or possibly have unspecified other impact by triggering (1) certain error responses from a MySQL server or (2) a loss of a network connection to a MySQL server. The use-after-free defect was introduced by relying on incorrect Oracle mysql_stmt_close documentation and code examples.

Source: MITRE **Last Modified:** 07/01/2017

<https://nvd.nist.gov/vuln/detail/CVE-2017-10788#vulnDescriptionTitle>

What Is CVE & Vulnerability Database ?

Impact

CVSS Severity (version 3.0):

CVSS v3 Base Score: 9.8 Critical

Vector: CVSS:3.0/AV:N/AC:L/

(legend)

Impact Score: 5.9

Exploitability Score: 3.9

CVSS Version 3 Metrics:

Attack Vector (AV): Network

Attack Complexity (AC): Low

Privileges Required (PR): None

User Interaction (UI): None

Scope (S): Unchanged

Confidentiality (C): High

Integrity (I): High

Availability (A): High

<https://nvd.nist.gov/vuln/detail/CVE-2017-10788#vulnDescriptionTitle>

What Is CVE & Vulnerability Database ?

CVSS Severity (version 2.0):

CVSS v2 Base Score: 7.5 HIGH

Vector: (AV:N/AC:L/Au:N/C:P/I:P/A:P) (legend)

Impact Subscore: 6.4

Exploitability Subscore: 10.0

CVSS Version 2 Metrics:

Access Vector: Network exploitable

Access Complexity: Low

Authentication: Not required to exploit

Impact Type: Allows unauthorized disclosure of information; Allows unauthorized modification; Allows disruption of service

<https://nvd.nist.gov/vuln/detail/CVE-2017-10788#vulnDescriptionTitle>

What Is CVE & Vulnerability Database ?

- Note that all the major vendors publish their security vulnerabilities online
 - Microsoft
 - Oracle
 - Cisco
 - Etc

END

What Is An Exploit ?

- What is an exploit ?
 - Program or some code that takes advantage of a security hole (i.e. a vulnerability) in an application or system, so that an attacker can use it for their benefit.

<https://www.welivesecurity.com/2015/02/27/exploits-work/>

What Is An Exploit ?

- Remote exploit:
 - *A remote exploit works over a network and exploits the security vulnerability without any prior access to the vulnerable system.*

[https://en.wikipedia.org/wiki/Exploit_\(computer_security\)](https://en.wikipedia.org/wiki/Exploit_(computer_security))

What Is An Exploit ?

A local exploit is a vulnerability in a Linux system that allows an ordinary user to gain root privileges by performing a certain sequence of actions.

- Local exploit:
 - A *local exploit* requires prior access to the vulnerable system and usually increases the privileges of the person running the exploit past those granted by the system administrator.

[https://en.wikipedia.org/wiki/Exploit_\(computer_security\)](https://en.wikipedia.org/wiki/Exploit_(computer_security))

What Is An Exploit ?

What is an exploit database?

Exploit Database (ExploitDB) is an archive of exploits for the purpose of public security, and it explains what can be found on the database. The ExploitDB is a very useful resource for identifying possible weaknesses in your network and for staying up to date on current attacks occurring in other networks.

- Exploit database:
 - The Exploit Database is a CVE compliant archive of public exploits and corresponding vulnerable software, developed for use by penetration testers and vulnerability researchers. Our aim is to serve the most

<https://www.exploit-db.com/about/>

What Is An Exploit ?

- Exploit database:
 - ... comprehensive collection of exploits gathered through direct submissions, mailing lists, as well as other public sources, and present them in a freely-available and easy-to-navigate database.

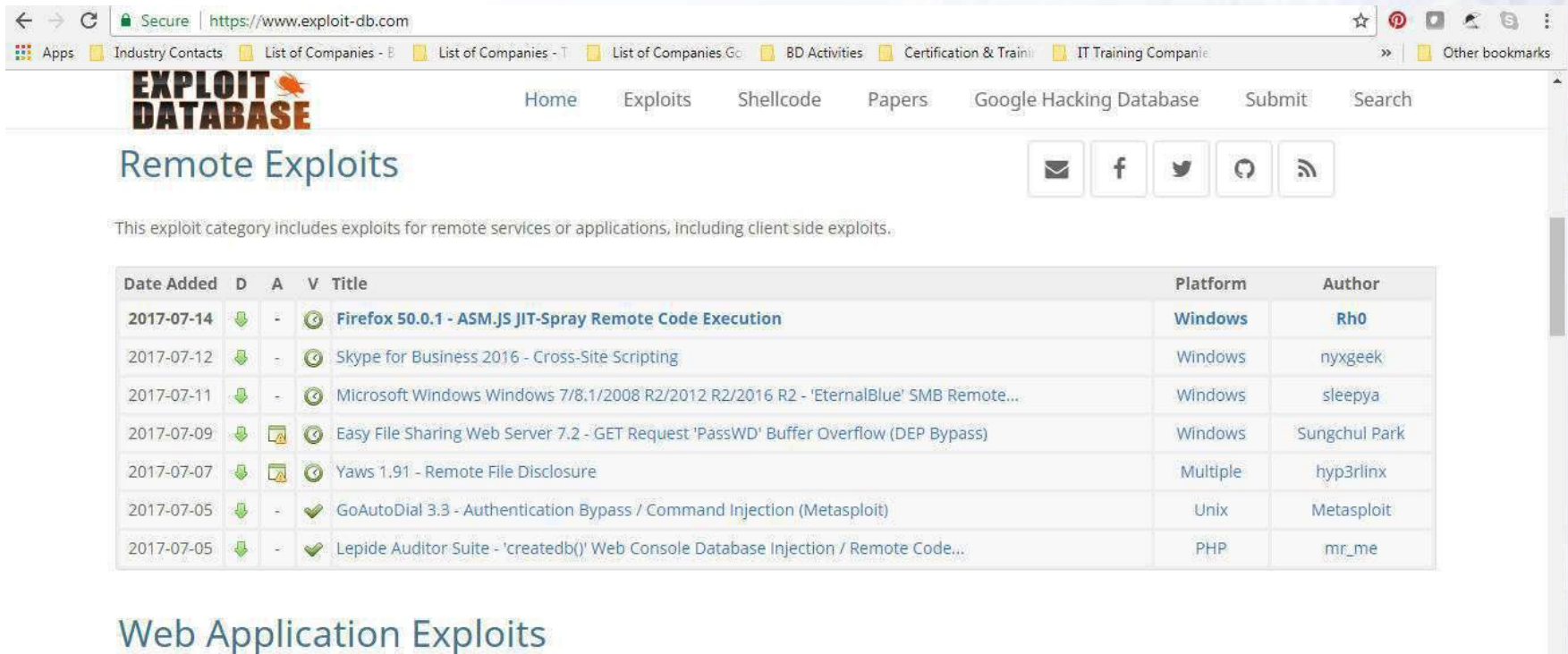
<https://www.exploit-db.com/about/>

What Is An Exploit ?

- Exploit database:
 - The Exploit Database is a repository for *exploits and proof-of-concepts* rather than *advisories*, making it a valuable resource for those who need actionable data right away.

<https://www.exploit-db.com/about/>

What Is An Exploit ?



The screenshot shows the Exploit-DB website interface. At the top, there's a navigation bar with links like Home, Exploits, Shellcode, Papers, Google Hacking Database, Submit, and Search. Below this, the 'Remote Exploits' section is highlighted. A description states: 'This exploit category includes exploits for remote services or applications, including client side exploits.' Below the description is a table listing various exploits.

Date Added	D	A	V	Title	Platform	Author
2017-07-14	↓	-	🕒	Firefox 50.0.1 - ASM.JS JIT-Spray Remote Code Execution	Windows	Rh0
2017-07-12	↓	-	🕒	Skype for Business 2016 - Cross-Site Scripting	Windows	nyxgeek
2017-07-11	↓	-	🕒	Microsoft Windows Windows 7/8.1/2008 R2/2012 R2/2016 R2 - 'EternalBlue' SMB Remote...	Windows	sleepya
2017-07-09	↓	📄	🕒	Easy File Sharing Web Server 7.2 - GET Request 'PassWD' Buffer Overflow (DEP Bypass)	Windows	Sungchul Park
2017-07-07	↓	📄	🕒	Yaws 1.91 - Remote File Disclosure	Multiple	hyp3rlinx
2017-07-05	↓	-	✅	GoAutoDial 3.3 - Authentication Bypass / Command Injection (Metasploit)	Unix	Metasploit
2017-07-05	↓	-	✅	Lepide Auditor Suite - 'createdb()' Web Console Database Injection / Remote Code...	PHP	mr_me

Web Application Exploits

What Is An Exploit ?

SNAPSHOT OF EXPLOIT CODE

EDB-ID: 42327	Author: Rh0	Published: 2017-07-14
CVE: CVE-2016-9079...	Type: Remote	Platform: Windows
Aliases: N/A	Advisory/Source: Link	Tags: N/A
E-DB Verified: 	Exploit:  Download /  View Raw	Vulnerable App: N/A

« Previous Exploit

```
1 <!DOCTYPE HTML>
2
3 <!--
4
5     FULL ASLR AND DEP BYPASS USING ASM.JS JIT SPRAY (CVE-2017-5375)
6     PoC Exploit against Firefox 50.0.1 (CVE-2016-9079 - Tor Browser 0day)
7
8     Tested on:
9
10    Release 50.0.1 32-bit - Windows 8.1 / Windows 10
11    https://ftp.mozilla.org/pub/firefox/releases/50.0.1/win32/en-US/Firefox%20Setup%2050.0.1.exe
12
13    Howto:
14
15    1) serve PoC over network and open it in Firefox 50.0.1 32-bit
16    2) if you don't see cmd.exe, open processexplorer and verify that cmd.exe was spawned by firefox.exe
17
18    A successfull exploit attempt should pop cmd.exe
19
```


What Is An Exploit ?

A zero-day vulnerability is a vulnerability in a system or device that has been disclosed but is not yet patched. An exploit that attacks a zero-day vulnerability is called a zero-day exploit.

- Zero-day exploit:
 - A zero day vulnerability refers to a hole in software that is unknown to the vendor. This security hole is then exploited by hackers before the vendor becomes aware and hurries to fix

What Is An Exploit ?

- Zero-day exploit:
 - it-this **exploit** is called a zero day attack.

<http://www.pctools.com/security-news/zero-day-vulnerability/>

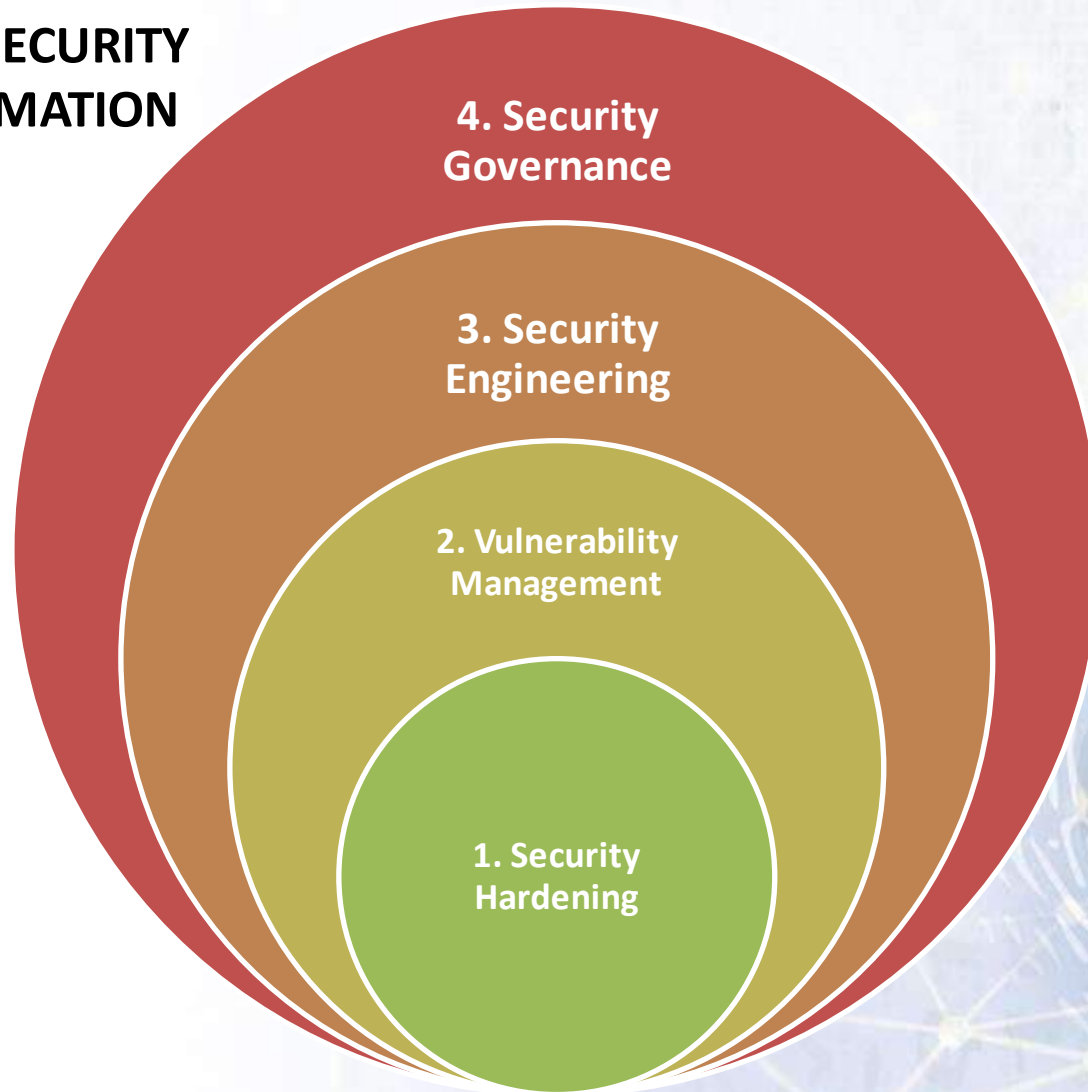
END

Effective Vulnerability Management: Stage 2

- Another look at the security transformation model...

Effective Vulnerability Management: Stage 2

4 – LAYER SECURITY TRANSFORMATION MODEL



Effective Vulnerability Management: Stage 2

- Stage 1: Security hardening
 - Taking stock of your assets
 - Prioritizing the assets
 - Establishing an MSB
 - Implement security controls with CIS/DISA/Other benchmarks
 - Basic/broader security hardening

Effective Vulnerability Management: Stage 2

- Note that Stage 1 (Hardening) and Stage 2 (Patching) are shown sequentially to show priority
- In practical terms, the two efforts may be done slightly staggered depending upon resources available
- Establish one program and then the other...

Effective Vulnerability Management: Stage 2

- Stage 1 (Hardening) is equivalent to tightening all the screws on machinery and will reduce impact of an attack (like a shield)
- Stage 2 (Patching) will seal all the entry points for an attacker to gain access or to penetrate a system

Effective Vulnerability Management: Stage 2

- Note that both Stage 1 and Stage 2 are equally important and necessary and assist in enhancing the security posture in their unique manner

END

Security Breach Case Study 1: Home Dept 2014

- 56 million payment cards compromised
- Early September 2014

Security Breach Case Study 1: Home Dept 2014

- Sequence of events:
 - The attackers were able to gain access to one of Home Depot's vendor environments by using a third-party vendor's logon credentials

Security Breach Case Study 1: Home Dept 2014

- Sequence of events:
 - Then they exploited a zero-day vulnerability in Windows, which allowed them to pivot from the vendor-specific environment to the Home Depot corporate environment.

Security Breach Case Study 1: Home Dept 2014

- Sequence of events:
 - Once they were in the Home Depot network, they were able install memory scraping malware on over 7,500 self-checkout POS terminals (Smith, 2014).

Security Breach Case Study 1: Home Dept 2014

- Sequence of events:
 - This malware was able to grab 56 million credit and debit cards. The malware was also able to capture 53 million email addresses (Winter, 2014).

Security Breach Case Study 1: Home Dept 2014

- Sequence of events:
 - The stolen payment cards were used to put up for sale and bought by carders. The stolen email addresses were helpful in putting together large phishing campaigns.

<https://www.sans.org/reading-room/whitepapers/breaches/case-study-home-depot-data-breach-36367>

Security Breach Case Study 1: Home Dept 2014

- Home Depot didn't have secure configuration of the software or hardware on the POS terminals.
- There was no proof of regularly scheduled vulnerability scanning of the POS environment.

<https://www.sans.org/reading-room/whitepapers/breaches/case-study-home-depot-data-breach-36367>

Security Breach Case Study 1: Home Depot 2014

- They didn't have proper network segregation between the Home Depot corporate network and the POS network.

<https://www.sans.org/reading-room/whitepapers/breaches/case-study-home-depot-data-breach-36367>

Security Breach Case Study 1: Home Dept 2014

- Overall: several controls missing, vendor management of IDs and access management missing, and monitoring of the network was missing

END

Security Breach Case Study 2: Anthem

- Health Insurer Anthem
- Affected 78.8 million individuals

<http://www.bankinfosecurity.com/new-in-depth-analysis-anthem-breach-a-9627>

Security Breach Case Study 2: Anthem

- Sequence of events:
 - Data [breach](#) began on Feb. 18, 2014, when a user within one of Anthem's subsidiaries opened a phishing email containing malicious content

<http://www.bankinfosecurity.com/new-in-depth-analysis-anthem-breach-a-9627>

Security Breach Case Study 2: Anthem

- Sequence of events:
 - Opening the email launched the download of malicious files to the user's computer and allowed hackers to gain remote access to that computer and dozens of other systems within the...

<http://www.bankinfosecurity.com/new-in-depth-analysis-anthem-breach-a-9627>

Security Breach Case Study 2: Anthem

- Sequence of events:
 - Anthem enterprise, including Anthem's data warehouse

<http://www.bankinfosecurity.com/new-in-depth-analysis-anthem-breach-a-9627>

Security Breach Case Study 2: Anthem

- Sequence of events:
 - Starting with the initial remote access, the attacker was able to move laterally across Anthem systems and escalate privileges, gaining increasingly greater ability to access information and make changes in the environment

Security Breach Case Study 2: Anthem

- Sequence of events:
 - The attacker utilized at least 50 accounts and compromised at least 90 systems within the Anthem enterprise environment including, eventually, the company's enterprise data warehouse -

Security Breach Case Study 2: Anthem

- Sequence of events:
 - a system that stores a large amount of consumer personally identifiable information
 - Queries to that data warehouse resulted in access to an exfiltration of approximately 78.8 m unique user records

Security Breach Case Study 2: Anthem

- Vulnerabilities:
 - Exploitable vulnerabilities were found in anthem network
 - User security awareness training conducted to prevent phishing and social engineering

<http://www.bankinfosecurity.com/new-in-depth-analysis-anthem-breach-a-9627>

Security Breach Case Study 2: Anthem

- Remediation measures:
 - Implemented two-factor [authentication](#) on all remote access tools, deployed a privileged account management solution and added enhanced logging resources to its security event and incident management solutions

Security Breach Case Study 2: Anthem

END

- Remediation measures:
 - Further, the company conducted a complete reset of passwords for all privileged users, suspended all remote access pending implementation of two-factor authentication and created new Network Admin IDs

Best Practices For Applying Security Patches

Take Inventory of Systems. ...
Determine Risk and Vulnerability. ...
Consolidate Software. ...
Create a Patch Management Policy. ...
Track Patch Availability. ...
Apply Patches Quickly. ...
Sufficiently Test Patches. ...
Automate Patching.

- "The risk of implementing the service pack, hotfix and security patch should ALWAYS be LESS than the risk of not implementing it."

<https://msdn.microsoft.com/en-us/library/cc750077.aspx>

Best Practices For Applying Security Patches

- *“You should never be worse off by implementing a service pack, hotfix and security patch. If you are unsure, then take steps to ensure that there is no doubt when moving them to production systems.”*

<https://msdn.microsoft.com/en-us/library/cc750077.aspx>

Best Practices For Applying Security Patches

1. Use a change control process
 - A good change control procedure has an identified owner, a path for customer input, an audit trail for any changes, a clear announcement and review period, testing procedures,

Best Practices For Applying Security Patches

1. Use a change control process
 - and a well-understood back-out plan.
 - Change control will manage the process from start to finish

Best Practices For Applying Security Patches

2. Read all related documentation:
 - Before applying any service pack, hotfix or security patch, all relevant documentation should be read and peer reviewed. The peer review process is critical as it mitigates the risk of..

Best Practices For Applying Security Patches

2. Read all related documentation:
 - ... a single person missing critical and relevant points when evaluating the update

Best Practices For Applying Security Patches

2. Read all related documentation:
 - Ensure the update is relevant, and will resolve an existing issue
 - Ensure adoption won't cause other issues resulting in a compromise of the production system

Best Practices For Applying Security Patches

2. Read all related documentation:
 - There are dependencies relating to the update, (i.e. certain features being enabled or disabled for the update to be effective.)

Best Practices For Applying Security Patches

2. Read all related documentation:

- Potential issues will arise from the sequencing of the update, as specific instructions may state or recommend a sequence of events or updates to occur before the service pack, hotfix or security patch is applied

Best Practices For Applying Security Patches

3. Apply updates on a need-only basis
4. Testing
5. Plan to uninstall
6. Working backup and production downtime
7. Always have roll-back plan
8. Don't get more than 2 service packs behind

<https://msdn.microsoft.com/en-us/library/cc750077.aspx>

Who Conducts Vulnerability Management

- A number of teams and resources may be involved in the VM lifecycle

Who Conducts Vulnerability Management

SN	ACTIVITY	TEAM	SUPPORTED BY
1	ANALYZE ASSETS	INFOSEC	IT OPS TEAM
2	PREPARE SCANNER	INFOSEC	-
3	RUN VULNERABILITY SCAN	INFOSEC	-
4	ASSESS RESULTS	INFOSEC	IT OPS TEAM
5	TEST & PATCH SYSTEMS	IT OPS TEAM	INFOSEC
6	VERIFY (RE-SCAN)	INFOSEC	IT OPS TEAM
7	REPORT FINDINGS	INFOSEC	IT STEERING COMMITTEE

Who Conducts Vulnerability Management

- Role of Infosec team:
 - Takes the primary ownership of the vulnerability management process
 - Runs scanning after coordinating with the relevant IT Ops team
 - Shares scanning reports with IT teams and management

Who Conducts Vulnerability Management

- ... Role of Infosec team:
 - Tracks remediation timelines
 - Understands criticality issues and helps to prioritize
 - Studies the security patch details as a backup resource
 - Assists with change management process

Who Conducts Vulnerability Management

- Role of IT Ops team:
 - Owner of the IT asset
 - Receives the vulnerability scan report from Infosec team
 - Studies the vulnerability
 - Understands criticality, impact, & dependencies

Who Conducts Vulnerability Management

- Role of IT Ops team:
 - Helps Infosec team develop a project plan (if required) and timelines for the patching
 - Tests the patches in test environment
 - Takes backups, develops roll-back plan

Who Conducts Vulnerability Management

- Role of IT Ops team:
 - Takes downtime and takes ownership of the change management process
 - Implements the patches
 - Monitors the systems after patch implementation
 - Rolls-back if necessary

Who Conducts Vulnerability Management

- Role of IT Ops team:
 - Creates the necessary documentation

END

Nessus Features

- Lets take a look at Nessus features

Nessus Features

- Nessus (Reports):
 - Customize reports to sort by vulnerability or host
 - Create an executive summary or compare scan results
 - Targeted email notifications of scan results

Nessus Features

- Nessus (Scan Types):
 - Asset discovery
 - Un-credentialed vulnerability discovery
 - Credentialed scanning for system hardening & missing patches

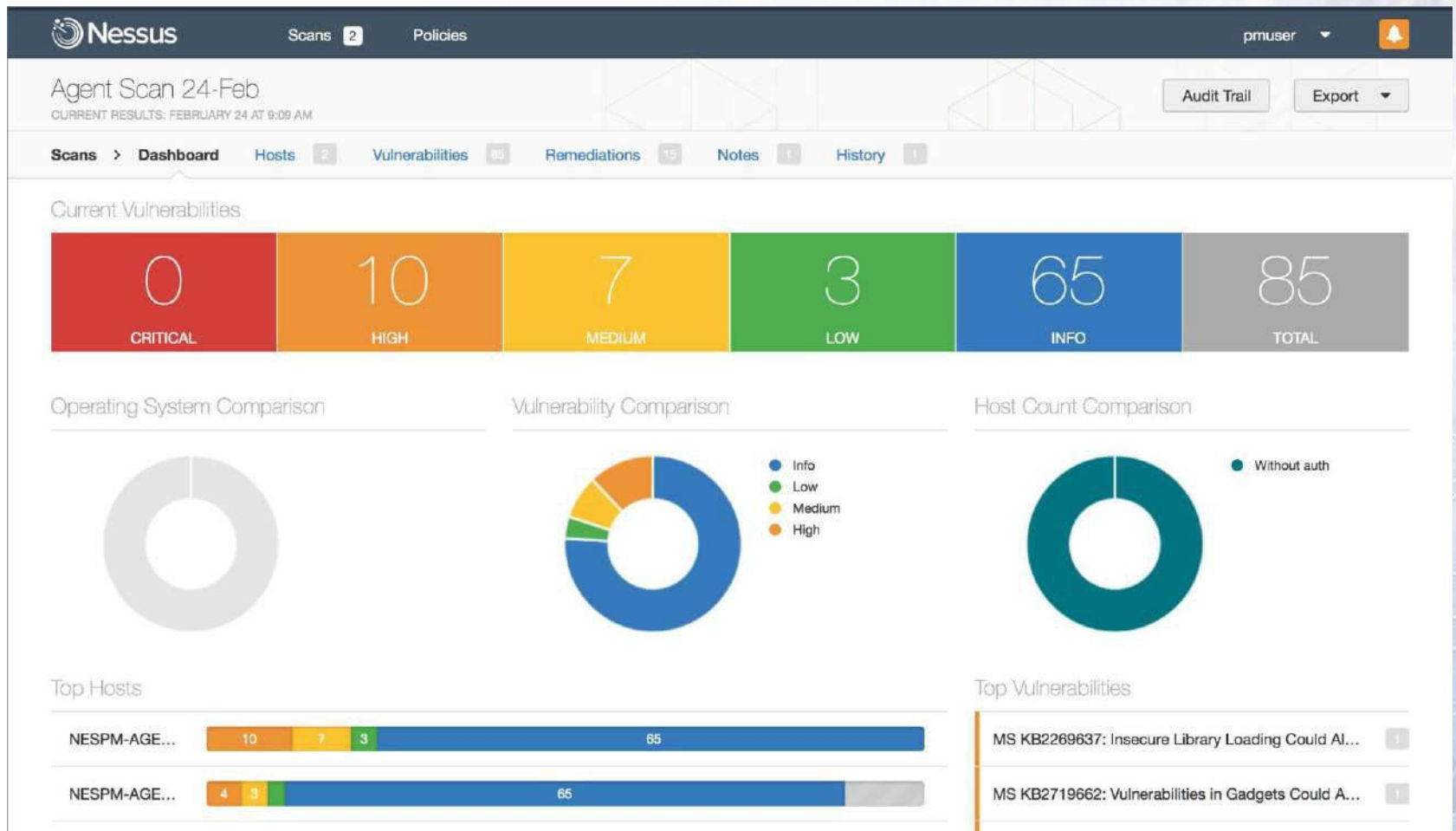
Nessus Features

- Nessus (Compliance & Config Scans):
 - Compliance auditing: FFIEC, FISMA, CyberScope, GLBA, HIPAA/ HITECH, NERC, PCI, SCAP, SOX
 - Configuration auditing: CERT, CIS, COBIT/ITIL, DISA STIGs, FDCC, ISO, NIST, NSA

Nessus Features

- Nessus (Risk scores):
 - Vulnerability ranking based on CVE, five severity levels (Critical, High, Medium, Low, Info), customizable severity levels for recasting of risk

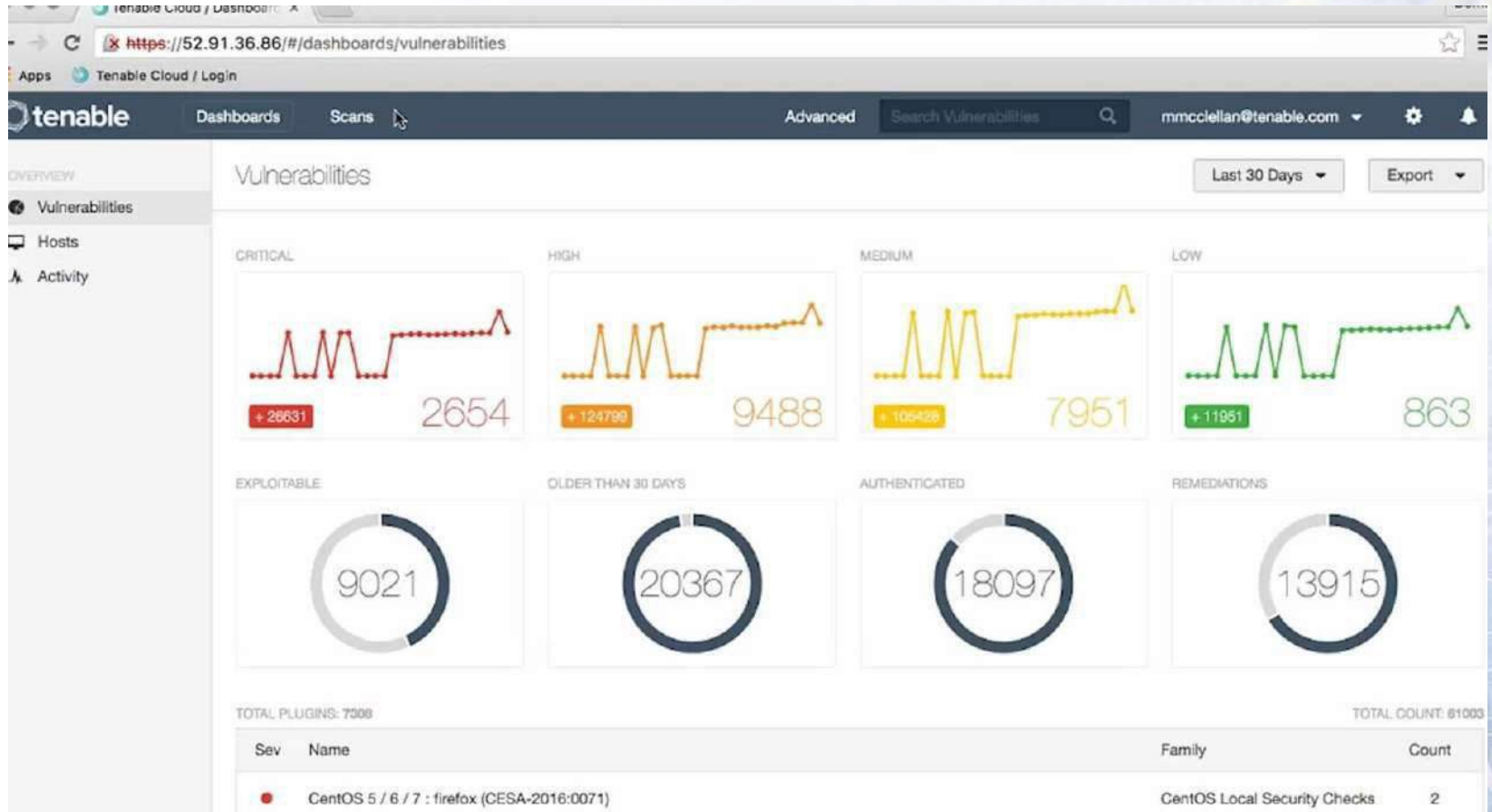
Nessus Features



Nessus Features



Nessus Features



Nessus Features

- Nessus is a cost-effective scanner that gets most of the job done for vulnerability scanning
- It has CIS and DISA compliance templates
- Has some flaws and bugs but overall useful tool

Qualys Features

- Lets take a look at Qualys features

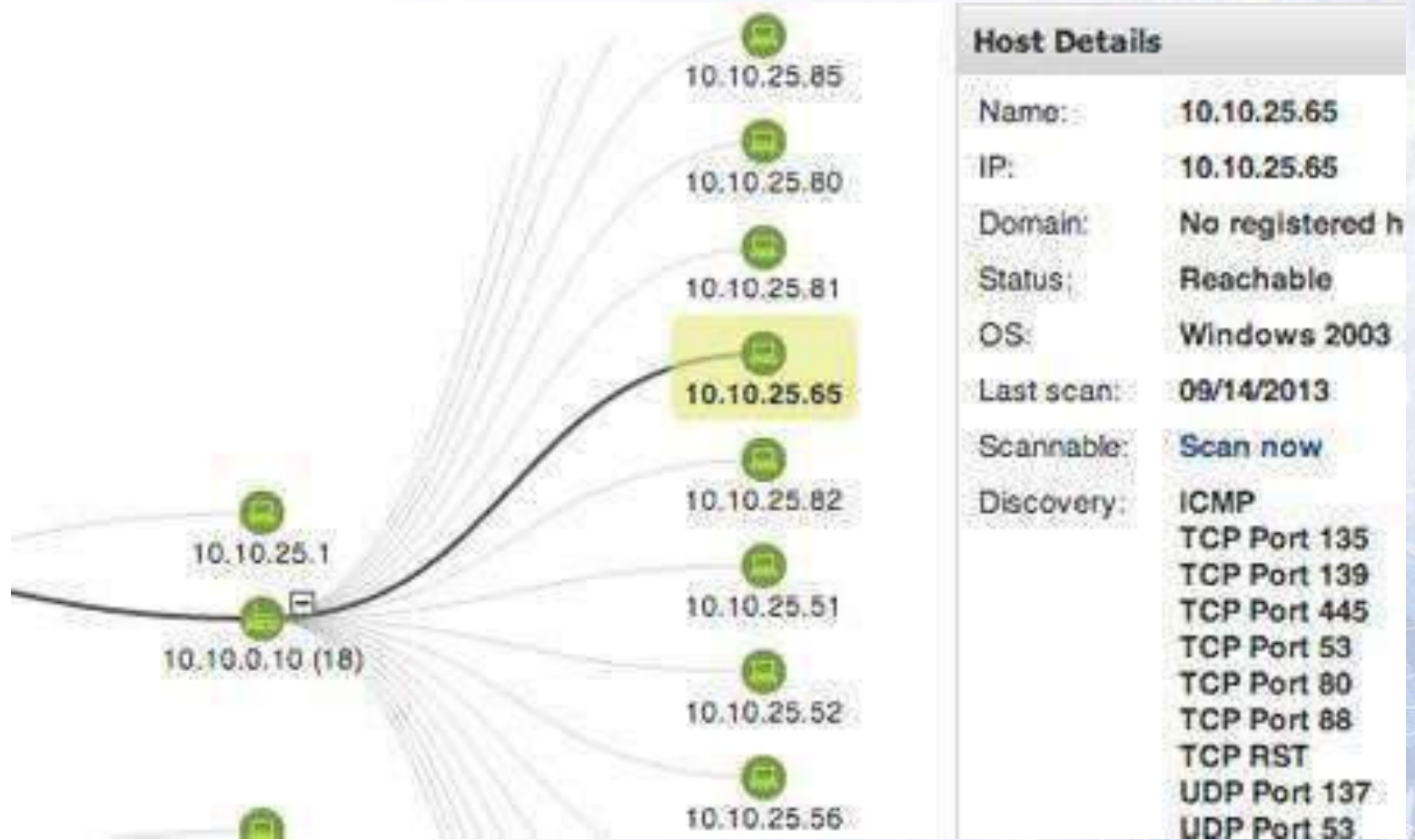
Qualys Features

- Qualys:
 - Cloud-based service
 - On-premise device
 - Complete suite
 - Scalable and immediate deployment

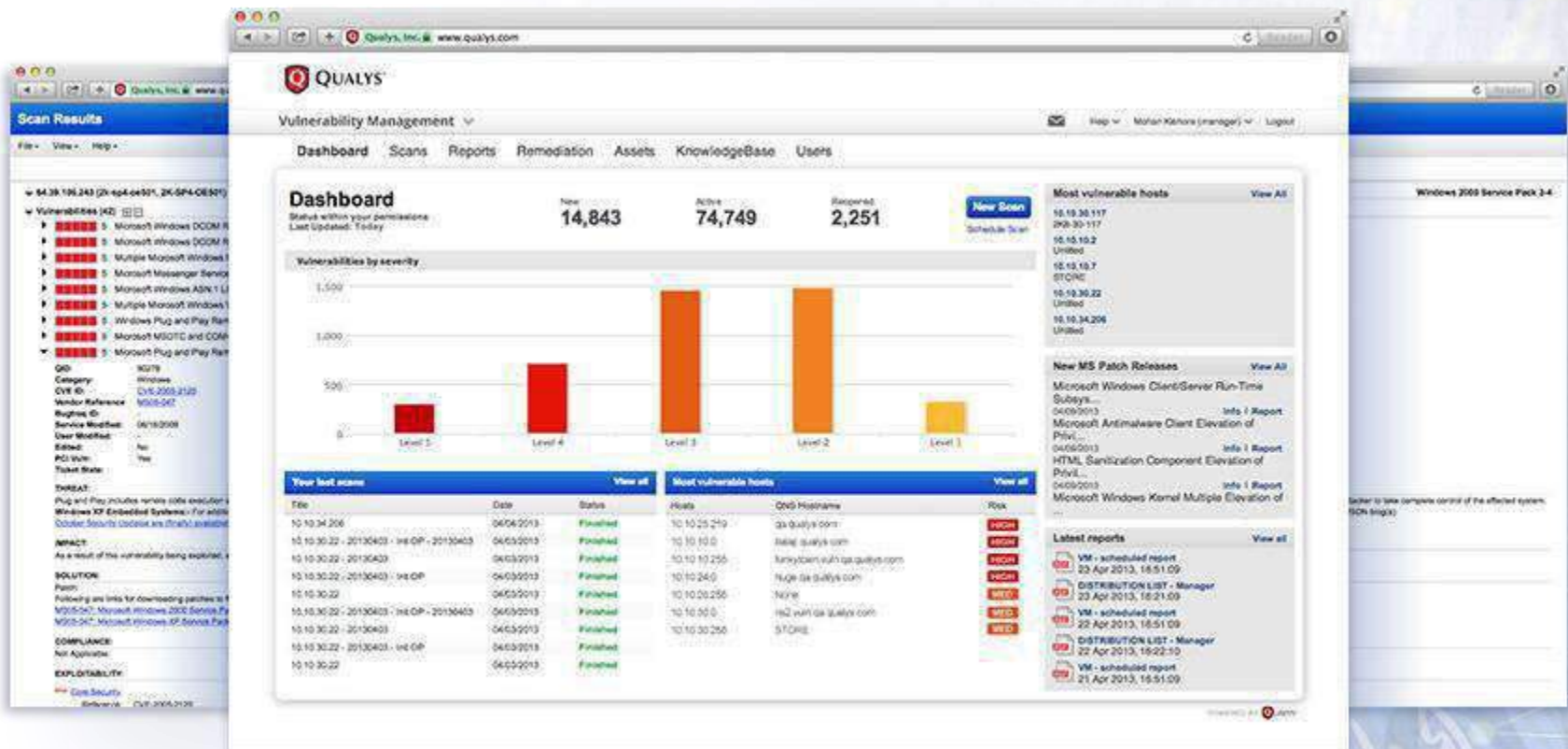
Qualys Features

- Qualys:
 - Asset discovery; find and organize hosts
 - Prioritize & manage remediation tickets
 - Continuous monitoring service
 - Policy compliance scanning
 - Qualys Secure Seal for websites

Qualys Features



Qualys Features



Qualys Features

Patch Report

Report Summary

Agency: Qualys Training
 Created by: Philip Niegos
 Created on: 01/10/2014

Total
Patches

149

Hosts Requiring
Patches

14

Vulnerabilities
Addressed

156

[Report Targets...](#)

HOSTS				PATCHES required on '192.168.1.211' (41)			
DNS Name	NetBIOS	OS	Patches	Vendor ID	Sev.	Title	Published
1.2... centos5.lab.local		CentOS 5.10	41	Apache1.3, A...	3	Apache 1.3 and 2.0 Web Server Multiple ...	6 years ago
1.2... cisco.lab.local		Cisco IOS 12.2(13)ZHI, EA...	40	FEDORA-200...	3	APR-util Library Integer Overflow Vulnera...	4 years ago
1.2... centos6.lab.local		CentOS 6.4	16	Apache 2.2.15	4	Apache HTTP Server Prior to 2.2.15 Multi...	3 years ago
1.2... windows8_1.lab.local	WINDOWSS...	Windows 8.1 Enterprise	10	Tomcat5, To...	3	Apache Tomcat Directory Traversal Weak...	3 years ago
1.2... ws2k8r2.lab.local	WS2K8R2	Windows Server 2008 R2 E...	9	Apache Tomc...	3	Apache Tomcat Servlet Host Manager Ser...	5 years ago
1.2... winserver2012.lab.lo...	WINSERVE...	Windows Server 2012 Stand...	7	Apache Tomc...	3	Apache Tomcat 5 and 6 Host Manager W...	5 years ago
1.2... vistax64.lab.local	VISTAX64	Windows Vista 64 bit Editio...	6	Tomcat4, To...	3	Apache Tomcat RequestDispatcher Infor...	5 years ago
1.2... win7x64.lab.local	WIN7X64	Windows 7 Ultimate 64 bit ...	5	Apache Tomc...	3	Apache Tomcat Java AJP Connector Invali...	4 years ago
Page 1 of 1	Filter	X	1 - 14 of 14	Page 1 of 2	Filter	X	

Qualys Features

The screenshot displays the QualysGuard Vulnerability Management interface. At the top, the QualysGuard logo is visible. Below it, a navigation bar includes links for Dashboard, Scans, Reports, Remediation, Assets, KnowledgeBase, and Users. The KnowledgeBase section is active, showing sub-tabs for KnowledgeBase, Predictions, Search Lists, and iDefense Intelligence. A 'New' dropdown and a 'Search' button are located above the table. The table lists several vulnerabilities with columns for QID, Title, Severity, Category, CVE ID, and Vendor R.

QID	Title	Severity	Category	CVE ID	Vendor R
1013	Hack a Tack backdoor detected	5	Backdoors and trojan horses		
1015	"NetBus" Backdoor	5	Backdoors and trojan horses		
1020	Potential Remote Shell Trojan	5	Backdoors and trojan horses		
1021	Installed Back Orifice 2000	5	Backdoors and trojan horses		
1135	Sasser Worm Detected	5	Backdoors and trojan horses		

Qualys Features

The image displays the Qualys SECURE SEAL interface. At the top, the Qualys logo is followed by the text "QUALYS® SECURE SEAL". Below this is a navigation bar with a home icon, the text "Qualys SECURE Seal", and a dropdown menu showing the URL "http://funkytown.vuln.qa.qualys.com". The main content area shows the same URL. On the left, there is a sidebar with links: "Results" (with a magnifying glass icon), "History" (with a clock icon), "Exceptions" (with a document icon), and "Recommend to Others" (with a person icon). Below these links is a "Filter Results" section with three checkboxes: "Perimeter", "Web Application", and "Malware". The main content area displays the "Seal Status: FAIL" in red, "Scan Status: Finished" in blue, and the "URL: http://funkytown.vuln.qa.qualys.com/cassium/xs/10.10.26.77". At the bottom, there are four icons representing different security checks: "Perimeter" (cloud icon), "Web App" (document icon), "Malware" (biohazard icon), and "Certificate" (lock icon). Each icon has a red "X" mark, indicating a failure in all four categories.

QUALYS® SECURE SEAL

Qualys SECURE Seal <http://funkytown.vuln.qa.qualys.com>

<http://funkytown.vuln.qa.qualys.com>

Results

History

Exceptions

Recommend to Others

Filter Results

- ☐ Perimeter
- ☐ Web Application
- ☐ Malware

Seal Status: **FAIL**

Scan Status: **Finished**

URL: <http://funkytown.vuln.qa.qualys.com/cassium/xs/10.10.26.77>

Perimeter Web App Malware Certificate

Qualys Features

- Qualys:
 - Website scanning
 - compliance
 - Annual subscription service model

Qualys Features

- Qualys is a convenient and scalable VM tool that comes with several modules
- Subscription-based pricing model which can be expensive
- Several advantages due to cloud-based service

Nessus Demo - 1

- Lets take a look at Nessus Demo
- <https://www.tenable.com/products/nessus/nessus-professional/evaluate>
- Download free 7 day trial
- Get activation key from website

Nessus Demo - 1

LOGIN SCREEN



The screenshot shows a web browser window with the title "Nessus / Login". The address bar displays "https://localhost:8834/#/". The main content area features a large, faint background graphic of a cube. Overlaid on this is a white login form with the Nessus logo at the top. The form contains a username field with the text "nahil", a password field with masked characters, a "Remember Me" checkbox which is checked, and a "Sign In" button. The Tenable logo is visible in the bottom right corner of the page.

Nessus / Login

https://localhost:8834/#/

Nessus
home

nahil

.....

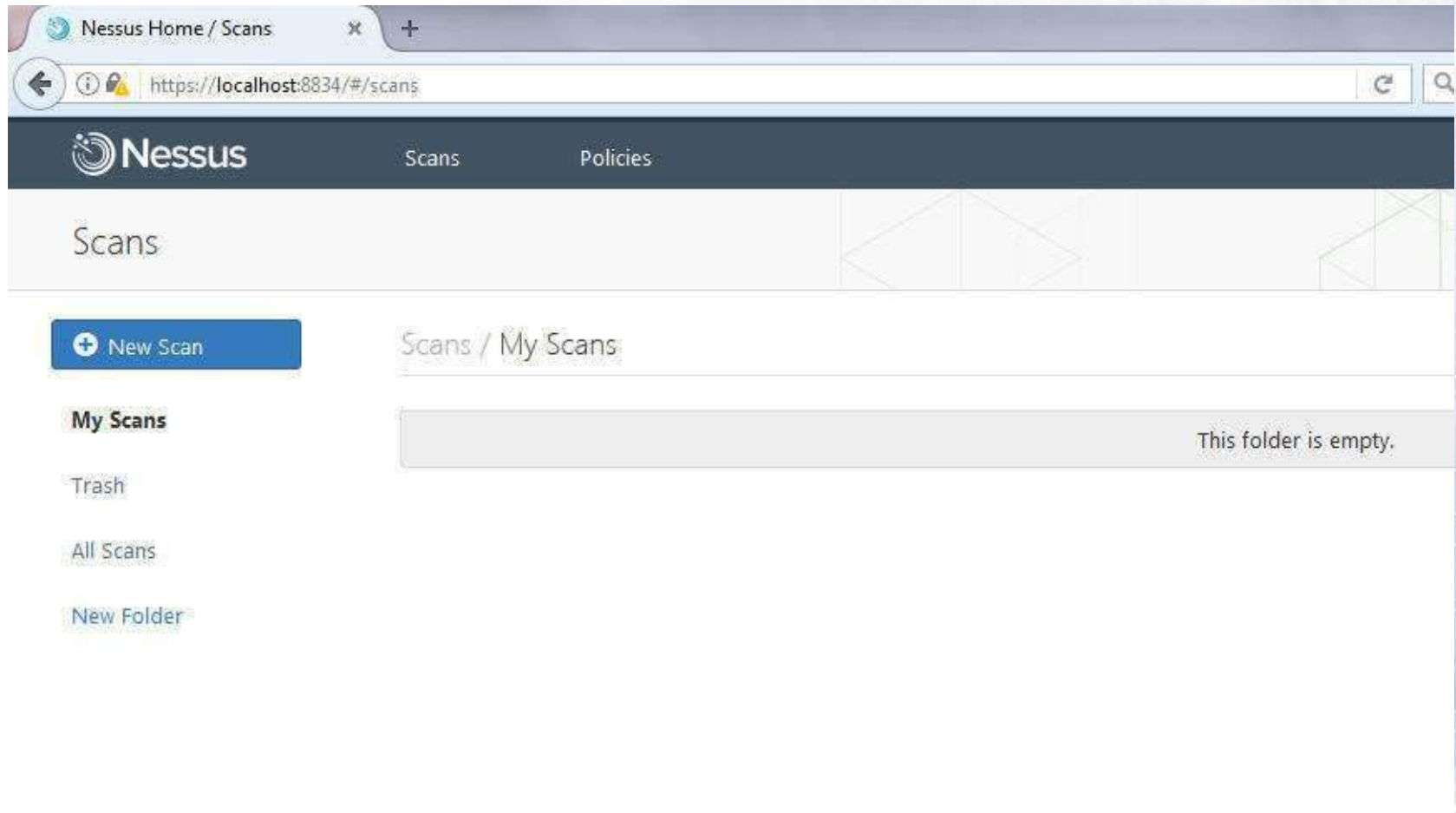
☒ Remember Me

Sign In

tenable
network security

Nessus Demo - 1

DASHBOARD



Nessus Demo - 1

NEW SCAN

Scanner Templates

 Advanced Scan Configure a scan without using any recommendations.	 Audit Cloud Infrastructure Audit the configuration of third-party cloud services. UPGRADE	 Badlock Detection Remote and local checks for CVE-2016-2118 and	 Bash Shellshock Detection Remote and local checks for CVE-2014-6271 and	 Basic Network Scan A full system scan suitable for any host.
 Credentialed Patch Audit Authenticate to hosts and enumerate missing updates.	 DROWN Detection Remote checks for CVE-2016-0800.	 Host Discovery A simple scan to discover live hosts and open ports.	 Intel AMT Security Bypass Remote and local checks for CVE-2017-5689.	 Internal PCI Network Scan Perform an internal PCI DSS (11.2.1) vulnerability scan. UPGRADE
 Malware Scan Scan for malware on Windows and Unix systems.	 MDM Config Audit Audit the configuration of mobile device managers. UPGRADE	 Mobile Device Scan Assess mobile devices via Microsoft Exchange or an MDM. UPGRADE	 Offline Config Audit Audit the configuration of network devices. UPGRADE	 PCI Quarterly External Scan Approved for quarterly external scanning as required by PCI. UPGRADE
 Policy Compliance Auditing Audit system configurations against a known baseline. UPGRADE	 SCAP and OVAL Auditing Audit systems using SCAP and OVAL definitions. UPGRADE	 Shadow Brokers Scan Scan for vulnerabilities disclosed in the Shadow Brokers leaks.	 WannaCry Ransomware Remote and local checks for MS17-010.	 Web Application Tests Scan for published and unknown web vulnerabilities.

Nessus Demo - 1

WANNACRY RANSOMWARE SCAN



WannaCry Ransomware

Remote and local checks for
MS17-010.

Nessus Demo - 1

NEW SCAN WINDOW

New Scan / WannaCry Ransomware

Scan Library > Settings Credentials

BASIC

General

Schedule

Notifications

DISCOVERY

REPORT

ADVANCED

Settings / Basic / General

This policy is used to perform remote and local checks for vulnerabilities exploited by WannaCry Ransomware (MS17-010 / CVE-2017-0144) be provided to test via WMI and enumerate missing software updates.

Name

REQUIRED

Description

Folder

My Scans

Targets

Example: 192.168.1.1-192.168.1.5, 192.168.2.0/24, test.com

REQUIRED

Nessus Demo - 1

DASHBOARD VIEW WITH SCANS

Scans

Upload

Search Scans

New Scan

Scans / My Scans

My Scans

Trash

All Scans

New Folder

☐	Name	Schedule	Last Modified		
☐	LOCAL PC WANNACRY	On Demand	✓ 12:53 AM	▶	✕
☐	NAHIL PC	On Demand	📅 N/A	▶	✕

Nessus Demo - 1

NEW SCAN...

Scanner Templates



Advanced Scan

Configure a scan without using any recommendations.



UPGRADE

Audit Cloud Infrastructure

Audit the configuration of third-party cloud services.



Credentialed Patch Audit

Authenticate to hosts and enumerate missing updates.



DROWN Detection

Remote checks for CVE-2016-0800.

Nessus Demo - 1

ENTER SCAN DETAILS

New Scan / Advanced Scan

Scan Library > **Settings** Credentials Compliance Plugins

BASIC ✓ Settings / Basic / General

General

Schedule

Notifications

DISCOVERY

ASSESSMENT

REPORT

ADVANCED

Name LOCALHOST ADVANCED SCAN

Description ADVANCED SCAN

Folder My Scans ▼

Targets LOCALHOST|

Nessus Demo - 1

CREDENTIAL SCAN

LOCALHOST ADVANCED SCAN / Confi...
POLICY: ADVANCED SCAN

Scan > Settings Credentials Compliance Plugins

CREDENTIALS

▶ Cloud Services

▶ Database

▼ Host

SNMPv3 1 +

SSH ∞ +

Windows ∞ +

▶ Miscellaneous

▶ Plaintext Authentication

ACTIVE CREDENTIALS

Save

Cancel

Nessus Demo - 1

COMPLIANCE SCAN

LOCALHOST ADVANCED SCAN / Confi...

POLICY: ADVANCED SCAN

Scan > Settings Credentials Compliance Plugins

COMPLIANCE CHECKS

▶ Adtran AOS

▶ Amazon AWS

▶ Arista EOS

▶ BlueCoat ProxySG

▶ Brocade FabricOS

▶ Check Point GAiA

▶ Cisco IOS

▶ Citrix XenServer

▶ Database

▶ Dell Force10 FTOS

ACTIVE COMPLIAN

Nessus Demo - 1

WINDOWS COMPLIANCE MENU (CIS)

▸ Unix File Contents	
▸ VMware vCenter/vSphere	
▸ WatchGuard	
▼ Windows	
(Upload a custom Windows audit file)	∞ +
CIS Exchange 2007 Enterprise Edge Transport 1...	1 +
CIS Google Chrome L1 v1.1.0	1 +
CIS Google Chrome L2 v1.1.0	1 +
CIS IE 10 v1.1.0	1 +
CIS IE 11 v1.0.0	1 +
CIS IE 9 v1.0.0	1 +
CIS IIS 10 v1.0.0 Level 1	1 +
CIS IIS 10 v1.0.0 Level 2	1 +
CIS IIS 6.0 v1.0.0	1 +
CIS IIS 7 L2 v1.8.0	1 +
CIS IIS 8.0 v1.5.0 Level 1	1 +
CIS IIS 8.0 v1.5.0 Level 2	1 +

Nessus Demo - 1

WINDOWS COMPLIANCE MENU (CIS)...

ACTIVE COMPLIANCE CHECKS

CIS IIS 7 L1 v1.8.0	×
CIS Microsoft Office Outlook 2013 v1.1.0 Level 1	×
CIS Microsoft Office 2013 v1.1.0	×
CIS Microsoft Office Word 2013 v1.1.0	×
CIS IE 10 v1.1.0	×
▶ CIS Google Chrome L1 v1.1.0	×
CIS Microsoft Office PowerPoint 2013 v1.0.1	×
CIS Windows 7 Level 2 v3.0.1	×
▼ DISA STIG Google Chrome V1R8	×

Nessus Demo - 1

- Lets take a look at Nessus Demo
- <https://www.tenable.com/products/nessus/nessus-professional/evaluate>
- Download free 7 day trial
- Get activation key from website

Nessus Demo - 2

- Lets take a look at Nessus Demo
- <https://www.tenable.com/products/nessus/nessus-professional/evaluate>
- Download free 7 day trial
- Get activation key from website

Nessus Demo - 2

ADVANCED SCAN / COMPLIANCE

ACTIVE COMPLIANCE CHECKS

CIS IIS 7 L1 v1.8.0



CIS Microsoft Office Outlook 2013 v1.1.0 Level 1



CIS Microsoft Office 2013 v1.1.0



CIS Microsoft Office Word 2013 v1.1.0



CIS IE 10 v1.1.0



▶ CIS Google Chrome L1 v1.1.0



CIS Microsoft Office PowerPoint 2013 v1.0.1



CIS Windows 7 Level 2 v3.0.1



▼ **DISA STIG Google Chrome V1R8**



Nessus Demo - 2

ADVANCED SCAN / PLUG-INS

LOCALHOST ADVANCED SCAN / Confi... Disable All Enable All

Scan > **Settings** **Credentials** **Compliance** **Plugins**

[Show Enabled](#) | [Show All](#)

DISABLED	SuSE Local Security Checks	10107
DISABLED	Ubuntu Local Security Checks	3763
DISABLED	Virtuozzo Local Security Checks	130
DISABLED	VMware ESX Local Security Checks	114
DISABLED	Web Servers	1018
DISABLED	Windows	3772
ENABLED	Windows : Microsoft Bulletins	1323
DISABLED	Windows : User management	28

Status	Plugin Name	Plugin ID
ENABLED	2X ApplicationServer TuxSystem ActiveX ExportSettings() Method Ar...	58484
ENABLED	2X Client TuxClientSystem ActiveX InstallClient() Method Arbitrary M...	58321
ENABLED	3CTftpSvc Long Transport Mode Remote Overflow	23735
ENABLED	3D-FTP Multiple Directory Traversal Vulnerabilities	33218
ENABLED	3DGreetings Player ActiveX Multiple Buffer Overflows	26020
ENABLED	3ivx MPEG-4 < 5.0.2 Buffer Overflow	29749
ENABLED	7-Zip < 16.00 Multiple Vulnerabilities	91230

Save Cancel

Nessus Demo - 2

SCAN...IN PROGRESS

Scans

Upload

Search Scans

+ New Scan

My Scans

1

Trash

1

All Scans

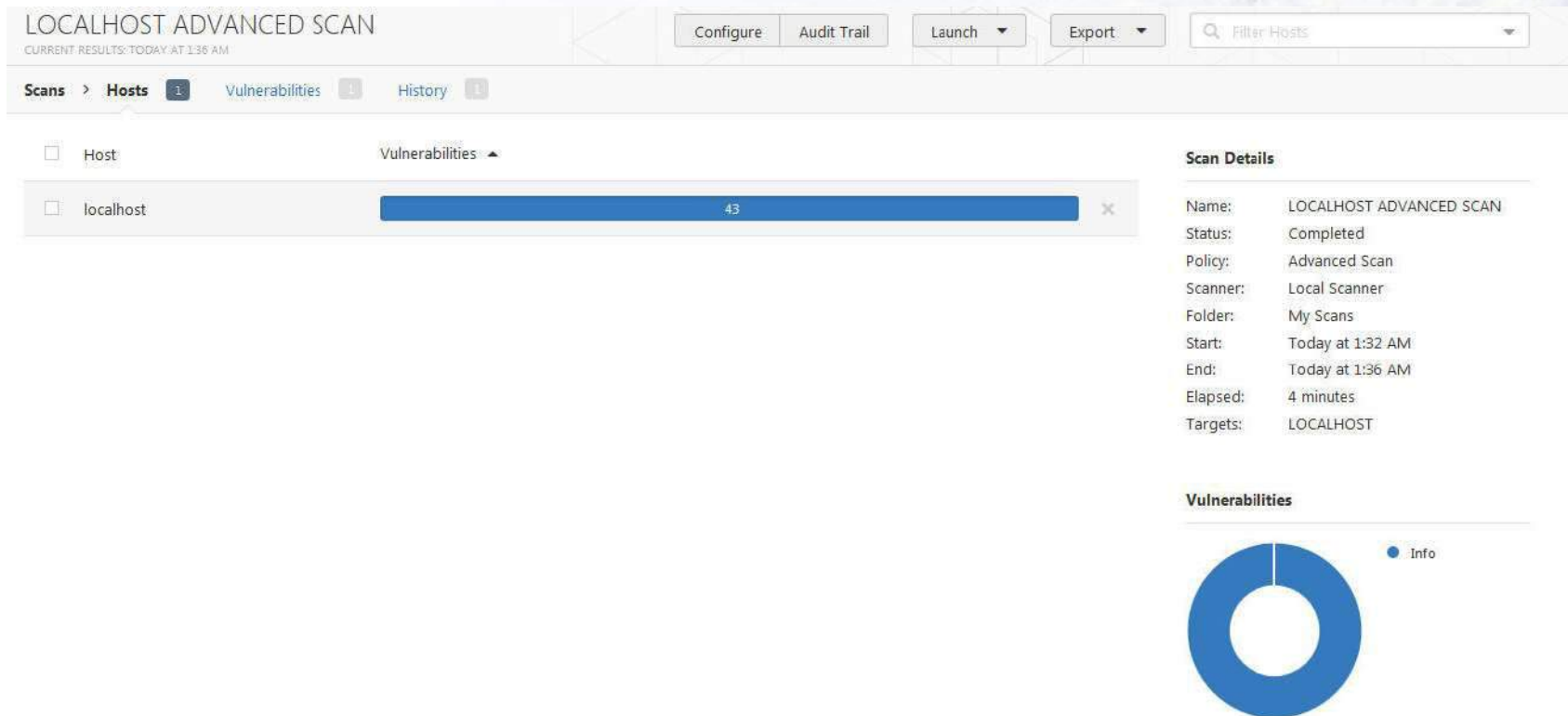
New Folder

Scans / My Scans

☐	Name	Schedule	Last Modified ▲	
☐	LOCALHOST ADVANCED SCAN	On Demand	 01:32 AM	

Nessus Demo - 2

SCAN REPORT [43 INFO]



Nessus Demo - 2

SCAN REPORT [DETAILS]

LOCALHOST ADVANCED SCAN
CURRENT RESULTS: TODAY AT 1:36 AM

Configure

Audit Trail

Launch ▼

Export ▼

Hosts > localhost > Vulnerabilities 1

☐	Severity ▲	Plugin Name	Plugin Family	Count
☐	INFO	Netstat Portscanner (SSH)	Port scanners	43

Host Details

IP: 127.0.0.1
DNS: localhost
OS: Microsoft Windows 7 Home
Start: Today at 1:32 AM
End: Today at 1:36 AM
Elapsed: 4 minutes
KB: [Download](#)

Vulnerabilities

Info



Nessus Demo - 2

SCAN REPORT [DETAILS...]

<https://en.wikipedia.org/wiki/Netstat>

Output

Port 68/udp was found to be open

Port ▼	Hosts
68 / udp	localhost 

Port 123/udp was found to be open

Port ▼	Hosts
123 / udp	localhost 

Port 135/tcp was found to be open

Port ▼	Hosts
135 / tcp / epmap	localhost 

Port 137/udp was found to be open

Port ▼	Hosts
137 / udp	localhost 

Nessus Demo - 2

WEB APPLICATION TEST

Audit

ration of
ices,

PCI Quarterly External Scan

Approved for quarterly external
scanning as required by PCI.

omware

checks for
l,



Web Application Tests

Scan for published and unknown
web vulnerabilities.

Nessus Demo - 2

WEB APPLICATION TEST - CREDENTIALS

New Scan / Web Application Tests

Scan Library > Settings Credentials

CREDENTIALS

All credentials in use

ACTIVE CREDENTIALS

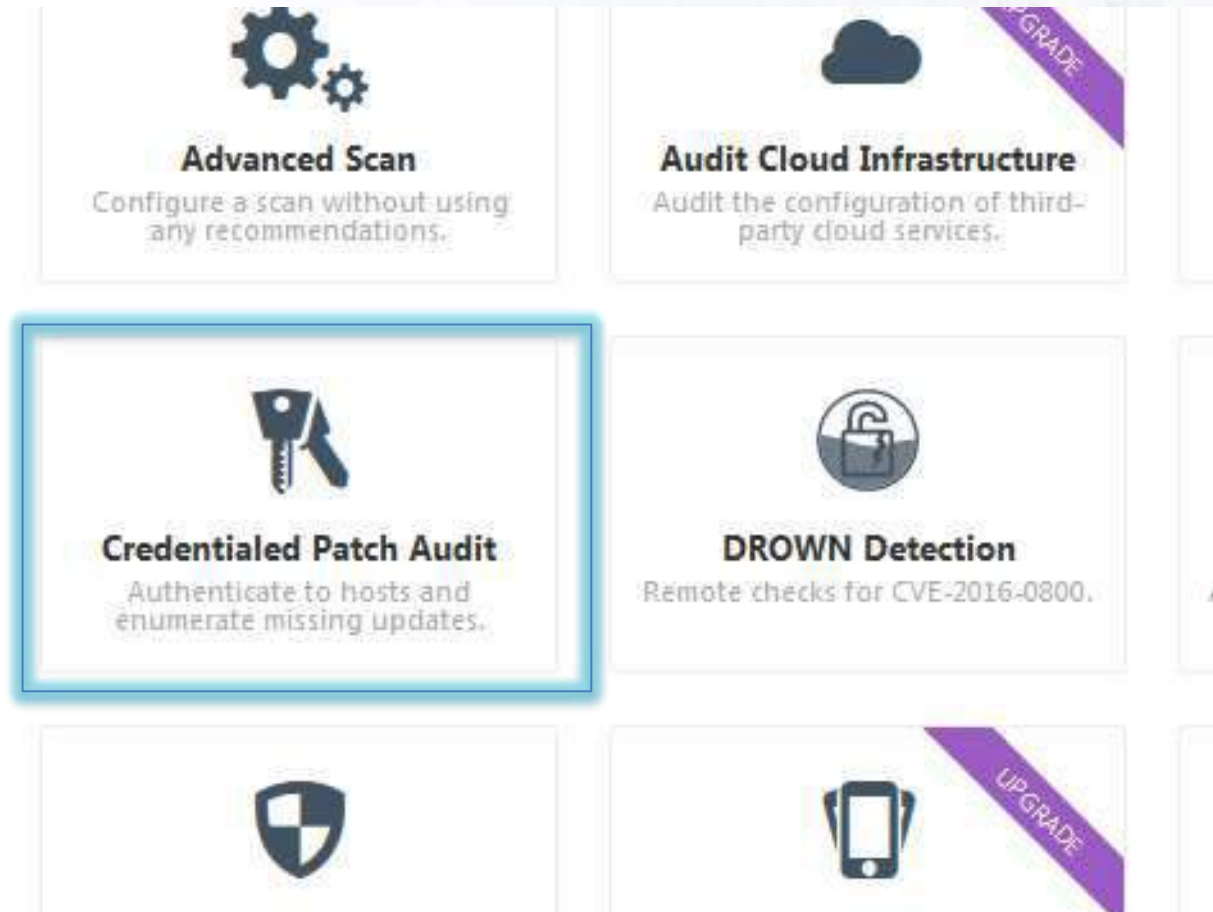
HTTP

Authentication method	HTTP login form
Username	admin REQUIRED
Password	REQUIRED
Login page	/login.php REQUIRED
Login submission page	/process_login.php REQUIRED
Login parameters	user=%USER%&pass=%PASS% REQUIRED

If the keywords %USER% and %PASS% are used, they will be substituted with the values above.

Nessus Demo - 2

CREDENTIALIALED PATCH AUDIT



Nessus Demo - 2

CREDENTIALIALED PATCH AUDIT

New Scan / Credentialed Patch Audit

Scan Library > Settings Credentials

CREDENTIALS

- Database
- Host
 - SSH
 - Windows
- Miscellaneous
- Plaintext Authentication

ACTIVE CREDENTIALS

Windows

Authentication method: Password

Username: administrator

Password:

Domain:

Global Settings

- ☒ Never send credentials in the clear
- ☒ Do not use NTLMv1 authentication

Nessus Demo - 2

SCANS DASHBOARD

Scans

New Scan

My Scans

1

Trash

1

All Scans

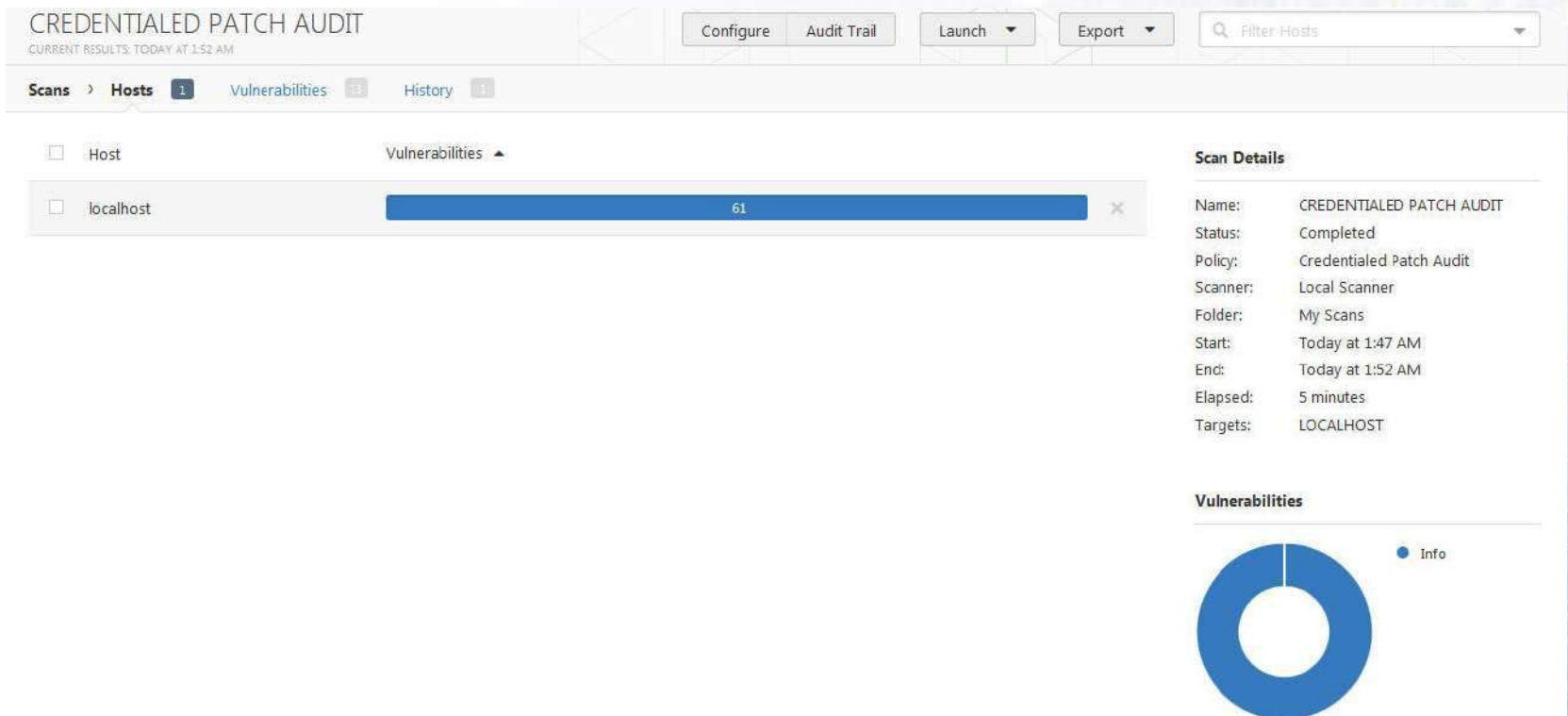
New Folder

Scans / My Scans

☐	Name	Schedule	Last Modified ▲		
☐	CREDENTIALIAED PATCH AUDIT	On Demand	 01:47 AM		■
☐	LOCALHOST ADVANCED SCAN	On Demand	 01:36 AM	▶	✕

Nessus Demo - 2

CREDENTIALIALED AUDIT SCAN RESULTS [61 INFO]



Nessus Demo - 2

CREDENTIALIALED AUDIT SCAN RESULTS [61 INFO]

CREDENTIALIALED PATCH AUDIT
CURRENT RESULTS: TODAY AT 1:52 AM

Configure Audit Trail Launch Export Filter Vulnerabilities

Hosts > localhost > Vulnerabilities 13

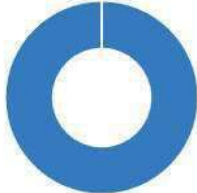
Severity	Plugin Name	Plugin Family	Count
INFO	Netstat Portscanner (SSH)	Port scanners	43
INFO	DCE Services Enumeration	Windows	7
INFO	Authenticated Check : OS Name and Installed Package Enumeration	Settings	1
INFO	Authentication Failure - Local Checks Not Run	Settings	1
INFO	Microsoft Windows NTLMSSP Authentication Request Remote Network Nam...	Windows	1
INFO	Microsoft Windows SMB Log In Possible	Windows	1
INFO	Microsoft Windows SMB NativeLanManager Remote System Information Dis...	Windows	1
INFO	Microsoft Windows SMB Registry : Nessus Cannot Access the Windows Regi...	Windows	1
INFO	Microsoft Windows SMB Service Detection	Windows	1

Host Details

IP: 127.0.0.1
DNS: localhost
OS: Microsoft Windows 7 Home
Start: Today at 1:47 AM
End: Today at 1:52 AM
Elapsed: 5 minutes
KB: [Download](#)

Vulnerabilities

Info



Nessus Demo - 2

CREDENTIALIALED AUDIT SCAN RESULTS [DETAILS]

INFO Netstat Portscanner (SSH) >

Description

Nessus was able to run 'netstat' on the remote host to enumerate the open ports.

See the section 'plugins options' about configuring this plugin.

See Also

<https://en.wikipedia.org/wiki/Netstat>

Output

Port 68/udp was found to be open

Port ▼	Hosts
68 / udp	localhost 

Port 123/udp was found to be open

Port ▼	Hosts
123 / udp	localhost 

Port 135/tcp was found to be open

Plugin Details

Severity:	Info
ID:	14272
Version:	1.68
Type:	remote
Family:	Port scanners
Published:	2004/08/15
Modified:	2017/06/16

Risk Information

Risk Factor: None

Nessus Demo - 2

- Lets take a look at Nessus Demo
- <https://www.tenable.com/products/nessus/nessus-professional/evaluate>
- Download free 7 day trial
- Get activation key from website

Nessus Demo - 3

- Lets take a look at Nessus Demo
- <https://www.tenable.com/products/nessus/nessus-professional/evaluate>
- Download free 7 day trial
- Get activation key from website

Nessus Demo - 3

SYSTEM MALWARE SCAN

Credentialed Patch Audit Authenticate to hosts and enumerate missing updates.	DROWN Detection Remote checks for CVE-2016-0800.
 Malware Scan Scan for malware on Windows and Unix systems.	 MDM Config Audit Audit the configuration of mobile device managers.
 Policy Compliance Auditing Audit system configurations against a known baseline.	 SCAP and OVAL Auditing Audit systems using SCAP and OVAL definitions.

Nessus Demo - 3

SYSTEM MALWARE SCAN

New Scan / Malware Scan

Scan Library > Settings Credentials

CREDENTIALS

Host
SSH  
Windows  

ACTIVE CREDENTIALS

Windows

Authentication method Password 

Username administrator

Password 

Domain

Global Settings

- ☒ Never send credentials in the clear
- ☒ Do not use NTLMv1 authentication
- ☐ Start the Remote Registry service during the scan

Nessus Demo - 3

SCAN DASHBOARD

Scans

+ New Scan

My Scans

1

Trash

1

All Scans

New Folder

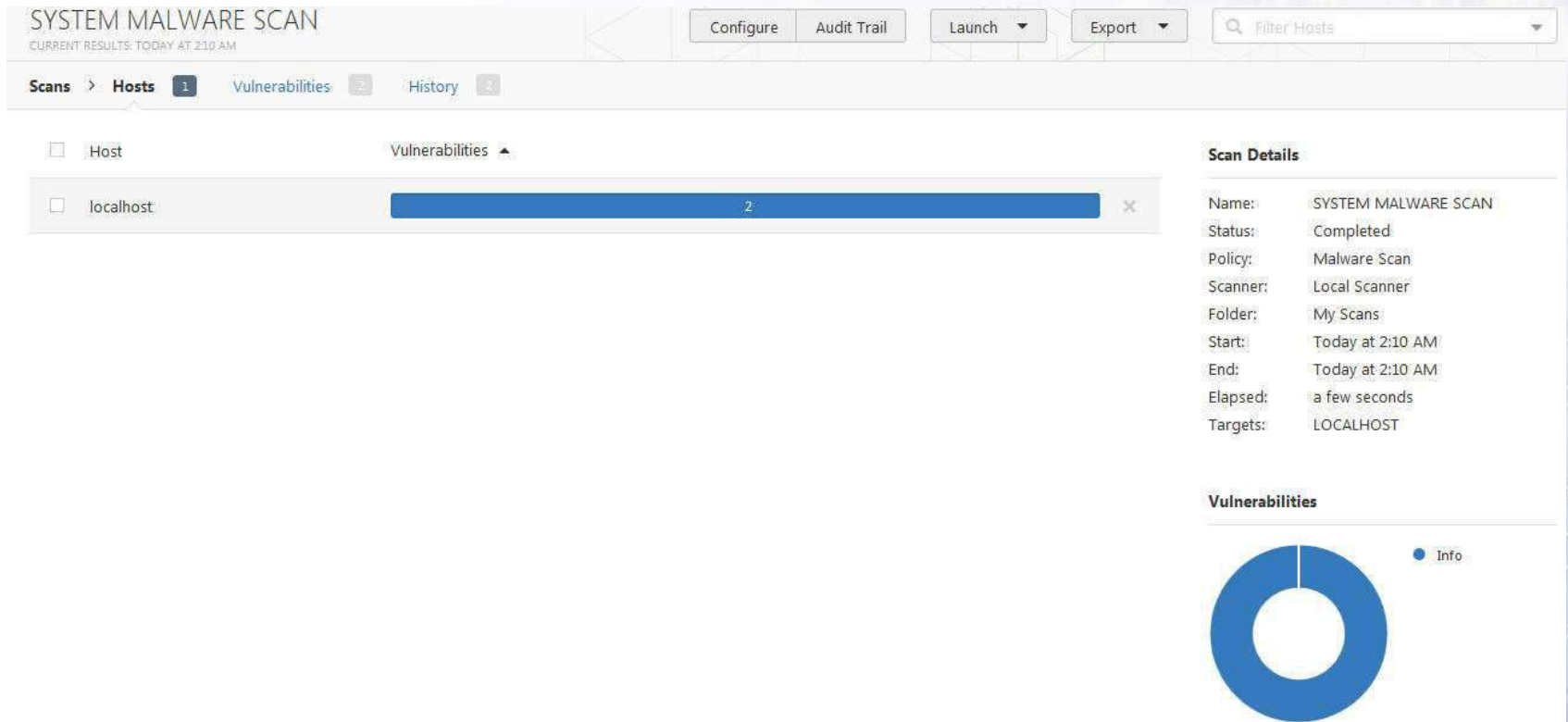
Scans / My Scans

☐	Name	Schedule	Last Modified ▲		
☐	WEBSITE	On Demand	 02:16 AM		■
☐	SYSTEM MALWARE SCAN	On Demand	✓ 02:10 AM	▶	✕
☐	CREDENTIAL PATCH AUDIT	On Demand	✓ 01:52 AM	▶	✕
☐	LOCALHOST ADVANCED SCAN	On Demand	✓ 01:36 AM	▶	✕

© 1996 - 2017 Tenable Network Security®. All Rights Reserved. Nessus Home v. 6.10.9

Nessus Demo - 3

SYSTEM MALWARE SCAN [2 INFO]



Nessus Demo - 3

SYSTEM MALWARE SCAN

SYSTEM MALWARE SCAN

CURRENT RESULTS: TODAY AT 2:10 AM

[Configure](#)[Audit Trail](#)[Launch](#)[Export](#)

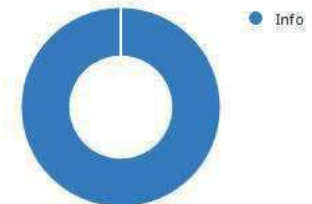
[Hosts](#) > [localhost](#) > [Vulnerabilities](#) **2**

☐	Severity ▲	Plugin Name	Plugin Family	Count
☐	INFO	Authentication Failure - Local Checks Not Run	Settings	1
☐	INFO	Nessus Windows Scan Not Performed with Admin Privileges	Settings	1

Host Details

IP: 127.0.0.1
DNS: localhost
Start: Today at 2:10 AM
End: Today at 2:10 AM
Elapsed: a few seconds
KB: [Download](#)

Vulnerabilities



Nessus Demo - 3

- Nessus is an easy to use and powerful scanner
- Dozens of scans on dashboard
- Setup a new scan
- Setup a profile as scan template
- Credentialed scan
- Thousands of plugins from CIS/DISA etc

END

Qualys Demo - 1

- Lets take a look at Qualys Demo
- Free Qualys tools:
 - BrowserCheck
 - SSL
- Qualys FreeScan
 - Vulnerability
 - OWASP
 - Patch Tuesday
 - SCAP

Qualys Demo - 1

QUALYS BROWSER CHECK

 **QUALYS® BROWSERCHECK**

[About](#) [FAQ](#) [Feedback](#) [Qualys.com](#)

Qualys® BrowserCheck Summary

Scan start time: **Sun Jul 16 2017, 1:01 AM**
Scan duration: **00:02** (mm:ss)

Congratulations! You passed Qualys BrowserCheck.
We recommend you scan your browser regularly to stay up to date with the latest versions and plugins.

Re-Scan



Google Chrome
59.0.3071.115

Up To Date

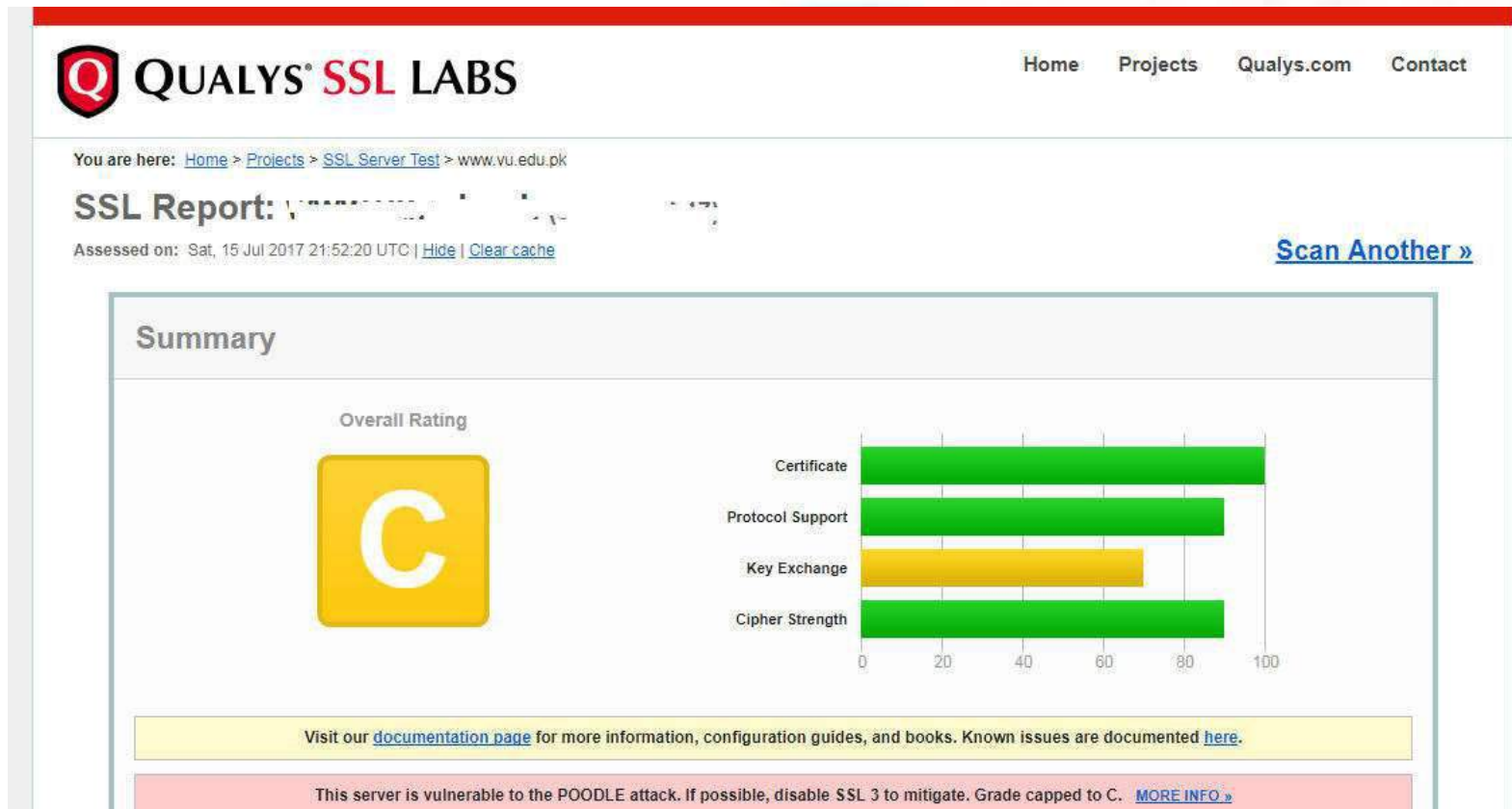


BROWSERCHECK
BUSINESS EDITION

Browser security for your organization

Qualys Demo - 1

SSL LABS REPORT

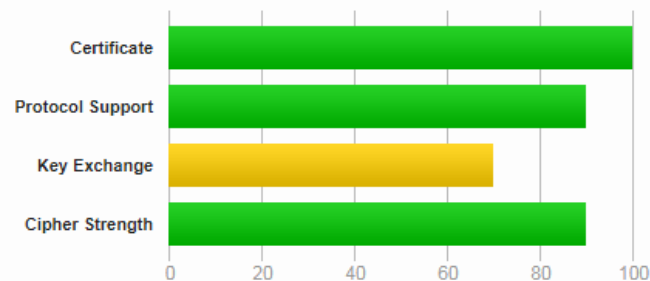


Qualys Demo - 1

SSL LABS REPORT

Summary

Overall Rating



Visit our [documentation page](#) for more information, configuration guides, and books. Known issues are documented [here](#).

This server is vulnerable to the POODLE attack. If possible, disable SSL 3 to mitigate. Grade capped to C. [MORE INFO »](#)

This server supports weak Diffie-Hellman (DH) key exchange parameters. Grade capped to B. [MORE INFO »](#)

This server accepts RC4 cipher, but only with older protocols. Grade capped to B. [MORE INFO »](#)

The server does not support Forward Secrecy with the reference browsers. [MORE INFO »](#)

Certificate #1: RSA 2048 bits (SHA256withRSA)

Qualys Demo - 1

PROTOCOL DETAILS

BEAST attack	Not mitigated server-side (more info)	SSL 3: 0xa, TLS 1.0: 0xc014
POODLE (SSLv3)	Vulnerable INSECURE (more info)	SSL 3: 0xa
POODLE (TLS)	No (more info)	
Downgrade attack prevention	No, TLS_FALLBACK_SCSV not supported (more info)	
SSL/TLS compression	No	
RC4	Yes INSECURE (more info)	
Heartbeat (extension)	No	
Heartbleed (vulnerability)	No (more info)	
Ticketbleed (vulnerability)	No (more info)	
OpenSSL CCS vuln. (CVE-2014-0224)	No (more info)	
OpenSSL Padding Oracle vuln. (CVE-2016-2107)	No (more info)	
Forward Secrecy	Weak key exchange WEAK	
ALPN	No	

Qualys Demo - 1

QUALYS FREESCAN

New Scan

Enter URL or IP address

Scan a URL and receive results on Web Application and Network Vulnerabilities, OWASP Security Risks, and Malware audits.
Or, enter an IP address to scan external or internal hosts for Vulnerabilities, authenticated Patch Tuesday audits, or run a SCAP compliance scan.

Choose Scan Type



VULNERABILITY
Network | WAS | MDS Scans



OWASP
Risk Scan



PATCH TUESDAY
Authenticated Scan



SCAP
Compliance Scan

Last Scan Result

OWASP Scan

Summary: No OWASP Categorie...

<http://www.delt...>

16 Jul 2017



Vulnerability Summary

VM(33) WAS(0) MDS(0)



Patch Audit Summary

4 Patches | 4 Vulns Addressed

Last 5 Scan Results

16 Jul 2017 <http://www.deltatechglobal.com>



16 Jul 2017 <http://www.deltatechglobal.com>

[View](#) [Rescan](#)

16 Jul 2017 <http://www.vu.edu.pk>



Qualys Demo - 1



Welcome Nahil

Thanks for choosing Qualys FreeScan. Using FreeScan you can quickly and easily verify the security of your business.

[Back to Home](#)

[Quick Tour](#) | [Upgrade Now](#) | [Nahil Mahmood](#) | [2 Scans](#)

Scan in Progress

[Cancel scan](#)

<http://www.delfin-tech.com>

Vulnerability Scan



In progress

Web Application Scan



In progress

Malware Detection



Scan complete

Scan in Progress

[Cancel scan](#)

<http://www.delfin-tech.com>

Vulnerability Scan



3 threats

Scan complete

Web Application Scan



In progress

Malware Detection



Scan complete

OWASP Scan rename

Summary: No OWASP Categories Found.

Threat Summary: 33 Vulnerabilities Found

Patch Report Summary: 4 Patches Available

<http://www.delfin-tech.com>

16 July 2017 at 1:25AM (GMT+0500)



[View Report >](#)

Qualys Demo - 1

OWASP SCAN PATCH REPORT



OWASP Scan [rename](#)
No Authentication Used

16 July 2017 at 11:25AM (GMT+0500)

4

Patches
Required

4

Vulnerabilities
Addressed

<http://www.deltatag.com>

www.deltatag.com
Ubuntu / Linux 2.6.x

Rescan URL

Filter by:

All (4) Microsoft (0) Oracle (0) Adobe (0) Others (4)

Patches

1 - 4 of 4 < >

OpenSSH LoginGraceTime Denial of Service Vulnerability	1
OpenSSH Commands Information Disclosure Vulnerability	1
OpenSSH J-PAKE Session Key Retrieval Vulnerability	1
OpenSSH "X SECURITY" Bypass Vulnerability	1

OpenSSH LoginGraceTime Denial of Service Vulnerability

QID: 42413

Published: 09 February 2013

Vendor ID: [OpenSSH](#)

CVE: [CVE-2010-5107](#)

Solution:

Customers are advised to upgrade to [OpenSSH 6.2](#) and apply the associated server configuration settings to remediate this vulnerability.

1 Vulnerabilities Addressed

QID: 42413

Published: 09 February 2013



OpenSSH LoginGraceTime Denial of Service Vulnerability

Qualys Demo - 1

THREAT REPORT

View by:

OWASP Report

Patch Report

Threat Report

Print Report ▼



OWASP Scan [rename](#)

External Host Vulnerability Report

16 July 2017 at 1:25AM (GMT+0500)

33

Vulnerabilities
Detected

0

HIGH
Risk

10

MED
Risk

23

LOW
Risk

78

INFO
Gathered

<http://www.deltatechglobal.com>

www.deltatechglobal.com

Ubuntu / Linux 2.6.x

Rescan URL

Filter by:

All (33)

Level 5 (0)

Level 4 (0)

Level 3 (10)

Level 2 (20)

Level 1 (3)

Info (78)

Search for Title, Category, CVE ID or QID

All Scan Results

1 - 25 of 111

Mail Server Accepts Plaintext Credentials	■■■
Discovery of Unix Account Names Vulnerability	■■■
Web Server Stopped Responding	■■■
Discovery of Unix Account Names Vulnerability	■■■
POP3 Server Allows Plain Text Authentication Vulnerability	■■■

Mail Server Accepts Plaintext Credentials

QID: 74147

CVE Base: 5.3

Port: 587

CVSS Temporal: 4.8

Category: Mail
services

CVE ID: -

Threat:

Your Mail Server responds to the EHLO command which implies that it uses the ESMTP protocol. ESMTP uses the AUTH command which indicates an authentication mechanism to the server. If the server supports the requested authentication mechanism, it performs an authentication protocol exchange to

Qualys Demo - 1

THREAT REPORT

Filter by:

All (33)

Level 5 (0)

Level 4 (0)

Level 3 (10)

Level 2 (20)

Level 1 (3)

Info (78)

Search for Title, Category, CVE ID or QID



All Scan Results

1 - 10 of 10

Mail Server Accepts Plaintext Credentials	
Discovery of Unix Account Names Vulnerability	
Web Server Stopped Responding	
Discovery of Unix Account Names Vulnerability	
POP3 Server Allows Plain Text Authentication Vulnerability	
OpenSSH J-PAKE Session Key Retrieval Vulnerability	
OpenSSH LoginGraceTime Denial of Service Vulnerability	
OpenSSH Commands Information Disclosure Vulnerability	
OpenSSH "X SECURITY" Bypass Vulnerability	
Apache Partial HTTP Request Denial of Service Vulnerability	

Discovery of Unix Account Names Vulnerability

QID: 5001

CVE Base: 3.3

Port: 80



CVSS Temporal: 3

Category: Brute Force Attack

CVE ID: [CVE-2001-1013](#)

Threat:

When a request for a user is made (<http://your.host/~user>), certain servers (such as Apache Versions 1.3.12 and 1.3.9) return a different reply depending on whether the account user exists on the host or not.

If a request is made for an account that exists on the host, a 403 error is returned. If a request is made for a non-existent account, then a 404 error is returned.

Impact:

Unauthorized remote users can implement brute force attacks on the Web server to guess a valid account name on the server. Even though they may be successful in obtaining a valid account, they will still have to guess the password. However, if user passwords are weak, some services may also be brute forced.

Solution:

Disable the default-enabled "UserDir" directive. To do so, add the following line to the httpd.conf file:

UserDir Disabled

Qualys Demo - 1

- Qualys is a powerful cloud-based vulnerability management tool
- Several online free tools
- Advanced web application security testing

END

QUALYS DEMO - PART 2

- Lets have a look at the Qualys features

QUALYS DEMO - PART 2

You have 14 applications available in your subscription

PCI Compliance

Achieve compliance with the PCI Data Security Standard (DSS).

[Visit now](#)

AssetView

Discover assets and use dynamic tags to keep your assets automatically organized.

[Visit now](#)

Cloud Agent

Stay updated with network security by deploying agents on your hosts.

[Visit now](#)

Vulnerability Management

Map and scan your network, prioritize your critical vulnerabilities and fix them.

[Visit now](#)

Continuous Monitoring

Set up monitoring and alerting of new security risks.

[Visit now](#)

Administration

Control user access permissions and activity in your subscription.

[Visit now](#)

Threat Protection

Add threat intelligence feed to your existing AssetView.

[Visit now](#)

Policy Compliance

Define, Audit and Document IT Security Compliance.

[Visit now](#)

Security Assessment Questionnaire

Automate risk and compliance through questionnaire campaigns.

[Visit now](#)

Web Application Scanning

Identify and manage web application security risks.

[Visit now](#)

Web Application Firewall

Detect attacks and protect your web applications.

[Visit now](#)

Malware Detection

Identify and manage web site malware risks.

[Visit now](#)

File Integrity Monitoring

Monitor changes on file systems.

[Visit now](#)

Certificate View

Analyse and manage SSL/TLS certificates and vulnerabilities.

[Visit now](#)

QUALYS 14 APPLICATIONS

QUALYS DEMO - PART 2

Qualys. Express

Vulnerability Management

Dashboard Scans Reports Remediation Assets KnowledgeBase Users

Scans Scans Maps Schedules Appliances Option Profiles Authentication Search Lists Setup

Actions (0) New Search Filters

Title	Targets	User	Reference
internal tst	192.168.0.103	Nahil Mahmood	scan/1536503914.55170
Certview FreeScheduledScan2018-07-04T14:03:12.881Z	192.168.0.103	Nahil Mahmood	scan/1534321994.94111
Certview FreeScheduledScan2018-07-04T14:03:12.881Z	192.168.0.103	Nahil Mahmood	scan/1533717201.49301
Certview FreeScheduledScan2018-07-04T14:03:12.881Z	192.168.0.103	Nahil Mahmood	scan/1533112468.01808
Certview FreeScheduledScan2018-07-04T14:03:12.881Z	192.168.0.103	Nahil Mahmood	scan/1532507598.57569
Certview FreeScheduledScan2018-07-04T14:03:12.881Z	192.168.0.103	Nahil Mahmood	scan/1531902800.14745
Certview FreeScheduledScan2018-07-04T14:03:12.881Z	192.168.0.103	Nahil Mahmood	scan/1531297997.70529
Certview FreeScan 2018-07-04T14:11:11.988Z	192.168.0.103	Nahil Mahmood	scan/1530713485.27682
Certview FreeScan 2018-07-04T14:03:15.421Z	192.168.0.103	Nahil Mahmood	scan/1530713013.27660
WAF and Website	192.168.0.103	Nahil Mahmood	scan/1530003752.74867

VULNERABILITY MANAGEMENT DASHBOARD

QUALYS DEMO - PART 2

Launch Vulnerability Scan

General Information

Give your scan a name, select a scan profile (a default is selected for you with recommended settings), and choose a scanner from the

Title:

Option Profile: * [Select](#)

Processing Priority:

Scanner Appliance: [View](#)

Choose Target Hosts from

Tell us which hosts (IP addresses) you want to scan.

☒ Assets ☐ Tags

Asset Groups [Select](#)

IPs/Ranges [Select](#)
Example: 192.168.0.87-192.168.0.92, 192.168.0.200

Exclude IPs/Ranges [Select](#)
Example: 192.168.0.87-192.168.0.92, 192.168.0.200

☐ Scan agent hosts in my target

Notification

☒ Send notification when this scan is finished

LAUNCH VULNERABILITY SCAN

QUALYS DEMO - PART 2

Scan Status (scan/1537463084.29199)

General Information >

Scanners >

Option Profile >

Targets >

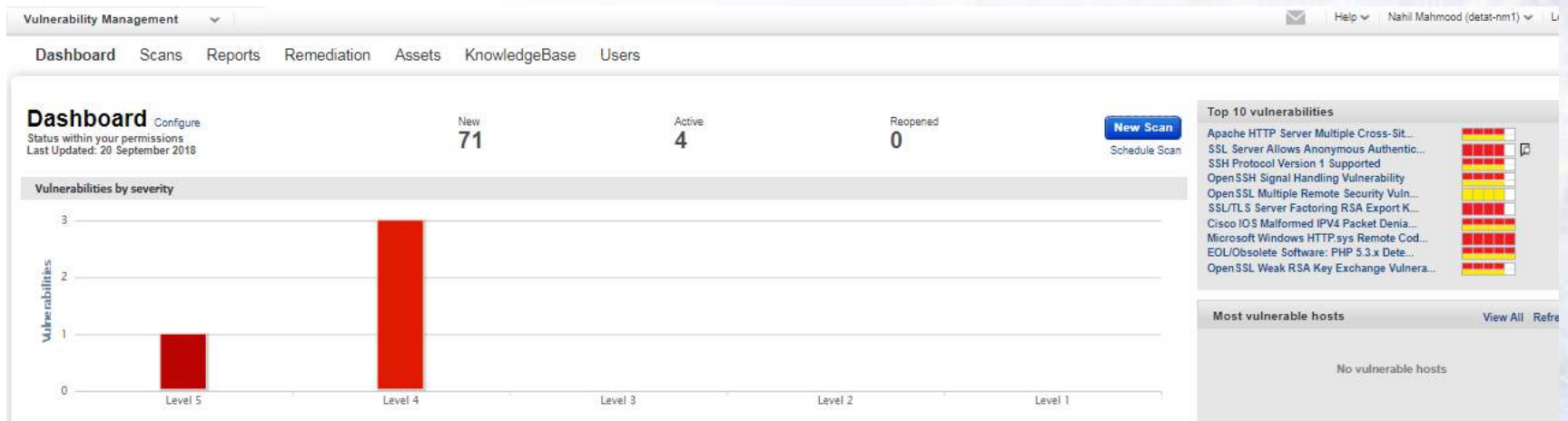
Scan Overview

Scan Information

Scan Title:	NEW SCAN
Launch Date:	09/20/2018 at 22:04:44 (GMT+0500)
Status:	Queued
Total IPs Scanned:	0
Scanner Appliance:	...

SCAN INITIATED

QUALYS DEMO - PART 2



VULNERABILITY MANAGEMENT DASHBOARD

QUALYS DEMO - PART 2

[Dashboard](#) [Scans](#) [Reports](#) [Remediation](#) [Assets](#) [KnowledgeBase](#) [Users](#)

 **Scans**

[Scans](#) [Maps](#) [Schedules](#) [Appliances](#) [Option Profiles](#) [Authentication](#) [Search Lists](#) [Setup](#)

 **Get Started Tutorials: Scans**

☐ Do not show tutorials

This is where you can manage your vulnerability scans and your scan configurations.



Manage Vulnerability Scans

Launch new vulnerability scans, monitor the status of running scans and view the details of vulnerabilities discovered after scans complete.

Watch demo  (3min 0sec)



Configure Scan Schedules

Configure scans to run automatically, or on a recurring basis and monitor results of your scans.

Watch demo  (4min 0sec)



Manage Discovery Scans

Use free discovery scans (maps) to discover live devices on your network. Discovered devices can be selected for vulnerability scanning based on the info gathered (OS, ports, etc.) in a map.

Watch demo  (5min 0sec)



Configure Scanner Appliances

Scanner Appliances (physical or virtual) are required to scan devices on internal networks. Managers can download appliances and configure them for scanning.



Configure Scan Settings

Customize the various scanning options required to run a scan. These can be saved as profiles for reuse. A default profile is provided for common environments.

Watch demo  (9min 20sec)



Set Up Host Authentication

Use the authentication feature (Windows, Linux, Oracle, etc) to discover and validate vulnerabilities by performing an in-depth assessment of your hosts.

Watch demo  (9min 20sec)



Configure Search Lists

Apply custom lists of vulnerabilities to scan profiles in order to limit scanning to certain vulnerabilities only.

SCAN TUTORIALS

7

QUALYS DEMO - PART 2

Launch Vulnerability Scan

General Information

Give your scan a name, select a scan profile (a default is selected for you with recommended settings), and choose a scanner.

Title:

Option Profile: * [Select](#)

Processing Priority:

Scanner Appliance: [View](#)

Choose Target Hosts from

Tell us which hosts (IP addresses) you want to scan.

☒ Assets ☐ Tags

Asset Groups [Select](#)

IPs/Ranges [Select](#)

Example: 192.168.0.87-192.168.0.92, 192.168.0.200

Exclude IPs/Ranges [Select](#)

Example: 192.168.0.87-192.168.0.92, 192.168.0.200

☐ Scan agent hosts in my target

Notification

☐ Send notification when this scan is finished

WANNACRY & SHADOW BROKERS SCAN

QUALYS DEMO - PART 3

- Lets have a look at some further features of Qualys:
- Qualys Continuous Monitoring

QUALYS DEMO - PART 3

Welcome to Qualys® Continuous Monitoring

Thank you for signing up to continuously monitor your perimeter network. Receive alerts to threats and unexpected changes as they happen. Make sure you schedule your scans to run on a frequent or continuous basis. [Learn more](#)

Get started with continuous monitoring

[Skip to Dashboard >](#)



Set up rulesets

Tell us the events you want to be alerted on - open ports, expiring certificates, new hosts, software applications, and more. [View the Initial Ruleset](#) provided by Qualys or create a new ruleset.



Configure monitoring profiles

Associate a ruleset with the hosts you want to monitor, and select when and how individuals and teams will be notified of new alerts.



View your alerts

Check out the alerts on your scanned hosts and search for specific alert and host details.

QUALYS CONTINUOUS MONITORING INTERFACE

QUALYS DEMO - PART 3

Ruleset BuilderLaunch help

Add one or more rules to this ruleset. Each rule describes an event you want to be alerted on.

Title*

WEBSITE CHANGES

Description

DETECT CHANGES TO WEBSITE

This is where you add and customize rules. Your rules can be simple (any new vulnerability) or complex (any new severity 5 vulnerability on a Linux host).

Rule Types


Host


Vulnerability


Certificate


Port / Service


Software


Ticket

Drag rules here to add them to the ruleset



RULESET BUILDER

QUALYS DEMO - PART 3

Ruleset BuilderLaunch help

Add one or more rules to this ruleset. Each rule describes an event you want to be alerted on.

Title*

Description

This is where you add and customize rules. Your rules can be simple (any new vulnerability) or complex (any new severity 5 vulnerability on a Linux host).

Rule Types


Host


Vulnerability


Certificate


Port / Service


Software


Ticket

Rule 1: New or Fixed or Active or Reopened VulnerabilityRemove

Your selection may result in excessive alerts. Select more filters to get fewer alerts.

When a vulnerability is* ☒ New ☒ Fixed ☒ Active ☒ Reopened

 Add Criteria

Rule 2: New or Expired or Expiring CertificateRemove

When a certificate is* ☒ New ☒ Expired ☐ Expiring in 10 days ☒ Expiring in 30 days ☒ Expiring in 90 days

 Add Criteria

Rule 3: Opened or Changed or Closed Port / ServiceRemove

When a port/service is* ☒ Opened ☒ Changed ☒ Closed

 Add Criteria

RULETYPES & CONFIGURATION

QUALYS DEMO - PART 3

Continuous Monitoring ▾

Help ▾ Nahil Mahmood ▾ Log out

Alerts Configuration

74 days remaining in trial. [Upgrade Now](#)

Configuration Monitoring Profiles Rulesets License Details

Search...

Actions (0) ▾ New Ruleset

2 rulesets ⚙ ▾

☐	Title	# Profiles	Created by	Created on
☐	WEBSITE CHANGES DETECT CHANGES TO WEBSITE	0	detst-nm1	20 Sep 2018 10:56PM GMT+0500
☐	Initial Ruleset (System) With the Initial Ruleset you will receive alerts when a new host is found, a port is open, or an SSL certificate is expired or is about to expire. Use this ruleset as is or save a copy of it to make changes.	0	System	19 May 2018 7:38PM GMT+0500

RULESETS INTERFACE

QUALYS DEMO - PART 3

Welcome to Qualys® Continuous Monitoring

Thank you for signing up to continuously monitor your perimeter network. Receive alerts to threats and unexpected changes as they happen. Make sure you schedule your scans to run on a frequent or continuous basis. [Learn more](#)

Get started with continuous monitoring

[Skip to Dashboard >](#)



Set up rulesets

Tell us the events you want to be alerted on - open ports, expiring certificates, new hosts, software applications, and more. [View the Initial Ruleset](#) provided by Qualys or create a new ruleset.



Configure monitoring profiles

Associate a ruleset with the hosts you want to monitor, and select when and how individuals and teams will be notified of new alerts.



View your alerts

Check out the alerts on your scanned hosts and search for specific alert and host details.

QUALYS CONTINUOUS MONITORING INTERFACE

QUALYS DEMO - PART 3

Monitoring Profile CreationTurn help tips: On | Off Launch help

Step 1 of 3

- Hosts** ✓
- Ruleset
- Notifications

Configure a profile for continuous monitoring of your hosts.

Profile for Continuous Monitoring (*) REQUIRED FIELDS

Title*

WEBSITE

Choose Target Hosts

Tell us which hosts (IP addresses) you would like to monitor.

☐ Select Tags ☒ Select IPs/Ranges

IPs/Ranges

192.18

Example: 192.168.0.87-192.168.0.92, 192.168.0.200

Exclude IPs/Ranges

Example: 192.168.0.87-192.168.0.92, 192.168.0.200

CancelContinue

PROFILE CREATION

QUALYS DEMO - PART 3

Monitoring Profile CreationTurn help tips: On | Off Launch help

Step 2 of 3

- 1 Hosts ✓
- 2 Ruleset
- 3 Notifications

Choose a set of alert rules to be used for this profile.

Choose Ruleset (*) REQUIRED FIELD

Your ruleset tells us the events you would like to be alerted on. For example: new host found, host changed, SSL certificate expired, vulnerability detected and more.

Alert Ruleset*

WEBSITE CHANGES

Create New

WEBSITE CHANGES [Edit](#)

Description:
DETECT CHANGES TO WEBSITE

Cancel

Previous

Continue

CHOOSE RULESET

QUALYS DEMO - PART 3

Monitoring Profile CreationTurn help tips: On | Off Launch help

Step 3 of 3

- 1 Hosts ✓
- 2 Ruleset ✓
- 3 Notifications ✓

You have the option to set up alert notifications for you and other users.

Frequency (*) REQUIRED FIELD

Tell us how often you want to receive notifications.

Send email alerts

Users

Tell us who should receive alerts. Select from your distribution groups.

Distribution Groups:

TECHNICAL (1 email)

NOTIFICATIONS

QUALYS DEMO - PART 3

Continuous Monitoring ▾

Alerts Configuration

Configuration Monitoring Profiles Rulesets License Details

Search...

Actions (0) ▾ New Profile

☐	Title	Ruleset	Notifications	Created by
☐	☒ WEBSITE	WEBSITE CHANGES	daily	detat-nm1

MONITORING PROFILE ACTIVE

QUALYS DEMO - PART 3

- Qualys Continuous Monitoring is very useful for watching critical changes that may impact security

END

How Do VM Scanners Work ?

- Lets take a look at Qualys scanning technique:

<https://community.qualys.com/docs/DOC-1068>

How Do VM Scanners Work ?

- QualysGuard scanning methodology mainly focuses on the different steps that an attacker might follow in order to perform an attack.
- It tries to use exactly the same discovery and information gathering techniques that will be used by an attacker.

<https://community.qualys.com/docs/DOC-1068>

How Do VM Scanners Work ?

1. **Checking if the remote host is alive**
 - The first step is to check if the host to be scanned is up and running in order to avoid wasting time on scanning a dead or unreachable host

<https://community.qualys.com/docs/DOC-1068>

How Do VM Scanners Work ?

1. **Checking if the remote host is alive**
 - This detection is done by probing some well-known TCP and UDP ports. If the scanner receives at least one reply from the remote host, it continues the scan

<https://community.qualys.com/docs/DOC-1068>

How Do VM Scanners Work ?

2. Firewall detection

The second test is to check if the host is behind any firewalling/filtering device. This test enables the scanner to gather more information about the network infrastructure and will help during the scan of TCP and UDP ports.

<https://community.qualys.com/docs/DOC-1068>

How Do VM Scanners Work ?

3. TCP / UDP Port scanning

The third step is to detect all open TCP and UDP ports to determine which services are running on this host. The number of ports is configurable, but the default scan is approximately 1900 TCP ports and 180 UDP ports.

<https://community.qualys.com/docs/DOC-1068>

How Do VM Scanners Work ?

4. OS Detection

Once the TCP port scanning has been performed, the scanner tries to identify the operating system running on the host.

This detection is based on sending specific TCP packets to open and closed ports.

<https://community.qualys.com/docs/DOC-1068>

How Do VM Scanners Work ?

5. TCP / UDP Service Discovery

Once TCP/UDP ports have been found open, the scanner tries to identify which service runs on each open port by using active discovery tests

<https://community.qualys.com/docs/DOC-1068>

How Do VM Scanners Work ?

6. Vulnerability assessment based on the services detected

Once the scanner has identified the specific services running on each open TCP and UDP port, it performs the actual vulnerability assessment. The scanner first tries to check the version of the service in order to detect...

<https://community.qualys.com/docs/DOC-1068>

How Do VM Scanners Work ?

Vulnerability scanning is an automated process that identifies your cyber security weaknesses. Penetration testing goes one step further. It involves professional ethical hackers combining the results of automated scans with their expertise to reveal vulnerabilities that may not be identified by scans alone

6. Vulnerability assessment based on the services detected

... only vulnerabilities applicable to this specific service version. Every vulnerability detection is non-intrusive, meaning that the scanner never exploits a vulnerability if it could negatively affect the host in any way.

<https://community.qualys.com/docs/DOC-1068>

How Do VM Scanners Work ?

- **Limitations:**
 - Vulnerability scanners work in the same manner as antivirus programs do by using databases that store descriptions of different types of vulnerabilities
 - False positive or false negative rate

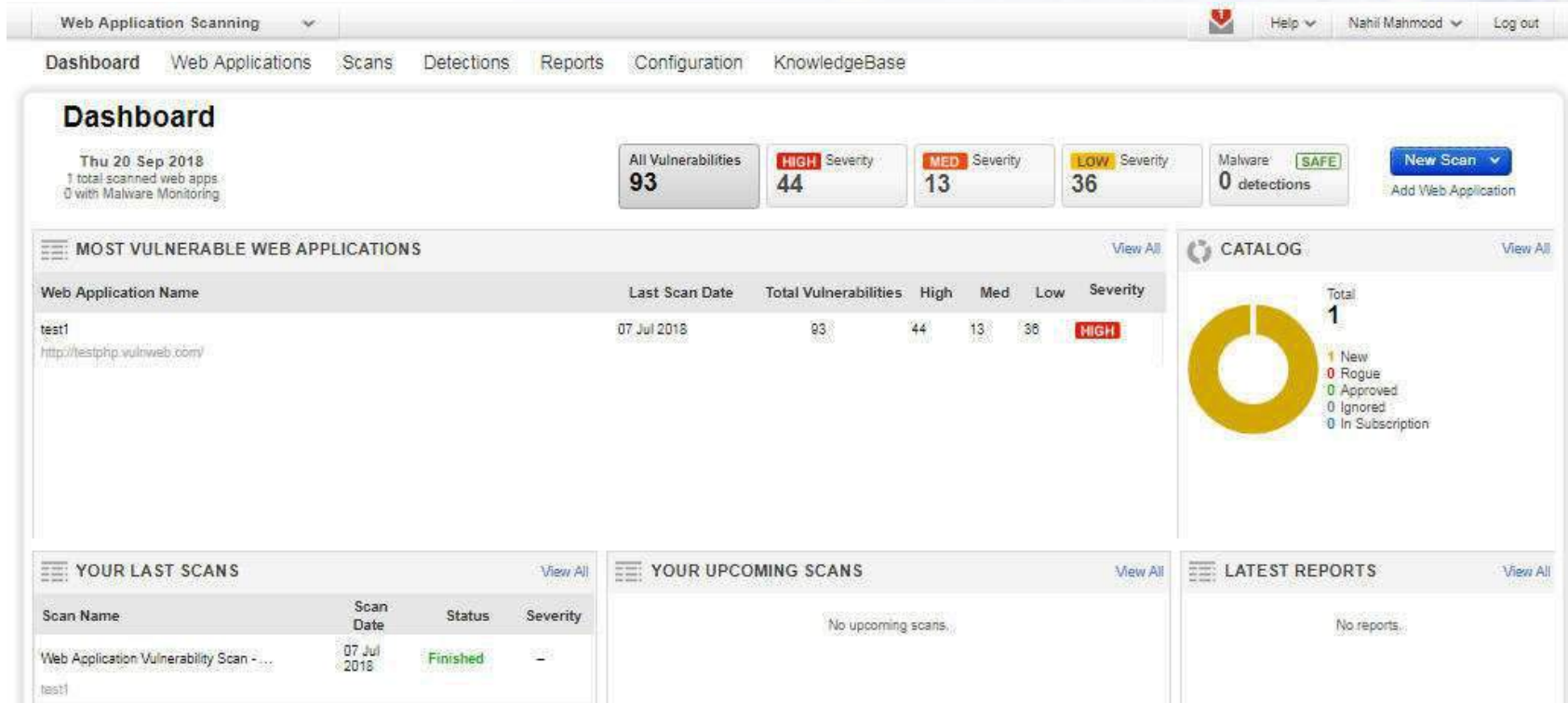
<http://www.spamlaws.com/how-vulnerability-scanning-works.html>

QUALYS WEB APPLICATION SCANNING

- Lets have a look at Qualys Web Application Scanning

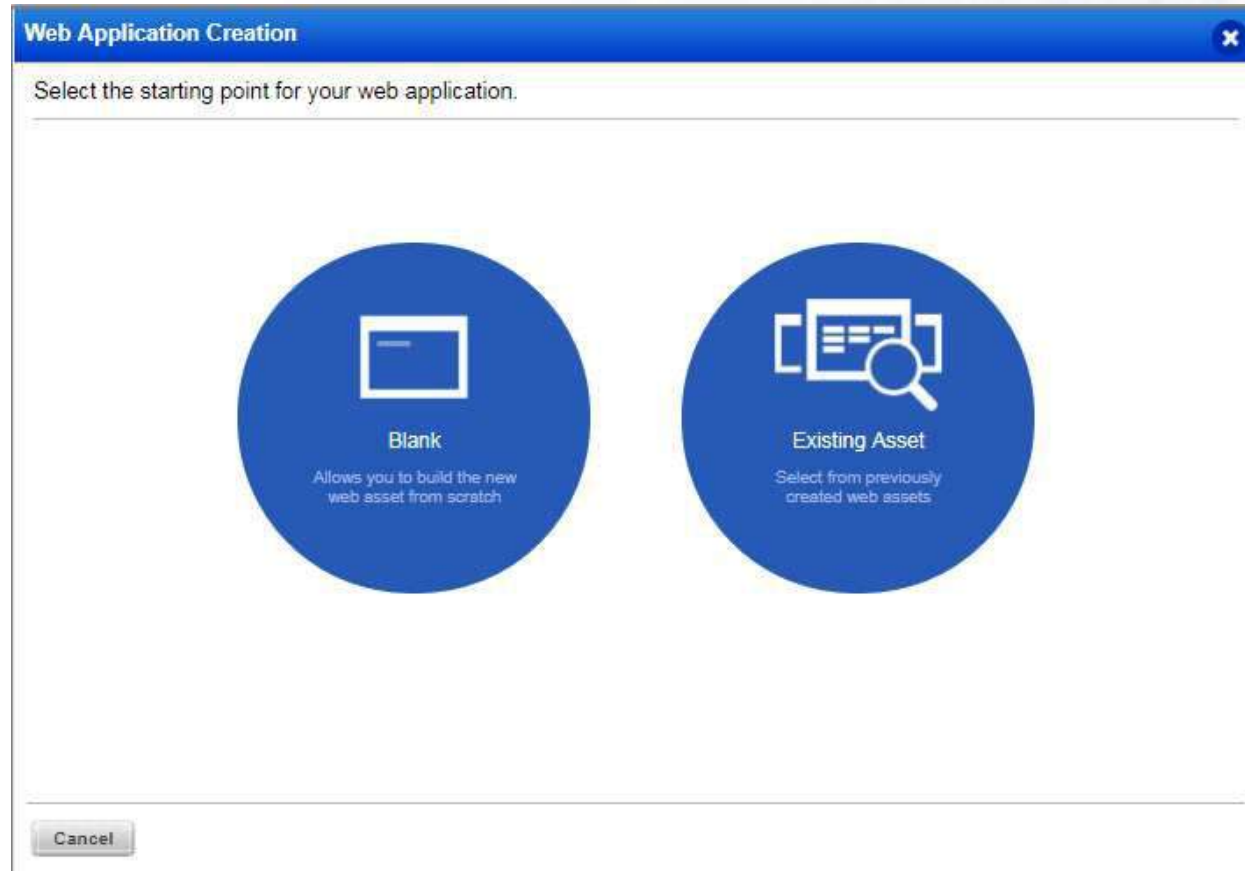
Qualys Web Application Scanning (WAS) is a cloud-based service that provides automated crawling and testing of custom web applications to identify vulnerabilities including cross-site scripting (XSS) and SQL injection

QUALYS WEB APPLICATION SCANNING



DASHBOARD

QUALYS WEB APPLICATION SCANNING



CREATION – BLANK OR EXISTING ASSET

QUALYS WEB APPLICATION SCANNING

Web Application CreationTurn help tips: On | Off Launch help

Step 1 of 11

- Asset Details** ✓
- Application Details
- Scan Settings
- Crawl Settings
- Redundant Links
- Authentication
- Exclusions
- Advanced Options
- Malware Monitoring
- Comments
- Review And Confirm

Tell us about the asset you want to scan

Definition (*) REQUIRED FIELDS

Let's start with some basic information.

Name*

Target Definition

Web Application URL*

For scanning Swagger-based REST APIs, the Web Application URL should point to the Swagger file. It is your responsibility to verify that you have permission to scan all web applications that you specify as scan targets.

Custom Attributes

Provide attribute information that will help you categorize this web application within your subscription.

Name	Value

Add

Tags

Select tags to apply to the web application Select | Create | Remove All

Cancel

Continue

ASSET DETAILS

QUALYS WEB APPLICATION SCANNING

Web Application CreationTurn help

Step 2 of 11

- 1 Asset Details
- 2 Application Details
- 3 Scan Settings
- 4 Crawl Settings
- 5 Redundant Links
- 6 Authentication
- 7 Exclusions

Tell us about the web application you want to scan

Target Definition

Web Application URL

Crawl Scope*

Limit to content located at or below URL subdirectory

Limit at or below URL hostname (www.i' .com)

Limit to content located at or below URL subdirectory

Limit to URL hostname and specified sub-domain

Limit to URL hostname and specified domains

CRAWL SCOPE

QUALYS WEB APPLICATION SCANNING

Web Application CreationTurn help tips: On | Off Launch help

Step 3 of 11

- Asset Details
- Application Details
- Scan Settings**
- Crawl Settings
- Redundant Links
- Authentication
- Exclusions
- Advanced Options
- Malware Monitoring
- Comments
- Review And Confirm

Tell us the scan settings you'd like to use

Default Scan Options

Choose the default scan settings for your web application. You can change the defaults for each scan.

Option Profile: **WEB SCANNING PROFILE (Default)** View Create

Scanner Appliance

Choose the default scanner appliance for your web application. You can change the defaults for each scan.

☒ External ☐ Individual ☐ Tags (Scanner pool)

☒ Lock this scanner appliance for this web application.

Duration

Cancel the scan after N hours or at a certain time. By default the scan will run until it completes, or the maximum scan time is reached.

When selecting Cancel After, the scan will cancel after the time period set once it begins running and may not reflect the time the scan was submitted. This may be due to scan queues or scanner availability. To end scan at a precise time, please use the option Cancel At and select the desired time the scan should end regardless of queues, scanner availability or submittal/run time.

Cancel Option: **Cancel Scan After** hour

CancelPreviousContinue

SCAN SETTINGS

QUALYS WEB APPLICATION SCANNING

Web Application CreationTurn help tips: On | Off Launch the wizard

Step 9 of 11

- Asset Details ✓
- Application Details ✓
- Scan Settings ✓
- Crawl Settings ✓
- Redundant Links ✓
- Authentication ✓
- Exclusions ✓
- Advanced Options ✓
- Malware Monitoring ✓**
- Comments
- Review And Confirm

Malware Monitoring

By enabling Malware Monitoring on this web application, you will allow QualysGuard to perform a regular scan for malware on your external web site. The application owner will receive an email notification when malicious software is detected. Note Malware Monitoring is available for external sites only.

Status

☒ Enable Malware Monitoring for this web application

Recurrence

Mode*:
Single occurrence

Launch Information

Start Date: Fri 21 Sep 2018
Time*: 12:37AM

Time Zone*: (GMT 05:00) French Southern & Antarctic Lands Time (TFT1)

Notification

Choose to send notifications about malware scans to the web application owner.

MALWARE MONITORING

QUALYS ADDITIONAL FEATURES

- Lets have a look at Qualys additional features

QUALYS ADDITIONAL FEATURES

The screenshot displays the Qualys Threat Protection interface. At the top, there's a navigation bar with 'Threat Protection' selected, and sub-tabs for 'Dashboard', 'Feed', 'Assets', and 'Configuration'. Below this is a 'Live Feed' section with a blue header and a 'Last updated a few seconds ago' timestamp. A 'Saved Searches' dropdown is visible. The main content area is divided into two columns: 'HIGH RATED FEED' (162 items) and 'MEDIUM / LOW RATED FEED' (17,477 items). The 'HIGH RATED FEED' column shows a high-severity alert for 'Microsoft Windows Task Scheduler Privilege Escalation Vulnerability (Zero...)' dated August 31, 2018, with 0 impacted assets. The 'MEDIUM / LOW RATED FEED' column shows two medium-severity alerts for 'PoC Exploit available for CVE-2018-8355' and 'PoC Exploit available for CVE-2006-4842', both dated 3 days ago, with 0 impacted assets.

Threat Protection ▼

Dashboard Feed Assets Configuration

Live Feed Last updated a few seconds ago

Saved Searches ▼

Search for threat news feeds

HIGH RATED FEED 162

MEDIUM / LOW RATED FEED 17,477

HIGH August 31, 2018 ☆ ☰

Microsoft Windows Task Scheduler Privilege Escalation Vulnerability (Zero...

Live Threat Intelligence Feed A security researcher has publicly disclosed the details of a zero-day vulnerability in Microsoft Windows operating system. It's a privilege escalation vulnerability, which...

Windows Zero Day ALPC Exploit
Privilege Escalation
Advanced Local Procedure Call Exploit
CVE-2018-8440

0
Impacted Assets

MEDIUM 3 days ago ☆ ☰

PoC Exploit available for CVE-2018-8355

An exploit for CVE-2018-8355 is now available from The Exploit-DB. Qualys has added QID(s) 91464, 100341 to detect this issue in your environment. Please check your ThreatPROTECT dashboard for...

0
Impacted Assets

HIGH August 30, 2018 ☆ ☰

PoC Exploit available for CVE-2006-4842

An exploit for CVE-2006-4842 is now available from The Exploit-DB.

QUALYS THREAT PROTECTION

QUALYS ADDITIONAL FEATURES



Microsoft Windows Task Scheduler Privilege Escalation Vulnerability (Zero Day)

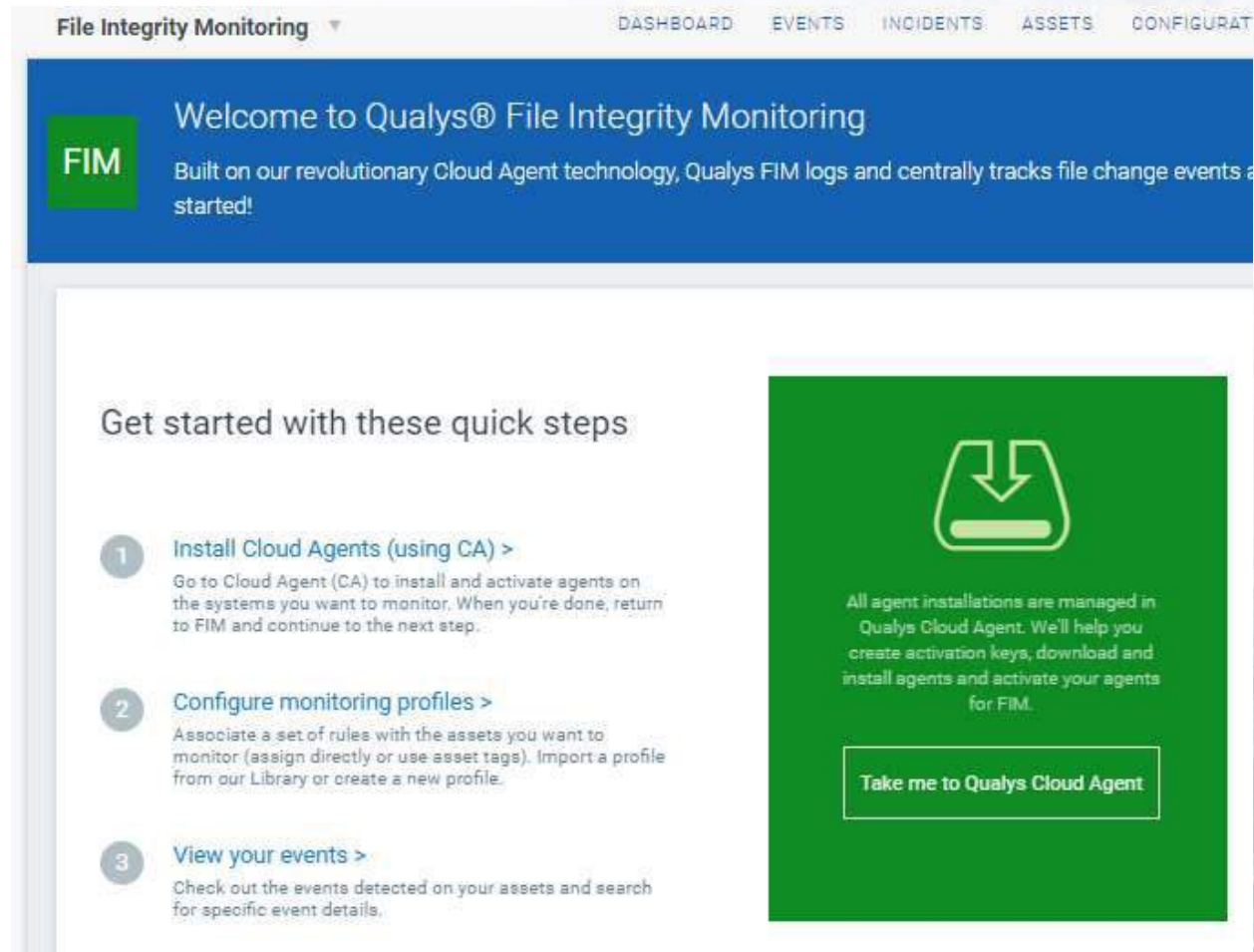
Posted by Mandar Jadhav on August 30, 2018

A security researcher has publicly disclosed the details of a zero-day vulnerability in Microsoft Windows operating system. It's a privilege escalation vulnerability, which resides in the Windows task scheduler program and occurred due to errors in the handling of Advanced Local Procedure Call (ALPC) systems. The ALPC interface is a Windows-internal mechanism that works as an inter-process communication system. ALPC enables a client process running within the OS to ask a server process running within the same OS to provide some information or perform some action.

The researcher has also released a [proof-of-concept](#) (PoC) code, which exploits the ALPC interface to gain SYSTEM access on a Windows system.

QUALYS VULNERABILITY DESCRIPTION

QUALYS ADDITIONAL FEATURES



File Integrity Monitoring ▾ DASHBOARD EVENTS INCIDENTS ASSETS CONFIGURATION

FIM Welcome to Qualys® File Integrity Monitoring

Built on our revolutionary Cloud Agent technology, Qualys FIM logs and centrally tracks file change events and alerts. You're all set! started!

Get started with these quick steps

- 1 Install Cloud Agents (using CA) >**
Go to Cloud Agent (CA) to install and activate agents on the systems you want to monitor. When you're done, return to FIM and continue to the next step.
- 2 Configure monitoring profiles >**
Associate a set of rules with the assets you want to monitor (assign directly or use asset tags). Import a profile from our Library or create a new profile.
- 3 View your events >**
Check out the events detected on your assets and search for specific event details.



All agent installations are managed in Qualys Cloud Agent. We'll help you create activation keys, download and install agents and activate your agents for FIM.

[Take me to Qualys Cloud Agent](#)

FILE INTEGRITY MONITORING

QUALYS ADDITIONAL FEATURES

Welcome to Qualys® Cloud Agent Platform

Thank you for signing up for our revolutionary new platform that gives you continuous network security updates through the cloud. Let's get started!

Get started with these quick steps



Cloud Agent Overview >

Become an expert in no time.
Learn how it all works, what you will need and which preliminary steps you can take.



Download & Install Agents >

This step will help you create activation keys and set up agents. Already have an activation key?
[Click here](#)



We're Ready to Start Syncing to the Cloud! >

Once your agents are installed they should start connecting to our cloud platform and registering themselves. Discovery results in a few minutes.
[Click here to troubleshoot.](#)

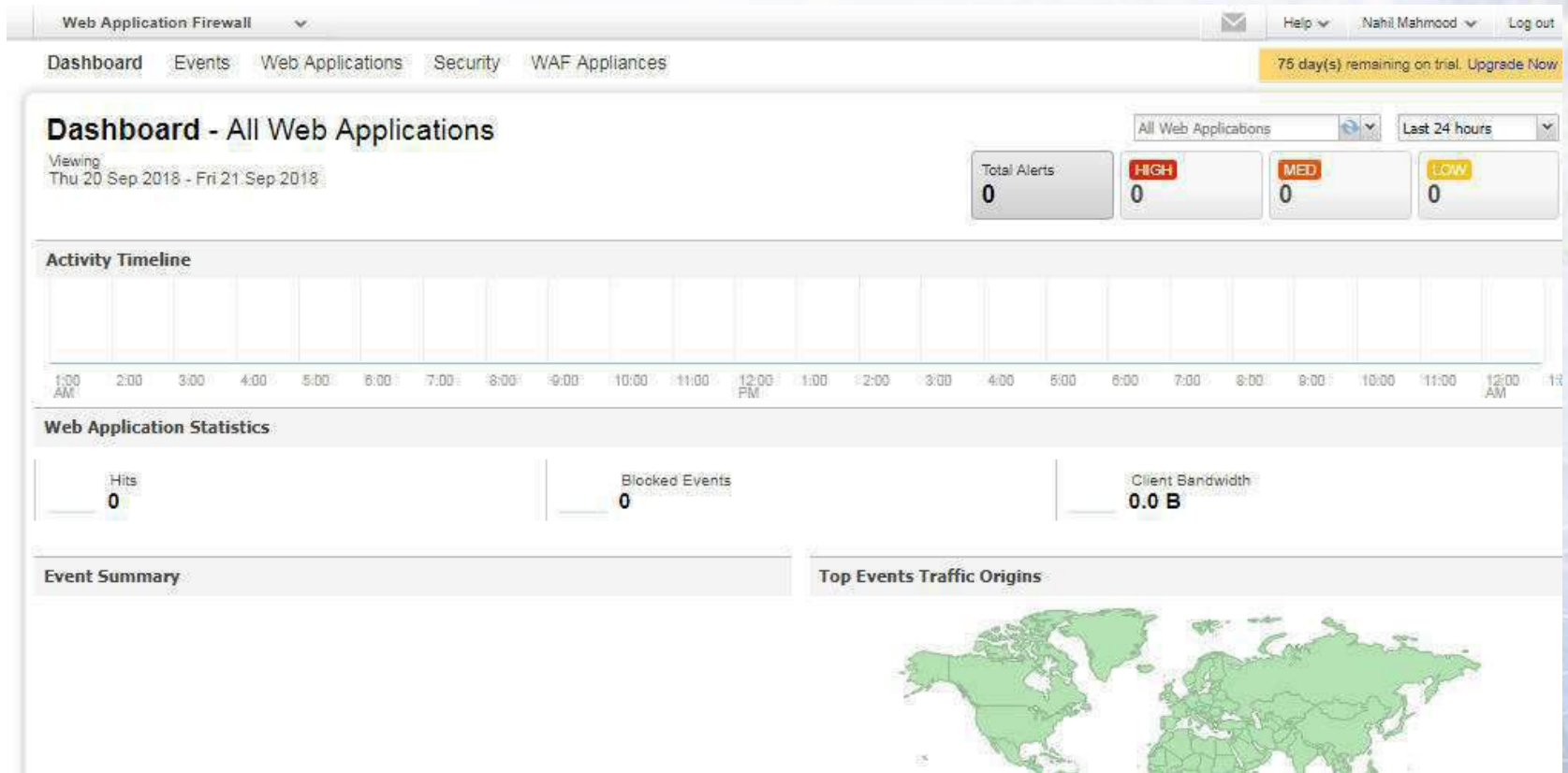


Change Configuration (optional) >

You can customize the behavior of your agents by creating custom profiles.

QUALYS CLOUD AGENT

QUALYS ADDITIONAL FEATURES



WEB APPLICATION FIREWALL

QUALYS ADDITIONAL FEATURES

Vulnerability Management

Dashboard Scans Reports Remediation Assets KnowledgeBase Users

KnowledgeBase KnowledgeBase Search Lists iDefense Intelligence Setup

New Search Filters

Trial expires in 29 days. | Upgrade

DOC ID		Title	Published
N/A	New	Oracle e-Business Suite "ibeCRgpPrimaryCreate.jsp" XSS Input Validation Vulnerability (iDefense Zero Day) CVSS Base Score 4.3	09/18/2018
N/A	New	Oracle e-Business Suite "ibeCAcpSSOReg.jsp" XSS Input Validation Vulnerability (iDefense Zero Day) CVSS Base Score 4.3	09/18/2018
N/A	New	Oracle e-Business Suite "ibeCRgpBusinessCreatePartial.jsp" XSS Input Validation Vulnerability (iDefense Zero Day) CVSS Base Score 4.3	09/18/2018
N/A	New	Oracle e-Business Suite "ibeCRgpIndividualCreatePartial.jsp" XSS Input Validation Vulnerability (iDefense Zero Day) CVSS Base Score 4.3	09/18/2018
N/A	New	Oracle e-Business Suite "ibeCRgpIndividualCreatePartial.jsp" XSS Input Validation Vulnerability (iDefense Zero Day) CVSS Base Score 4.3	09/18/2018
N/A	New	Oracle e-Business Suite "pvxCRgpPrtAddnInfo.jsp" XSS Input Validation Vulnerability (iDefense Zero Day) CVSS Base Score 4.3	09/17/2018

iDefense Intelligence

QUALYS ADDITIONAL FEATURES

Search ✕

Category:

☐ NOT

All

Patch Solution:

☒ Patch Available
☐ Trend Micro Virtual Patch Available
☐ No Patch Solution

CVE ID:

☐ NOT

CPE:

All

Exploitability:

All

Associated Malware:

All

Vendor Reference:

☐ NOT

CISCO

CVSS Base Score:

greater than or equal to

Search

SEARCH KNOWLEDGEBASE

QUALYS ADDITIONAL FEATURES

Vulnerability Management				
Dashboard Scans Reports Remediation Assets KnowledgeBase Users				
KnowledgeBase				
QID	Title		Category	CVE ID
87347	Cisco Data Center Network Manager Path Traversal Vulnerability		Web server	CVE-2018-0464
316166	Cisco Email Security Appliance and Content Security Management Appliance HTTP Response Splitting Vulnerability (cisco-sa-20171115-esa)		Cisco	CVE-2017-12309
38728	Cisco TelePresence VCS Denial of Service Vulnerability(cisco-sa-20180815-uomimps-dos)		General remote services	CVE-2018-0409
316315	Cisco Unity Connection Apache Struts Remote Code Execution Vulnerability(cisco-sa-20180823-apache-struts)		Cisco	CVE-2018-11776
316314	Cisco Unified Communications Manager IM And Presence Service Apache Struts Remote Code Execution Vulnerability(cisco-sa-20180823-apache-struts)		Cisco	CVE-2018-11776
316313	Cisco Unified Communications Manager Apache Struts Remote Code Execution Vulnerability(cisco-sa-20180823-apache-struts)		Cisco	CVE-2018-11776
87350	Cisco Data Center Network Manager Cross-Site Scripting Vulnerability(cisco-sa-20180905-dcnm-xss)		Web server	CVE-2018-0450

CISCO VULNERABILITIES – PATCH AVAILABLE

QUALYS ADDITIONAL FEATURES

- Have a look at additional features in your Qualys free trial

END

Open Source Vulnerability Scanners

- Lets take a look at OpenVAS
- <http://www.openvas.org/livedemo.html>
- Login and password: livedemo

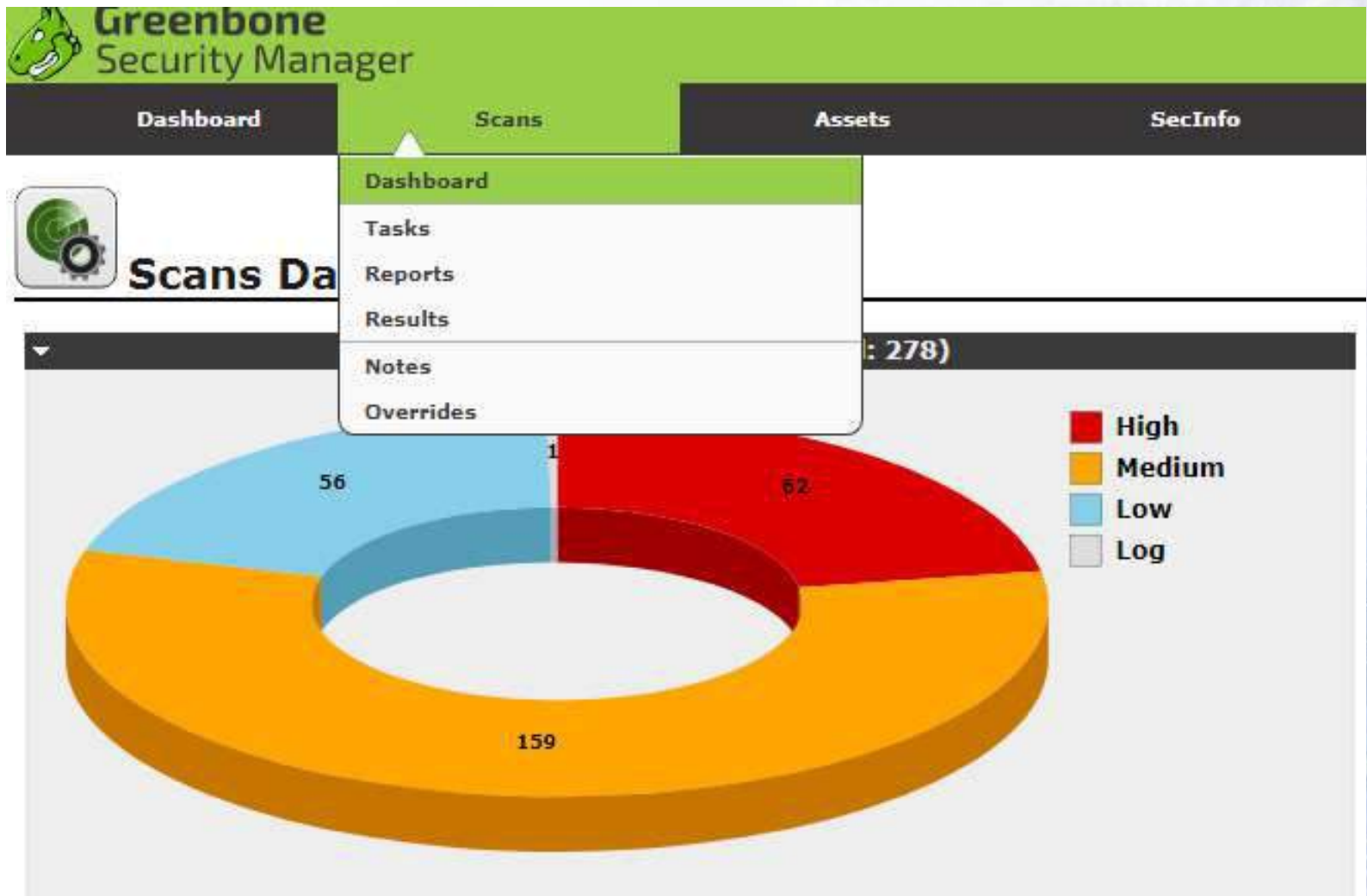
Open Source Vulnerability Scanners

DASHBOARD VIEW



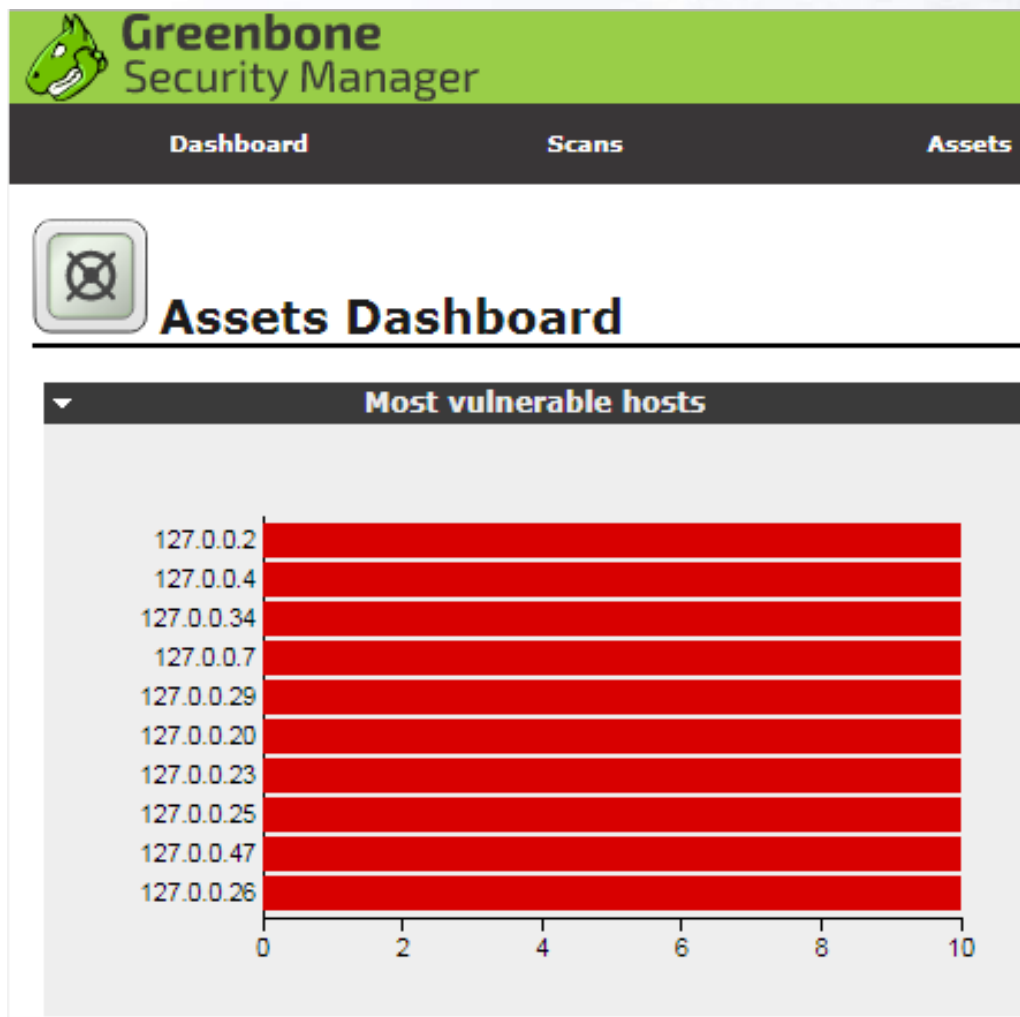
Open Source Vulnerability Scanners

SCANS DASHBOARD



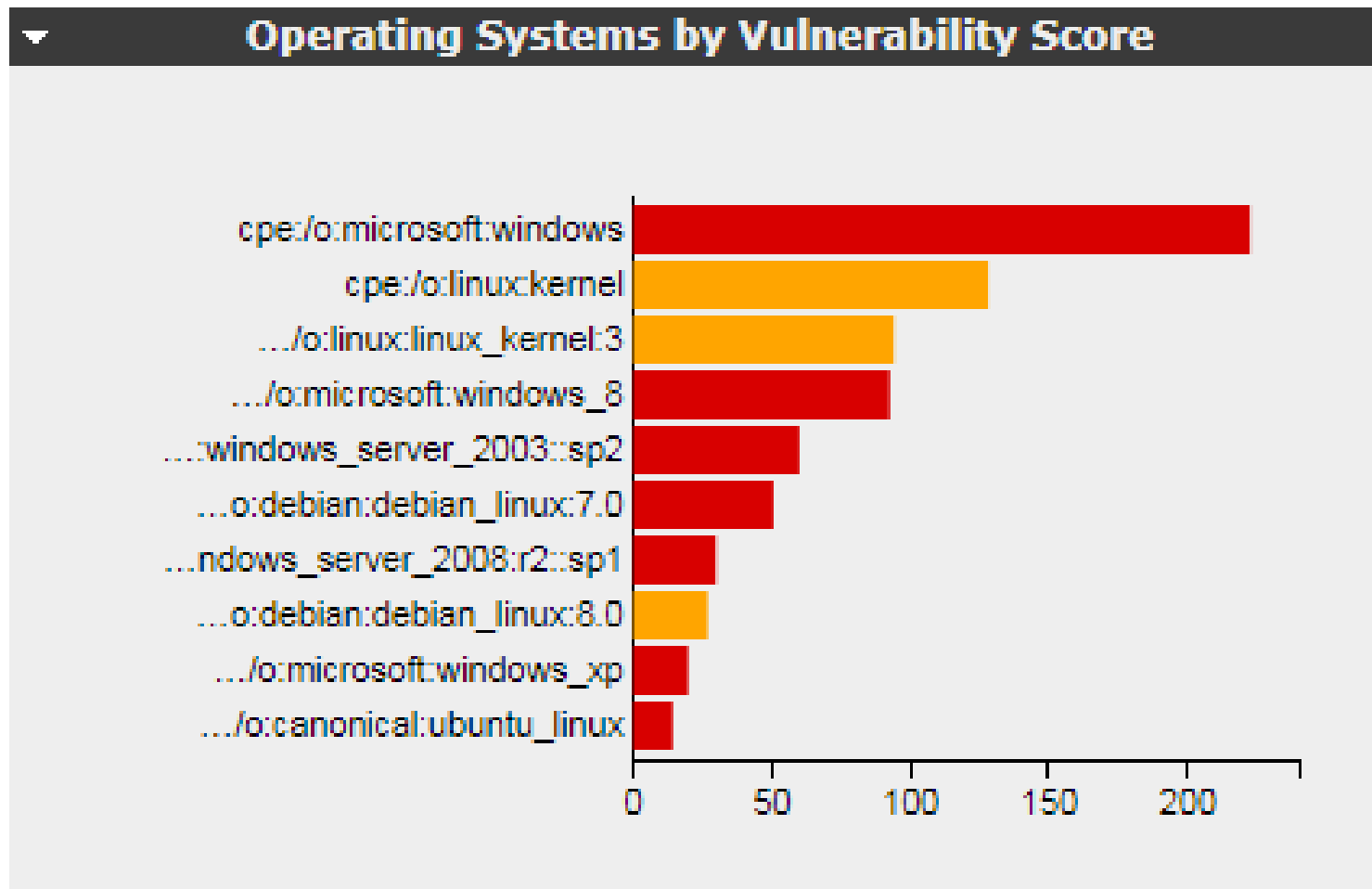
Open Source Vulnerability Scanners

ASSETS DASHBOARD



Open Source Vulnerability Scanners

OS BY VULNERABILITY SCORE



Open Source Vulnerability Scanners

ASSETS>HOSTS CLASSIC VIEW

The screenshot displays the Greenbone Security Manager (GVM) interface. The top navigation bar includes 'Dashboard', 'Scans', 'Assets', 'SecInfo', 'Configuration', 'Extras', and 'Help'. The 'Assets' menu is open, showing 'Dashboard', 'Hosts', 'Operating Systems', and 'Hosts (Classic)'. The 'Hosts (Classic)' view is selected, showing a table of filtered hosts. The table has columns for IP, severity counts (High, Medium, Low, Log), Last Report, OS, Ports, Apps, Distance, Prognosis, Reports, and Actions. The table shows 7 hosts with various severity levels and last reports from February 21, 2017.

Greenbone Security Manager No auto-refresh Logged in as **livedemo** | Log Sat Jul 15 18:04:26 2017

Host Filtering

Results per page:

Text phrase:

Severity: ☒ High ☒ Medium ☐ Low ☐ Log

Filtered Hosts 1 - 42 of 42

IP	High	Medium	Low	Log	Last Report	OS	Ports	Apps	Distance	Prognosis	Reports	Actions
127.0.0.1	4	4	0	0	Feb 21 2017	Windows	5	1		High	1	
127.0.0.2	1	4	0	0	Feb 21 2017	Windows	4	0			1	
127.0.0.3	1	2	0	0	Feb 21 2017	Windows	4	2			1	
127.0.0.4	2	5	0	0	Feb 21 2017	Windows	8	3		High	1	
127.0.0.5	1	1	0	0	Feb 21 2017	Windows	5	2		High	1	
127.0.0.6	1	5	0	0	Feb 21 2017	Windows	4	1			1	
127.0.0.7	4	14	0	0	Feb 21 2017	Windows	13	4		High	1	

Open Source Vulnerability Scanners

CONFIGURATION > TARGETS

 **Greenbone**
Security Manager

[Dashboard](#) [Scans](#) [Assets](#) [SecInfo](#) [Configuration](#) [Extra](#)



 **Targets (4 of 4)**

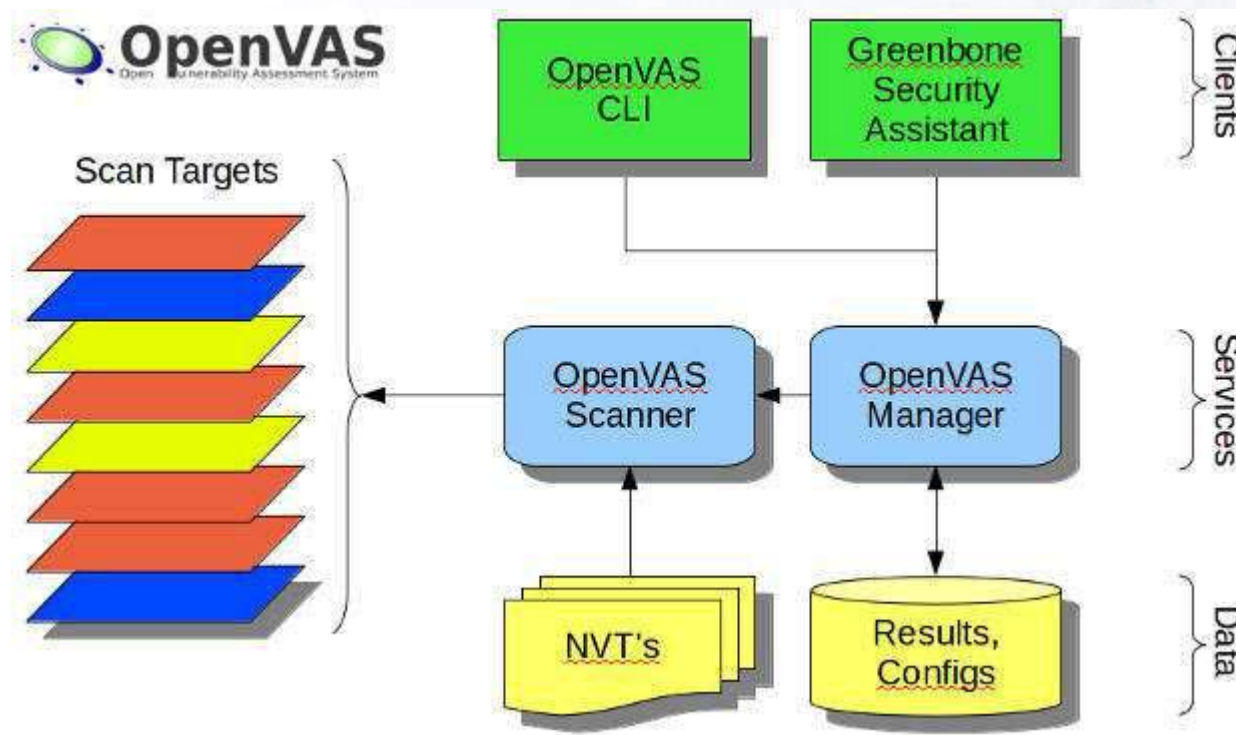
Name	Hosts	IPs	Port List
Central Webservers	192.168.12.3, 192.168.12.4	2	All IANA assigned
DMZ	192.168.12.0/24	254	All IANA assigned TCP 2012-02-10
Printers	192.168.40.0/24	254	All IANA assigned TCP 2012-02-10
Windows Desktops	192.168.70.0-192.168.71.255	512	All IANA assigned TCP 2012-02-10

[Targets](#)
[Port Lists](#)
[Credentials](#)
[Scan Configs](#)
[Report Formats](#)
[Scanners](#)
[Filters](#)
[Tags](#)
[Permissions](#)

[SSH: s](#)
[SMB: D](#)

Open Source Vulnerability Scanners

OPENVAS ARCHITECTURE



APPROXIMATELY 50k NETWORK VULNERABILITY TESTS

<http://www.openvas.org/software.html>

Open Source Vulnerability Scanners

- OpenVAS is a simple, free (opensource) VA scanner
- It has source code documentation, virtual images for download, and mailing lists on its website

END

Suggested Frequency For VM Scanning

- Pre-requisites
 - Information security team
 - Vulnerability management policy
 - Inhouse scanner or openvas tool
 - Trained staff

Suggested Frequency For VM Scanning

- At the start:
 - Organizations scanning once a year or not at all
 - Vulnerabilities identified by internal scanning or external VA report
 - Not remediated
 - Lack of discipline and management support

Suggested Frequency For VM Scanning

- As organizations get more mature in scanning discipline:
 - Quarterly scan
 - Quarterly remediation by IT teams
 - Quarterly report to IT Steering Committee

Suggested Frequency For VM Scanning

- Mature organizations:
 - Monthly scan
 - Monthly remediation
 - Quarterly or bi-annual external VA/PT
 - Monthly reports to IT Steering Committee

Suggested Frequency For VM Scanning

- Most mature organizations:
 - Fortnightly scan
 - Fortnightly remediation
 - Monthly reporting

VM Challenges & Pitfalls

- Challenges:
 - Internal expertise on VM tool
 - Not enough support from IT teams
 - Vulnerability patching causing application failure
 - Management support

VM Challenges & Pitfalls

- Internal expertise on VM tool
 - Not too much expertise required
 - Create testbed
 - Monitor traffic pattern
 - Train staff if possible
 - Patch small portions of the network first

VM Challenges & Pitfalls

- Not enough support from IT teams:
 - Create reports and share among IT management
 - Highlight and educate risks to IT management and board
 - Create departmental competition and relationship-building

VM Challenges & Pitfalls

- Patching causing application failure:
 - In test environment create work around or compensating controls
 - Test the compensating controls
 - Document the compensating controls

VM Challenges & Pitfalls

- Not enough management support:
 - Share reports with management highlighting recent incidents
 - Share industry-specific or geographically relevant breach reports
 - Create awareness

IT Asset Management Challenges

- The typical enterprise has hundreds or thousands of IT assets with a fast-paced business environment
- Tough challenge to keep all IT assets tracked and updated with all the right software patches and updates

IT Asset Management Challenges

- Challenges:
 - Asset discovery & tracking
 - Antivirus status
 - Windows & OS updates
 - Patch management
 - Change management

IT Asset Management Challenges

- Asset discovery & tracking
 - New assets added & old assets removed
 - Temporary or replacement machines
 - Travelling staff
 - Test beds
 - Vendor environments

IT Asset Management Challenges

- Antivirus status:
 - Working and updated antivirus critical to a security managed network
 - Geographically dispersed network
 - Some stations not responding or updating

IT Asset Management Challenges

- Windows & OS updates:
 - Windows, Linux, Unix, AIX and database systems
 - Vendor patches from multiple sources
 - Testing the patches
 - Acquiring downtime windows
 - Monitoring the performance

IT Asset Management Challenges

- Patch management:
 - Scanning for vulnerabilities
 - Passing on reports to IT teams
 - Tracking the remediation
 - Re-scanning for verification
 - Reporting to management

IT Asset Management Challenges

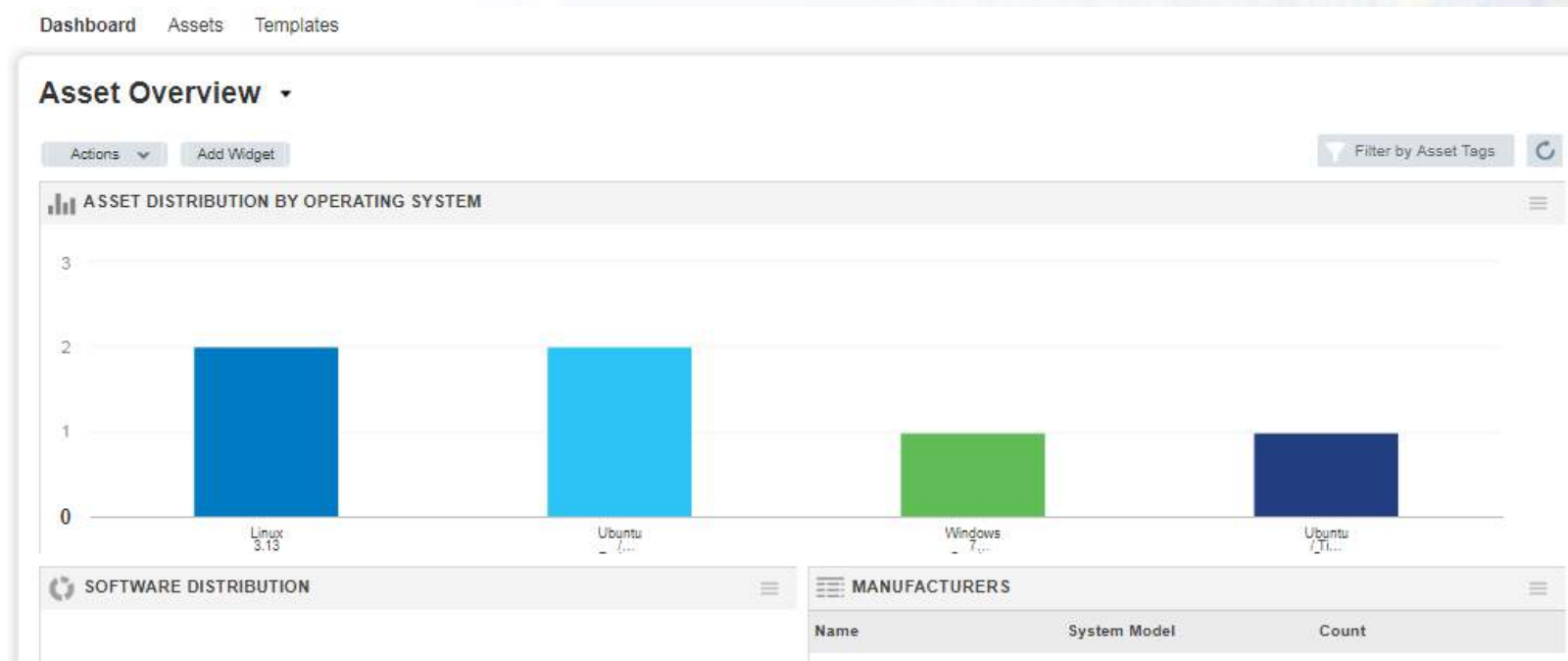
- Change management:
 - Change management inherent to all change processes
 - Change management requires reviews and approvals
 - Configuration management database or repository

END

ASSET MANAGEMENT THROUGH QUALYS

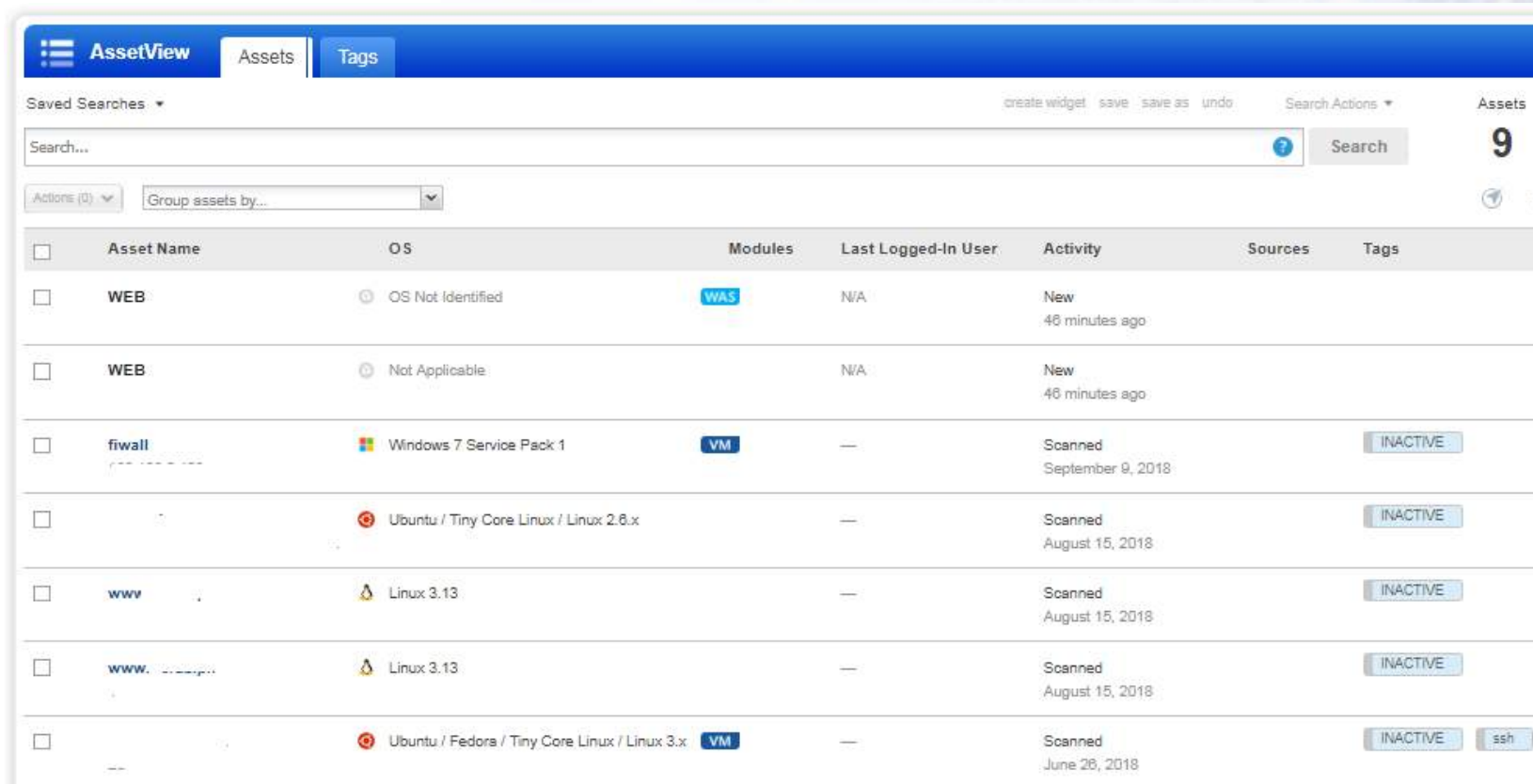
- Lets have a look at Qualys asset management capabilities

ASSET MANAGEMENT THROUGH QUALYS



QUALYS ASSET OVERVIEW DASHBOARD

ASSET MANAGEMENT THROUGH QUALYS



The screenshot displays the Qualys AssetView interface. At the top, there's a navigation bar with 'AssetView', 'Assets', and 'Tags' tabs. Below this, a search bar is present with a 'Search' button and a '9' indicating the number of results. A table lists various assets with columns for Asset Name, OS, Modules, Last Logged-In User, Activity, Sources, and Tags. The assets include 'WEB', 'fiwall', 'www', and 'www.ubuntu.com'. Some assets are marked as 'INACTIVE' or have specific tags like 'WAS' or 'VM'.

☐	Asset Name	OS	Modules	Last Logged-In User	Activity	Sources	Tags
☐	WEB	OS Not Identified	WAS	N/A	New 46 minutes ago		
☐	WEB	Not Applicable		N/A	New 46 minutes ago		
☐	fiwall	Windows 7 Service Pack 1	VM	—	Scanned September 9, 2018		INACTIVE
☐		Ubuntu / Tiny Core Linux / Linux 2.6.x		—	Scanned August 15, 2018		INACTIVE
☐	www	Linux 3.13		—	Scanned August 15, 2018		INACTIVE
☐	www.ubuntu.com	Linux 3.13		—	Scanned August 15, 2018		INACTIVE
☐		Ubuntu / Fedora / Tiny Core Linux / Linux 3.x	VM	—	Scanned June 28, 2018		INACTIVE ssh

ASSETS LIST

ASSET MANAGEMENT THROUGH QUALYS

Add a new widget to your dashboard

Templates

Search

All22

Threat13

Assets5

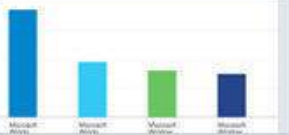
Shared0

Pick a preconfigured widget to add to your dashboard or [create a custom widget](#)

You can also create and customize your own widgets.

Assets with exploits available

A column chart displaying your assets which have an exploit available, broken down by operating system.



Assets with Qualys TOP-10 external vulnerabilities

See how many assets contain vulnerabilities listed amongst Qualys TOP-10 external vulns.

ASSETS WITH QUALYS TOP 10 EXTERNAL VULNERABILITIES
116

Assets with Qualys TOP-10 internal vulnerabilities

See how many assets contain vulnerabilities listed amongst Qualys TOP-10 internal vulns.

ASSETS WITH QUALYS TOP 10 INTERNAL VULNERABILITIES
69

Latest Threat Feeds

View the Latest Threats as provided by the Qualys threat intelligence feed. Get correlation data with your existing assets and measure the threat severity.

LATEST THREATS FROM LIVE FEED

Title	Impa...	Seve...	Publi...
Adobe Flash Player under ne...	101	HIGH	4/5/2018
Latest Adobe 0-day now in An...	101	HIGH	3/26/20...
Oracle patches 0-day in Java	118	HIGH	3/24/20...

Custom Count

ASSETS WITH HINDATCMARIE

Cancel

Add to Dashboard

ADD NEW ASSET WIDGET TO DASHBOARD

4

ASSET MANAGEMENT THROUGH QUALYS

Create a new dashboard

Templates

Search

All8

Threat2

Assets5

Shared0

Create a new dashboard from an existing template

Start by picking the desired template and click Next to customize it.

Stack Clash

This dashboard provides details on systems that have not been patched for the Stack Clash vulnerability. A widget is also included to track a related privilege escalation vulnerability in sudo. The checks against this vulnerability require authenticated scanning or the Qualys Cloud Agent.



WannaCry and Shadow Brokers

This dashboard provides details on systems that have not been patched for vulnerabilities exploited by EternalBlue, such as WannaCry and other malware. It also contains widgets for tracking exploited systems that have WannaCry or the DoublePulsar backdoor as well as widgets to track other Shadow Brokers vulnerabilities.



Asset Overview

This dashboard provides a general overview of your assets.

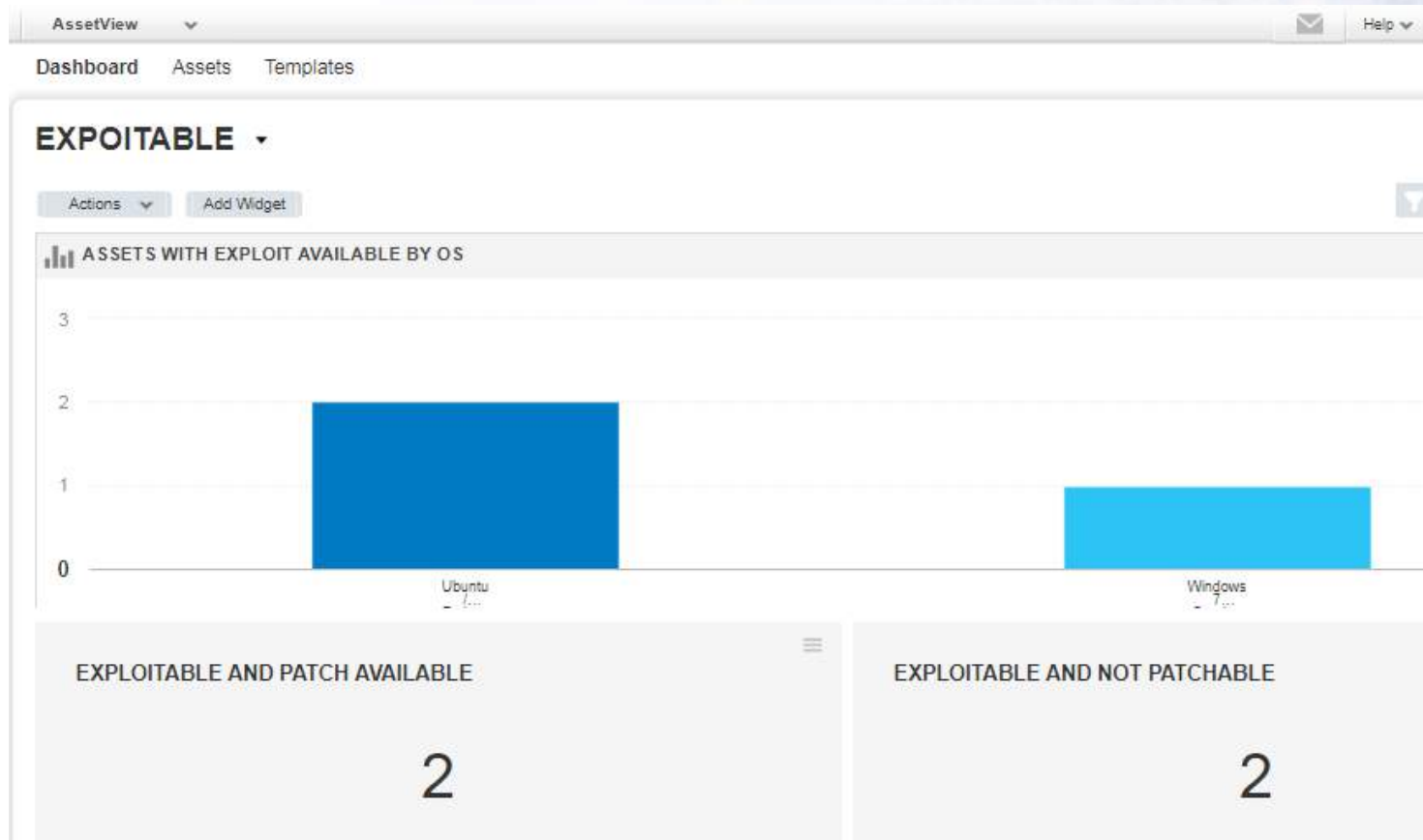


Cancel

Next

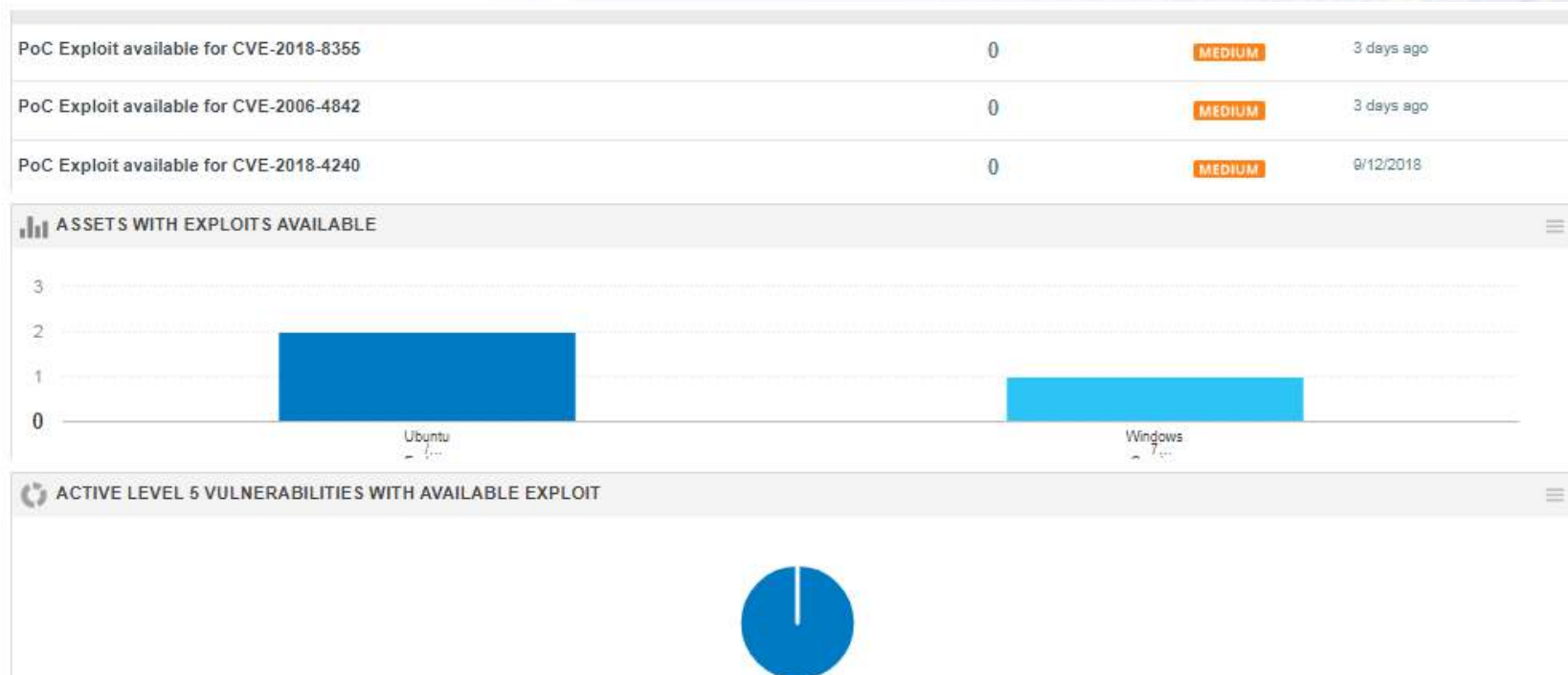
CREATE A NEW DASHBOARD

ASSET MANAGEMENT THROUGH QUALYS



NEW DASHBOARD CREATED

ASSET MANAGEMENT THROUGH QUALYS



ASSETS WITH EXPLOITS AVAILABLE

ASSET MANAGEMENT THROUGH QUALYS

- Qualys allows various reporting and views on assets and their characteristics

END

ASSET MANAGEMENT TOOLS FOR SECURITY FUNCTIONS

- Asset management helps with the following security functions:
 1. Patch management
 2. Software whitelisting
 3. Software assets discovery and management
 4. Enterprise tracking and reporting

ASSET MANAGEMENT TOOLS FOR SECURITY FUNCTIONS

- Gartner refers to this area as Unified endpoint management (UEM):

ASSET MANAGEMENT TOOLS FOR SECURITY FUNCTIONS



GARTNER MAGIC QUADRANT FOR
UNIFIED ENDPOINT MANAGEMENT 2018

ASSET MANAGEMENT TOOLS FOR SECURITY FUNCTIONS

- Unified endpoint management (UEM) tools combine the management of multiple endpoint types in a single console. UEM tools perform the following functions:

GARTNER UEM 2018
REPORT

ASSET MANAGEMENT TOOLS FOR SECURITY FUNCTIONS

1. Configure, manage and monitor iOS, Android, Windows 10 and macOS, and manage some Internet of Things (IoT) and wearable endpoints.
2. Unify the application of configurations, management profiles, device compliance and data protection.

ASSET MANAGEMENT TOOLS FOR SECURITY FUNCTIONS

3. Provide a single view of multidevice users, enhancing efficacy of end-user support and gathering detailed workplace analytics.

4. Act as a coordination point to orchestrate the activities of related endpoint technologies such as identity services and security infrastructure.

ASSET MANAGEMENT TOOLS FOR SECURITY FUNCTIONS



Compliance

Continuous policy enforcement and reporting

→ [Learn more](#)



Lifecycle

Software patching, distribution and provisioning

→ [Learn more](#)



Inventory

Audit authorized and unauthorized software

→ [Learn more](#)



Patch

Automated patching with high first-pass success

→ [Learn more](#)

<https://www.ibm.com/security/endpoint-security/bigfix>

ASSET MANAGEMENT TOOLS FOR SECURITY FUNCTIONS

MICROSOFT SOFTWARE RESTRICTION POLICIES (SRP) FOR WHITELISTING

- Software Restriction Policies (SRP) is Group Policy-based feature that identifies software programs running on computers in a domain, and controls the ability of those programs to run.

ASSET MANAGEMENT TOOLS FOR SECURITY FUNCTIONS

- ... Software restriction policies are part of the Microsoft security and management strategy to assist enterprises in increasing the reliability, integrity, and manageability of their computers.

ASSET MANAGEMENT TOOLS FOR SECURITY FUNCTIONS

- ... You can also use software restriction policies to create a highly restricted configuration for computers, in which you allow only specifically identified applications to run. Software restriction policies are integrated with Microsoft Active Directory and Group Policy.

ASSET MANAGEMENT TOOLS FOR SECURITY FUNCTIONS

- You can also create software restriction policies on stand-alone computers. Software restriction policies are trust policies, which are regulations set by an administrator to restrict scripts and other code that is not fully trusted from running.

<https://docs.microsoft.com/en-us/windows-server/identity/software-restriction-policies/software-restriction-policies>

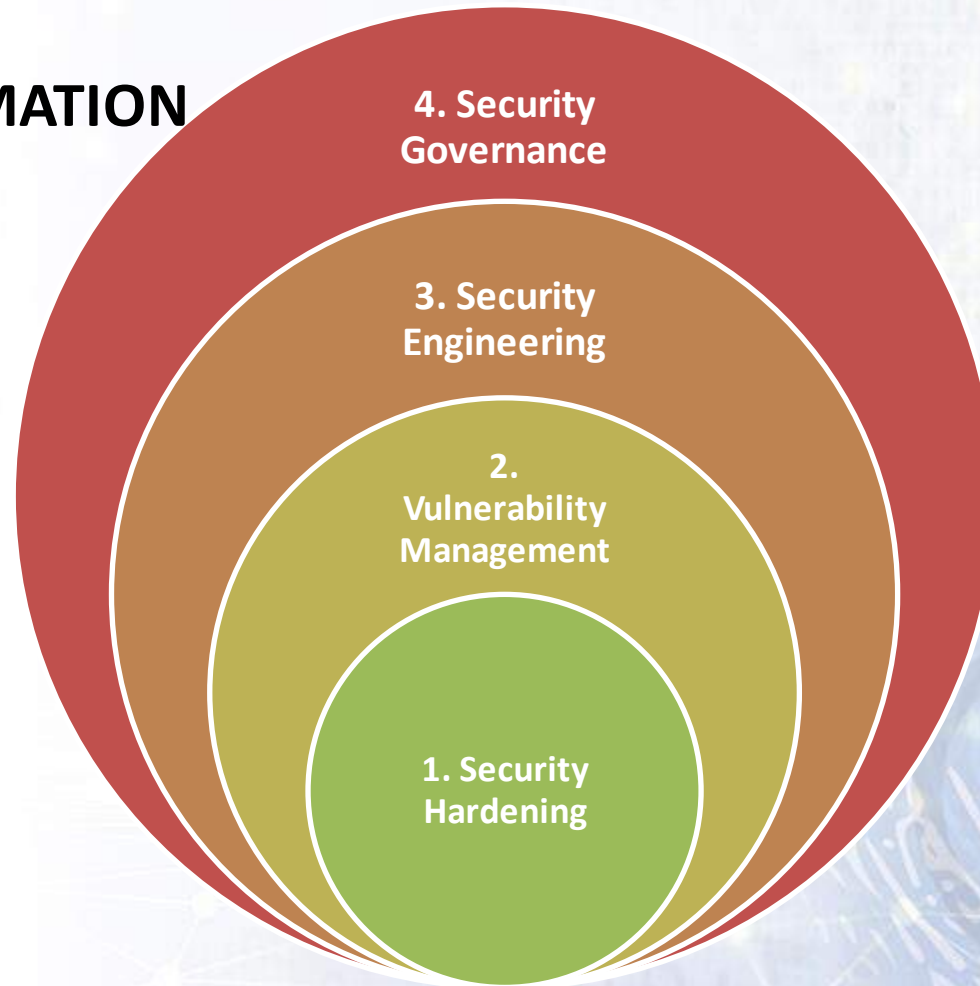
END

WHAT IS SECURITY ENGINEERING ?

- Security Engineering is the third layer of the Security Transformation Model
- Consists of more in-depth and complicated security activities which take more time and effort
- Many times related to security architecture

WHAT IS SECURITY ENGINEERING ?

SECURITY TRANSFORMATION MODEL



WHAT IS SECURITY ENGINEERING ?

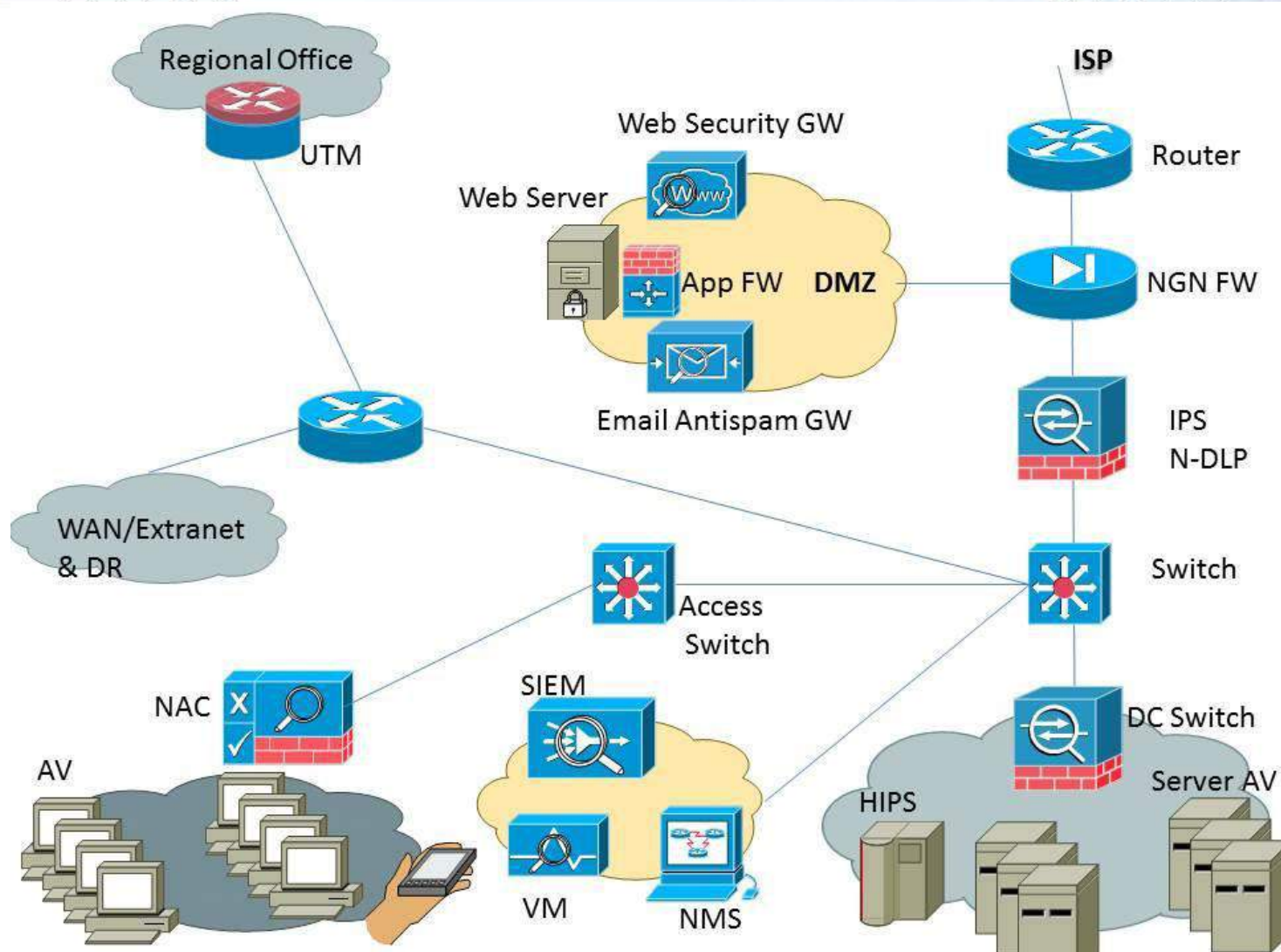
- Types of activities for security engineering:
 - FW granular access lists
 - Building an effective DMZ architecture
 - Segregating the network with VLANs
 - Adding a security tool such as SIEM, FW, DLP, NAC, etc
 - App-DB encryption

alag kerna

WHAT IS SECURITY ENGINEERING ?

- DMZ Architecture Case Study:
 - DMZ is an important zone in the overall security architecture
 - Devices which need to communicate to outside world placed in DMZ
 - Web servers, email gateways, web gateways

WHAT IS SECURITY ENGINEERING ?



WHAT IS SECURITY ENGINEERING ?

- FW Access List Case Study:
 - Most of the industry has not worked on building granular access lists
 - Most FWs have “allow all” for traffic
 - Granular access lists need to be built based on servers, or traffic flows

WHAT IS SECURITY ENGINEERING ?

- Why at Layer 3 of Security Transformation Model?
 - Low hanging fruit first
 - Teams tend to get bogged down with advanced security tasks
 - These take time, effort, and often budget approval

END

WHAT IS THE OBJECTIVE OF SECURITY ENGINEERING ?

- Security architecture as per best-practices
- The right security devices in the right places
- Effective security configuration of security devices (features)
- Optimum operation of security devices
- Aggregate controls

WHAT IS THE OBJECTIVE OF SECURITY ENGINEERING ?

**SECURITY ENGINEERING
STRUCTURE**

OPERATION

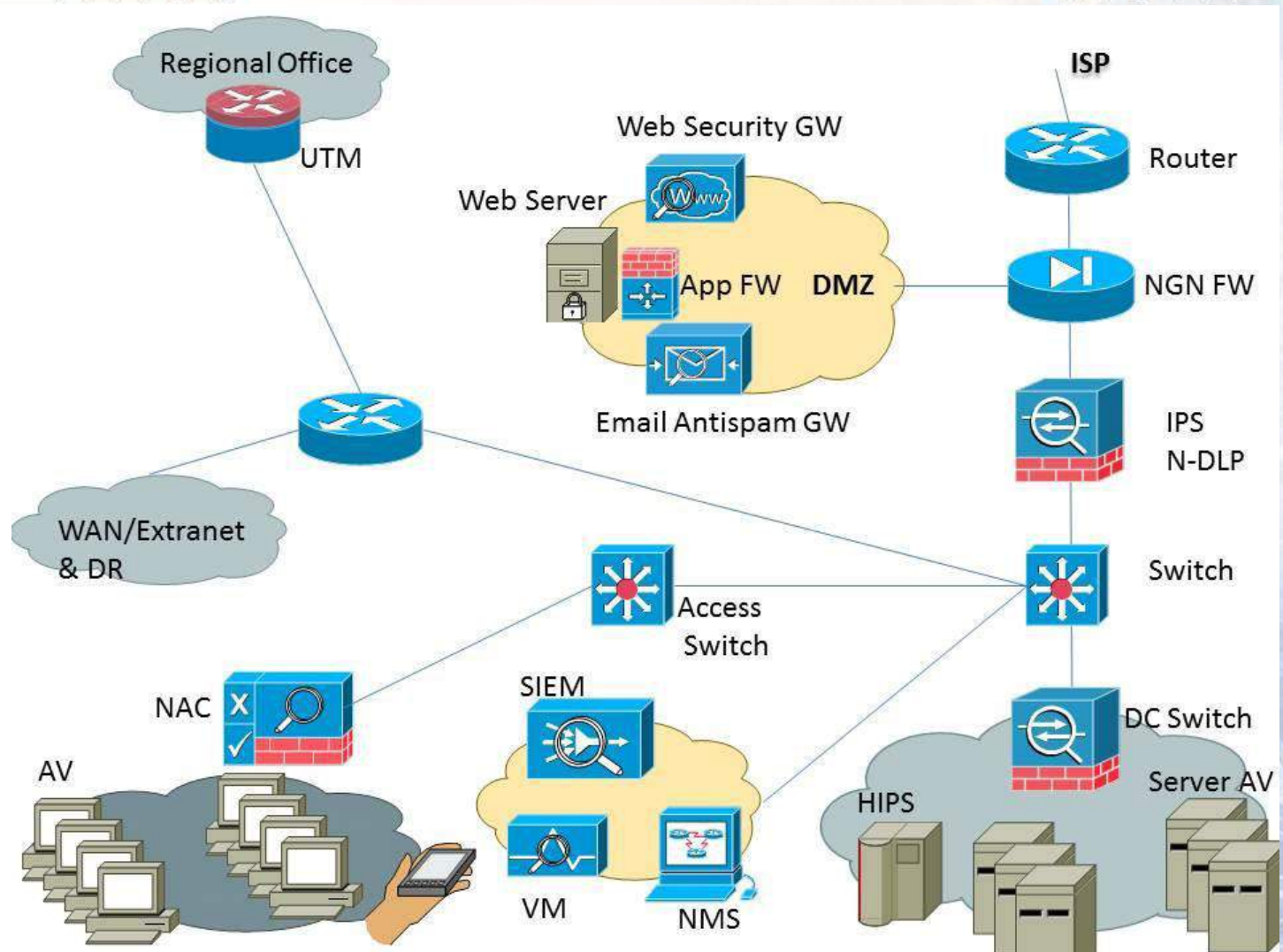
FEATURES & CONFIG

ARCHITECTURE

WHAT IS THE OBJECTIVE OF SECURITY ENGINEERING ?

- Examples:
 - FW first and then IPS
 - Edge FW, data center FW
 - Malware protection at the network edge
 - VPN termination on remote access VPN device
 - VPN tunnels for extranet connectivity

WHAT IS THE OBJECTIVE OF SECURITY ENGINEERING ?



WHAT IS THE OBJECTIVE OF SECURITY ENGINEERING ?

- The right time for setting up security engineering is when a new network is being designed & implemented
- Fixing a poorly architected operational network is an arduous task

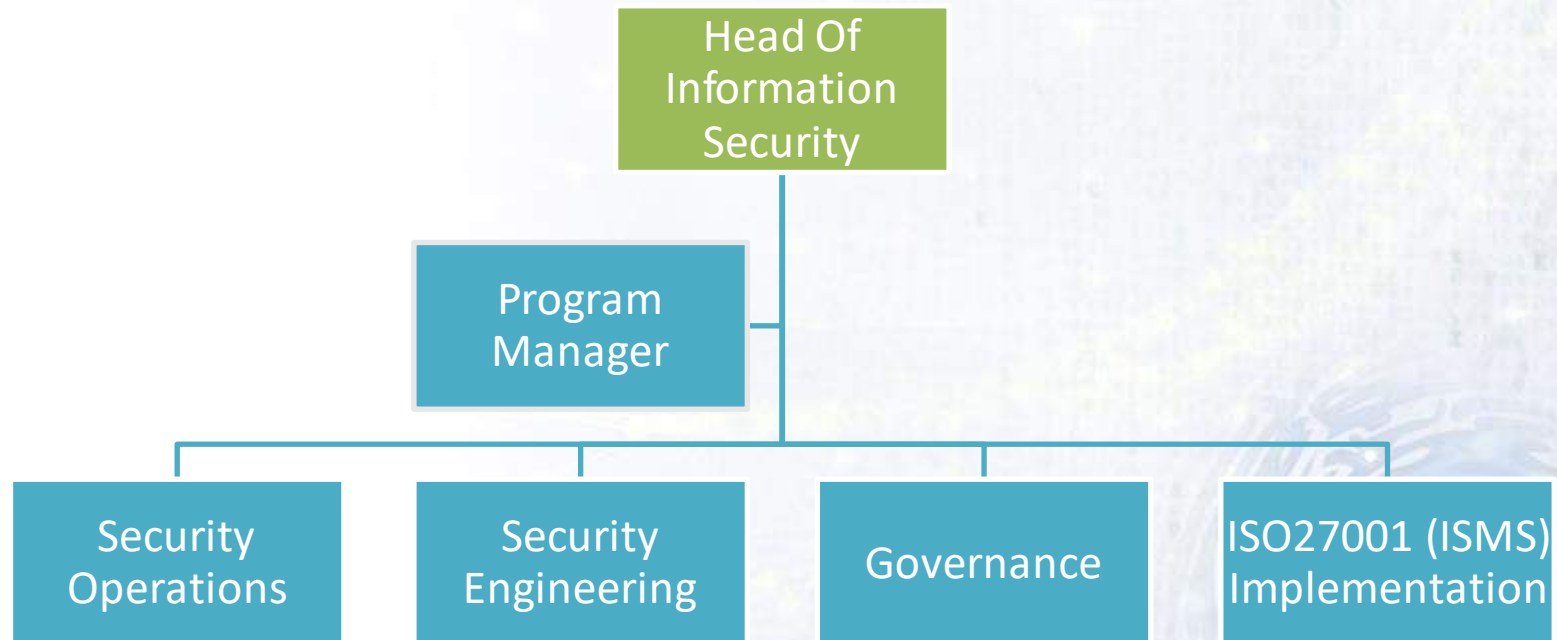
END

WHOSE RESPONSIBILITY IS SECURITY ENGINEERING ?

- Security Engineering can best be accomplished with effective team work

WHOSE RESPONSIBILITY IS SECURITY ENGINEERING ?

TYPICAL STRUCTURE OF AN INFORMATION SECURITY TEAM



WHOSE RESPONSIBILITY IS SECURITY ENGINEERING ?

ACTIVITY	TEAM
SECURITY REQUIREMENTS	INFORMATION SECURITY WITH IT CONSULTATION
SECURITY DESIGN	NETWORK/IT SECURITY ASSISTED BY VENDOR
VALIDATING SECURITY DESIGN	INFORMATION SECURITY
SECURITY IMPLEMENTATION	NETWORK/IT SECURITY ASSISTED BY VENDOR
VALIDATING SECURITY REQMTS MET	INFORMATION SECURITY TEAM

WHOSE RESPONSIBILITY IS SECURITY ENGINEERING ?

- As Security Engineering involves in-depth knowledge of IT & Security, the necessary resources, knowledge, skills, and people need to be pooled to achieve the objectives effectively

END

CIS 20 CRITICAL SECURITY CONTROLS

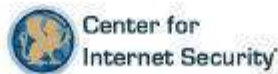
- What are the CIS 20 Critical Security Controls?

CIS 20 CRITICAL SECURITY CONTROLS



The CIS Critical Security Controls for Effective Cyber Defense

Version 6.1



<https://www.cisecurity.org/controls/>

CIS 20 CRITICAL SECURITY CONTROLS

CIS Controls

- 
- 1: Inventory of Authorized and Unauthorized Devices →
 - 2: Inventory of Authorized and Unauthorized Software →
 - 3: Secure Configurations for Hardware and Software →
 - 4: Continuous Vulnerability Assessment and Remediation →
 - 5: Controlled Use of Administrative Privileges →
 - 6: Maintenance, Monitoring, and Analysis of Audit Logs →
 - 7: Email and Web Browser Protections →
 - 8: Malware Defenses →
 - 9: Limitation and Control of Network Ports →
 - 10: Data Recovery Capability →
 - 11: Secure Configurations for Network Devices →
 - 12: Boundary Defense →
 - 13: Data Protection →
 - 14: Controlled Access Based on the Need to Know →
 - 15: Wireless Access Control →
 - 16: Account Monitoring and Control →
 - 17: Security Skills Assessment and Appropriate Training to Fill Gaps →
 - 18: Application Software Security →
 - 19: Incident Response and Management →
 - 20: Penetration Tests and Red Team Exercises →

<https://www.cisecurity.org/controls/>

CIS Critical Security Controls

https://www.cisecurity.org/wp-content/uploads/2017/03/Poster_Winter2016_CSCs.pdf

CIS 20 CRITICAL SECURITY CONTROLS

- CSC 1: Inventory of Authorized and Unauthorized Devices
- CSC 2: Inventory of Authorized and Unauthorized Software
- CSC 3: Secure Configurations for Hardware and Software on Mobile Devices, Laptops, Workstations, and Servers

CIS 20 CRITICAL SECURITY CONTROLS

- CSC 4: Continuous Vulnerability Assessment and Remediation
- CSC 5: Controlled Use of Administrative Privileges
- CSC 6: Maintenance, Monitoring, and Analysis of Audit Logs

CIS 20 CRITICAL SECURITY CONTROLS

- CSC 8: Malware Defenses
- CSC 9: Limitation and Control of Network Ports, Protocols, and Services
- CSC 10: Data Recovery Capability

CIS 20 CRITICAL SECURITY CONTROLS

- CSC 11: Secure Configurations for Network Devices such as Firewalls, Routers, and Switches
- CSC 12: Boundary Defense
- CSC 13: Data Protection

CIS 20 CRITICAL SECURITY CONTROLS

- CSC 14: Controlled Access Based on the Need to Know
- CSC 15: Wireless Access Control
- CSC 16: Account Monitoring and Control

CIS 20 CRITICAL SECURITY CONTROLS

- CSC 17: Security Skills Assessment and Appropriate Training to Fill Gaps
- CSC 18: Application Software Security
- CSC 19: Incident Response and Management

CIS 20 CRITICAL SECURITY CONTROLS

- CSC 20: Penetration Tests and Red Team Exercises

END

CSC1: Inventory Of Authorized & Unauthorized Devices

- 1.1: Deploy an automated asset inventory discovery tool and use it to build a preliminary inventory of systems connected to an organization's public and private network(s).

CSC1: Inventory Of Authorized & Unauthorized Devices

- 1.1: ... Both active tools that scan through IPv4 or IPv6 network address ranges and passive tools that identify hosts based on analyzing their traffic should be employed.

CSC1: Inventory Of Authorized & Unauthorized Devices

- 1.2: If the organization is dynamically assigning addresses using DHCP, then deploy dynamic host configuration protocol (DHCP) server logging, and use this information to improve the asset inventory and help detect unknown systems.

CSC1: Inventory Of Authorized & Unauthorized Devices

- 1.3: Ensure that all equipment acquisitions automatically update the inventory system as new, approved devices are connected to the network.

CSC1: Inventory Of Authorized & Unauthorized Devices

- 1.4: Maintain an asset inventory of all systems connected to the network and the network devices themselves, recording at least the network addresses, machine name(s), purpose of each system, an asset owner responsible for each device...

CSC1: Inventory Of Authorized & Unauthorized Devices

- 1.4: ... and the department associated with each device.
- The inventory should include every system that has an Internet protocol (IP) address on the network, including but not limited to desktops, laptops, servers...

CSC1: Inventory Of Authorized & Unauthorized Devices

- ... network equipment (routers, switches, firewalls, etc.), printers, storage area networks, Voice Over-IP telephones, multi-homed addresses, virtual addresses, etc.

CSC1: Inventory Of Authorized & Unauthorized Devices

- The asset inventory created must also include data on whether the device is a portable and/or personal device.

CSC1: Inventory Of Authorized & Unauthorized Devices

- Devices such as mobile phones, tablets, laptops, and other portable electronic devices that store or process data must be identified, regardless of whether they are attached to the organization's network.

CSC1: Inventory Of Authorized & Unauthorized Devices

- 1.5: Deploy network level authentication via 802.1x to limit and control which devices can be connected to the network. The 802.1x must be tied into the inventory data to determine authorized versus unauthorized systems.

CSC1: Inventory Of Authorized & Unauthorized Devices

- 1.6: Use client certificates to validate and authenticate systems prior to connecting to the private network.

END

CSC2: Inventory Of Authorized & Unauthorized Software

- 2.1: Devise a list of authorized software and version that is required in the enterprise for each type of system, including servers, workstations, and laptops of various kinds and uses.

CSC2: Inventory Of Authorized & Unauthorized Software

- 2.1: ... This list should be monitored by file integrity checking tools to validate that the authorized software has not been modified.

CSC2: Inventory Of Authorized & Unauthorized Software

- 2.2: Deploy application whitelisting technology that allows systems to run software only if it is included on the whitelist and prevents execution of all other software on the system.

CSC2: Inventory Of Authorized & Unauthorized Software

- 2.2: ... The whitelist may be very extensive (as is available from commercial whitelist vendors), so that users are not inconvenienced when using common software.

CSC2: Inventory Of Authorized & Unauthorized Software

- 2.2: ... Or, for some special-purpose systems (which require only a small number of programs to achieve their needed business functionality), the whitelist may be quite narrow.

CSC2: Inventory Of Authorized & Unauthorized Software

- 2.3: Deploy software inventory tools throughout the organization covering each of the operating system types in use, including servers, workstations, and laptops.

CSC2: Inventory Of Authorized & Unauthorized Software

- 2.3: ... The software inventory system should track the version of the underlying operating system as well as the applications installed on it.

CSC2: Inventory Of Authorized & Unauthorized Software

- 2.3: ... The software inventory systems must be tied into the hardware asset inventory so all devices and associated software are tracked from a single location.

CSC2: Inventory Of Authorized & Unauthorized Software

- 2.4: Virtual machines and/or air-gapped systems should be used to isolate and run applications that are required for business operations but based on higher risk should not be installed within a networked environment.

END

CSC3-I: Secure Configurations For HW & SW

CSC3-I: Secure Configurations For HW & SW

CIS Controls

- 1: Inventory of Authorized and Unauthorized Devices →
- 2: Inventory of Authorized and Unauthorized Software →
- 3: Secure Configurations for Hardware and Software →
- 4: Continuous Vulnerability Assessment and Remediation →
- 5: Controlled Use of Administrative Privileges →
- 6: Maintenance, Monitoring, and Analysis of Audit Logs →
- 7: Email and Web Browser Protections →
- 8: Malware Defenses →
- 9: Limitation and Control of Network Ports →
- 10: Data Recovery Capability →
- 11: Secure Configurations for Network Devices →
- 12: Boundary Defense →
- 13: Data Protection →
- 14: Controlled Access Based on the Need to Know →
- 15: Wireless Access Control →
- 16: Account Monitoring and Control →
- 17: Security Skills Assessment and Appropriate Training to Fill Gaps →
- 18: Application Software Security →
- 19: Incident Response and Management →
- 20: Penetration Tests and Red Team Exercises →

<https://www.cisecurity.org/controls/>

CSC3-I: Secure Configurations For HW & SW

- 3.1 Establish standard secure configurations of your operating systems and software applications.
- Standardized images should represent hardened versions of the underlying operating system and the applications installed on the system.

CSC3-I: Secure Configurations For HW & SW

- 3.1...: These images should be validated and refreshed on a regular basis to update their security configuration in light of recent vulnerabilities and attack vectors.

CSC3-I: Secure Configurations For HW & SW

- 3.2: Follow strict configuration management, building a secure image that is used to build all new systems that are deployed in the enterprise.
- Any existing system that becomes compromised should be re-imaged with the secure build.

CSC3-I: Secure Configurations For HW & SW

- 3.2: Regular updates or exceptions to this image should be integrated into the organization's change management processes.
- Images should be created for workstations, servers, and other system types used by the organization.

CSC3-I: Secure Configurations For HW & SW

- 3.3: Store the master images on securely configured servers, validated with integrity checking tools capable of continuous inspection, and change management to ensure that only authorized changes to the images are possible.

CSC3-I: Secure Configurations For HW & SW

- 3.3...: Alternatively, these master images can be stored in offline machines, air-gapped from the production network, with images copied via secure media to move them between the image storage servers and the production network.

CSC3-I: Secure Configurations For HW & SW

- 3.4: Perform all remote administration of servers, workstation, network devices, and similar equipment over secure channels.

CSC3-I: Secure Configurations For HW & SW

- 3.4...: Protocols such as telnet, VNC, RDP, or others that do not actively support strong encryption should only be used if they are performed over a secondary encryption channel, such as SSL, TLS or IPSEC.

END

CSC3-II: Secure Configurations For HW & SW

CSC3-II: Secure Configurations For HW & SW

CIS Controls

- 1: Inventory of Authorized and Unauthorized Devices →
- 2: Inventory of Authorized and Unauthorized Software →
- 3: Secure Configurations for Hardware and Software →
- 4: Continuous Vulnerability Assessment and Remediation →
- 5: Controlled Use of Administrative Privileges →
- 6: Maintenance, Monitoring, and Analysis of Audit Logs →
- 7: Email and Web Browser Protections →
- 8: Malware Defenses →
- 9: Limitation and Control of Network Ports →
- 10: Data Recovery Capability →
- 11: Secure Configurations for Network Devices →
- 12: Boundary Defense →
- 13: Data Protection →
- 14: Controlled Access Based on the Need to Know →
- 15: Wireless Access Control →
- 16: Account Monitoring and Control →
- 17: Security Skills Assessment and Appropriate Training to Fill Gaps →
- 18: Application Software Security →
- 19: Incident Response and Management →
- 20: Penetration Tests and Red Team Exercises →

<https://www.cisecurity.org/controls/>

CSC3-II: Secure Configurations For HW & SW

- 3.5: Use file integrity checking tools to ensure that critical system files (including sensitive system and application executables, libraries, and configurations) have not been altered.

CSC3-II: Secure Configurations For HW & SW

- 3.5...: The reporting system should have the ability to account for routine and expected changes; highlight and alert on unusual or unexpected alterations; show the history of configuration changes over time and identify who made the change...

CSC3-II: Secure Configurations For HW & SW

- 3.5: (including the original logged-in account in the event of a user ID switch, such as with the su or sudo command).

CSC3-II: Secure Configurations For HW & SW

- 3.5...: These integrity checks should identify suspicious system alterations such as: owner and permissions changes to files or directories; the use of alternate data streams which could be used to hide malicious activities;

CSC3-II: Secure Configurations For HW & SW

- 3.5...: and the introduction of extra files into key system areas (which could indicate malicious payloads left by attackers or additional files inappropriately added during batch distribution processes).

CSC3-II: Secure Configurations For HW & SW

- 3.6: Implement and test an automated configuration monitoring system that verifies all remotely testable secure configuration elements, and alerts when unauthorized changes occur.

CSC3-II: Secure Configurations For HW & SW

- 3.6...: This includes detecting new listening ports, new administrative users, changes to group and local policy objects (where applicable), and new services running on a system.

CSC3-II: Secure Configurations For HW & SW

- 3.6...: Whenever possible use tools compliant with the Security Content Automation Protocol (SCAP) in order to streamline reporting and integration.

CSC3-II: Secure Configurations For HW & SW

- 3.7: Deploy system configuration management tools, such as **Active Directory Group Policy Objects** for Microsoft Windows systems or **Puppet for UNIX systems** that will automatically enforce and redeploy configuration settings to systems at regularly scheduled intervals.

CSC3-II: Secure Configurations For HW & SW

- 3.7...: They should be capable of triggering redeployment of configuration settings on a scheduled, manual, or event-driven basis.

END

CSC4-I: Continuous Vuln. Assessment & Remediation

CSC4-I: Continuous Vuln. Assessment & Remediation

CIS Controls

- 
- The diagram shows a list of 20 CIS Controls. A blue bracket on the left groups the first five controls (1-5). An orange bracket on the left groups the remaining 15 controls (6-20).
- 1: Inventory of Authorized and Unauthorized Devices →
 - 2: Inventory of Authorized and Unauthorized Software →
 - 3: Secure Configurations for Hardware and Software →
 - 4: Continuous Vulnerability Assessment and Remediation →
 - 5: Controlled Use of Administrative Privileges →
 - 6: Maintenance, Monitoring, and Analysis of Audit Logs →
 - 7: Email and Web Browser Protections →
 - 8: Malware Defenses →
 - 9: Limitation and Control of Network Ports →
 - 10: Data Recovery Capability →
 - 11: Secure Configurations for Network Devices →
 - 12: Boundary Defense →
 - 13: Data Protection →
 - 14: Controlled Access Based on the Need to Know →
 - 15: Wireless Access Control →
 - 16: Account Monitoring and Control →
 - 17: Security Skills Assessment and Appropriate Training to Fill Gaps →
 - 18: Application Software Security →
 - 19: Incident Response and Management →
 - 20: Penetration Tests and Red Team Exercises →

<https://www.cisecurity.org/controls/>

CSC4-I: Continuous Vuln. Assessment & Remediation

- 4.1: Run automated vulnerability scanning tools against all systems on the network on a weekly or more frequent basis and deliver prioritized lists of the most critical vulnerabilities to each responsible system administrator...

CSC4-I: Continuous Vuln. Assessment & Remediation

- 4.1...: along with risk scores that compare the effectiveness of system administrators and departments in reducing risk.

CSC4-I: Continuous Vuln. Assessment & Remediation

- 4.1...: Use a SCAP-validated vulnerability scanner that looks for both code-based vulnerabilities (such as those described by Common

CSC4-I: Continuous Vuln. Assessment & Remediation

- Vulnerabilities and Exposures entries) and configuration-based vulnerabilities (as enumerated by the Common Configuration Enumeration Project).

CSC4-I: Continuous Vuln. Assessment & Remediation

- 4.2: Correlate event logs with information from vulnerability scans to fulfill two goals.
- First, personnel should verify that the activity of the regular vulnerability scanning tools is itself logged.

CSC4-I: Continuous Vuln. Assessment & Remediation

- 4.2...: Second, personnel should be able to correlate attack detection events with prior vulnerability scanning results to determine whether the given exploit was used against a target known to be vulnerable.

CSC4-I: Continuous Vuln. Assessment & Remediation

- 4.3: Perform vulnerability scanning in authenticated mode either with agents running locally on each end system to analyze the security configuration or with remote scanners that are given administrative rights on the system being tested.

CSC4-I: Continuous Vuln. Assessment & Remediation

- 4.3...: Use a dedicated account for authenticated vulnerability scans, which should not be used for any other administrative activities and should be tied to specific machines at specific IP addresses.

CSC4-I: Continuous Vuln. Assessment & Remediation

- 4.3...: Ensure that only authorized employees have access to the vulnerability management user interface and that roles are applied to each user

CSC4-I: Continuous Vuln. Assessment & Remediation

- 4.4: Subscribe to vulnerability intelligence services in order to stay aware of emerging exposures, and use the information gained from this subscription to update the organization's vulnerability scanning activities on at least a monthly basis.

CSC4-I: Continuous Vuln. Assessment & Remediation

- 4.4...: Alternatively, ensure that the vulnerability scanning tools you use are regularly updated with all relevant important security vulnerabilities.

END

CSC4-II: Continuous Vuln. Assessment & Remediation

CSC4-II: Continuous Vuln. Assessment & Remediation

CIS Controls

- 
- The diagram shows a list of 20 CIS Controls. A blue bracket on the left groups the first five controls (1-5). An orange bracket on the left groups the remaining 15 controls (6-20).
- 1: Inventory of Authorized and Unauthorized Devices →
 - 2: Inventory of Authorized and Unauthorized Software →
 - 3: Secure Configurations for Hardware and Software →
 - 4: Continuous Vulnerability Assessment and Remediation →
 - 5: Controlled Use of Administrative Privileges →
 - 6: Maintenance, Monitoring, and Analysis of Audit Logs →
 - 7: Email and Web Browser Protections →
 - 8: Malware Defenses →
 - 9: Limitation and Control of Network Ports →
 - 10: Data Recovery Capability →
 - 11: Secure Configurations for Network Devices →
 - 12: Boundary Defense →
 - 13: Data Protection →
 - 14: Controlled Access Based on the Need to Know →
 - 15: Wireless Access Control →
 - 16: Account Monitoring and Control →
 - 17: Security Skills Assessment and Appropriate Training to Fill Gaps →
 - 18: Application Software Security →
 - 19: Incident Response and Management →
 - 20: Penetration Tests and Red Team Exercises →

<https://www.cisecurity.org/controls/>

CSC4-II: Continuous Vuln. Assessment & Remediation

- 4.5: Deploy automated patch management tools and software update tools for operating system and software/applications on all systems for which such tools are available and safe.

CSC4-II: Continuous Vuln. Assessment & Remediation

- 4.5...: Patches should be applied to all systems, even systems that are properly air gapped.
- 4.6: Monitor logs associated with any scanning activity and associated administrator accounts to ensure that this activity is limited to the timeframes of legitimate scans.

CSC4-II: Continuous Vuln. Assessment & Remediation

- 4.7: Compare the results from back-to-back vulnerability scans to verify that vulnerabilities were addressed either by patching, implementing a compensating control, or documenting and accepting a reasonable business risk.

CSC4-II: Continuous Vuln. Assessment & Remediation

- 4.7...: Such acceptance of business risks for existing vulnerabilities should be periodically reviewed to determine if newer compensating controls or subsequent patches can address vulnerabilities that were previously accepted, or if conditions have changed, increasing the risk.

CSC4-II: Continuous Vuln. Assessment & Remediation

- 4.8: Establish a process to risk-rate vulnerabilities based on the exploitability and potential impact of the vulnerability, and segmented by appropriate groups of assets (example, DMZ servers, internal network servers, desktops, laptops).

CSC4-II: Continuous Vuln. Assessment & Remediation

- 4.8...: Apply patches for the riskiest vulnerabilities first.
- A phased rollout can be used to minimize the impact to the organization.
- Establish expected patching timelines based on the risk rating level.

END

CSC5-I: Controlled Use Of Administrative Privileges

CSC5-I: Controlled Use Of Administrative Privileges

CIS Controls

- 1: Inventory of Authorized and Unauthorized Devices →
- 2: Inventory of Authorized and Unauthorized Software →
- 3: Secure Configurations for Hardware and Software →
- 4: Continuous Vulnerability Assessment and Remediation →
- 5: Controlled Use of Administrative Privileges →
- 6: Maintenance, Monitoring, and Analysis of Audit Logs →
- 7: Email and Web Browser Protections →
- 8: Malware Defenses →
- 9: Limitation and Control of Network Ports →
- 10: Data Recovery Capability →
- 11: Secure Configurations for Network Devices →
- 12: Boundary Defense →
- 13: Data Protection →
- 14: Controlled Access Based on the Need to Know →
- 15: Wireless Access Control →
- 16: Account Monitoring and Control →
- 17: Security Skills Assessment and Appropriate Training to Fill Gaps →
- 18: Application Software Security →
- 19: Incident Response and Management →
- 20: Penetration Tests and Red Team Exercises →

<https://www.cisecurity.org/controls/>

CSC5-I: Controlled Use Of Administrative Privileges

- 5.1: Minimize administrative privileges and only use administrative accounts when they are required. Implement focused auditing on the use of administrative privileged functions and monitor for anomalous behavior.

CSC5-I: Controlled Use Of Administrative Privileges

- 5.2: Use automated tools to inventory all administrative accounts and validate that each person with administrative privileges on desktops, laptops, and servers is authorized by a senior executive.

CSC5-I: Controlled Use Of Administrative Privileges

- 5.3: Before deploying any new devices in a networked environment, change all default passwords for applications, operating systems, routers, firewalls, wireless access points, and other systems to have values consistent with administration-level accounts.

CSC5-I: Controlled Use Of Administrative Privileges

- 5.4: Configure systems to issue a log entry and alert when an account is added to or removed from a domain administrators' group, or when a new local administrator account is added on a system.

CSC5-I: Controlled Use Of Administrative Privileges

- 5.5: Configure systems to issue a log entry and alert on any unsuccessful login to an administrative account.

END

CSC5-II: Controlled Use Of Administrative Privileges

CSC5-II: Controlled Use Of Administrative Privileges

CIS Controls

- 
- The diagram shows a list of 20 CIS Controls. A blue bracket on the left groups the first five controls (1-5). An orange bracket on the left groups the remaining 15 controls (6-20).
- 1: Inventory of Authorized and Unauthorized Devices →
 - 2: Inventory of Authorized and Unauthorized Software →
 - 3: Secure Configurations for Hardware and Software →
 - 4: Continuous Vulnerability Assessment and Remediation →
 - 5: Controlled Use of Administrative Privileges →
 - 6: Maintenance, Monitoring, and Analysis of Audit Logs →
 - 7: Email and Web Browser Protections →
 - 8: Malware Defenses →
 - 9: Limitation and Control of Network Ports →
 - 10: Data Recovery Capability →
 - 11: Secure Configurations for Network Devices →
 - 12: Boundary Defense →
 - 13: Data Protection →
 - 14: Controlled Access Based on the Need to Know →
 - 15: Wireless Access Control →
 - 16: Account Monitoring and Control →
 - 17: Security Skills Assessment and Appropriate Training to Fill Gaps →
 - 18: Application Software Security →
 - 19: Incident Response and Management →
 - 20: Penetration Tests and Red Team Exercises →

<https://www.cisecurity.org/controls/>

CSC5-II: Controlled Use Of Administrative Privileges

- 5.6: Use multifactor authentication for all administrative access, including domain administrative access.

CSC5-II: Controlled Use Of Administrative Privileges

- 5.6...: Multi-factor authentication can include a variety of techniques, to include the use of smart cards, certificates, One Time Password (OTP) tokens, biometrics, or other similar authentication methods.

CSC5-II: Controlled Use Of Administrative Privileges

- 5.7: Where multi-factor authentication is not supported, user accounts shall be required to use long passwords on the system (longer than 14 characters).

CSC5-II: Controlled Use Of Administrative Privileges

- 5.8: Administrators should be required to access a system using a fully logged and non-administrative account.

CSC5-II: Controlled Use Of Administrative Privileges

- 5.8...: Then, once logged on to the machine without administrative privileges, the administrator should transition to administrative privileges using tools such as Sudo on Linux/UNIX, RunAs on Windows, and other similar facilities for other types of systems.

CSC5-II: Controlled Use Of Administrative Privileges

- 5.9: Administrators shall use a dedicated machine for all administrative tasks or tasks requiring elevated access.

CSC5-II: Controlled Use Of Administrative Privileges

END

- 5.9...: This machine shall be isolated from the organization's primary network and not be allowed Internet access. This machine shall not be used for reading e-mail, composing documents, or surfing the Internet.

CIS CONTROL 9: LIMITATION & CONTROL OF NETWORK

CIS 20 Critical Security Controls

CIS CONTROL 9: LIMITATION & CONTROL OF NETWORK



V7

Basic

- 1 Inventory and Control of Hardware Assets
- 2 Inventory and Control of Software Assets
- 3 Continuous Vulnerability Management
- 4 Controlled Use of Administrative Privileges
- 5 Secure Configuration for Hardware and Software on Mobile Devices, Laptops, Workstations and Servers
- 6 Maintenance, Monitoring and Analysis of Audit Logs

Foundational

- 7 Email and Web Browser Protections
- 8 Malware Defenses
- 9 Limitation and Control of Network Ports, Protocols, and Services
- 10 Data Recovery Capabilities
- 11 Secure Configuration for Network Devices, such as Firewalls, Routers and Switches
- 12 Boundary Defense
- 13 Data Protection
- 14 Controlled Access Based on the Need to Know
- 15 Wireless Access Control
- 16 Account Monitoring and Control

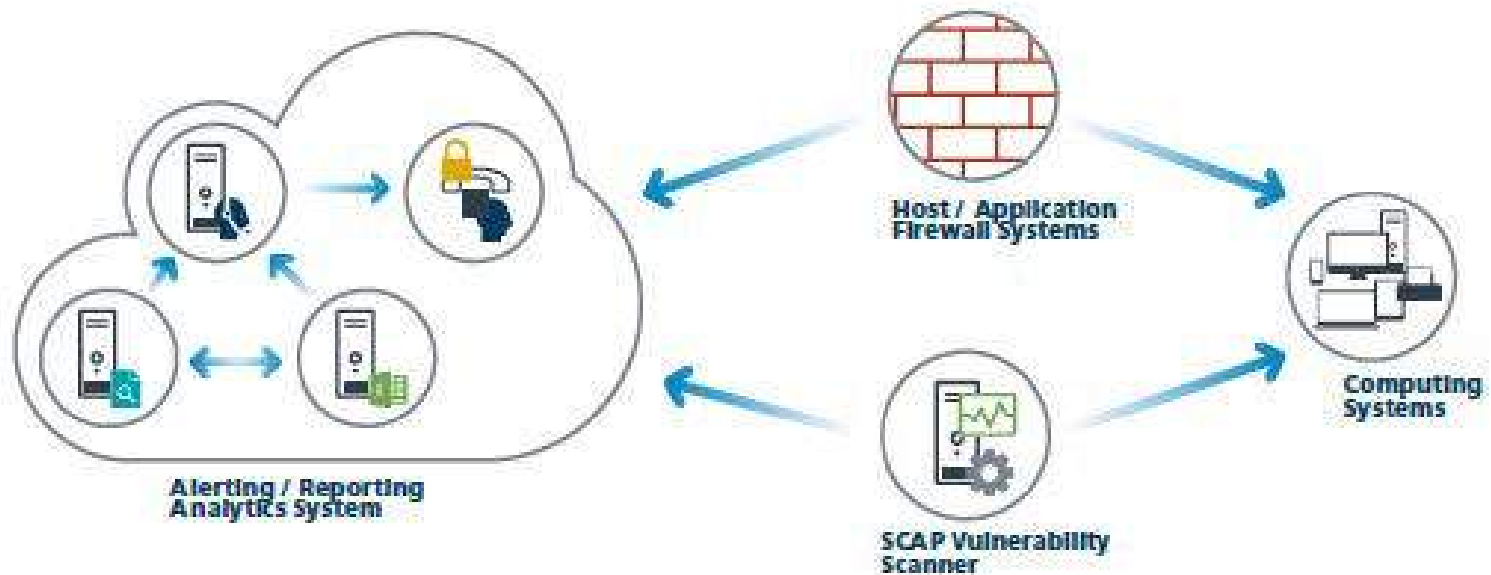
Organizational

- 17 Implement a Security Awareness and Training Program
- 18 Application Software Security
- 19 Incident Response and Management
- 20 Penetration Tests and Red Team Exercises

<https://www.cisecurity.org/controls/>

CIS CONTROL 9: LIMITATION & CONTROL OF NETWORK

CIS Control 9: System Entity Relationship Diagram



<https://www.cisecurity.org/controls/>

CIS CONTROL 9: LIMITATION & CONTROL OF NETWORK

9.1: Associate Active Ports, Services and Protocols to Asset Inventory

- Associate active ports, services and protocols to the hardware assets in the asset inventory.

CIS CONTROL 9: LIMITATION & CONTROL OF NETWORK

9.2: Ensure Only Approved Ports, Protocols and Services Are Running

- Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.

CIS CONTROL 9: LIMITATION & CONTROL OF NETWORK

9.3: Perform Regular Automated Port Scans

- Perform automated port scans on a regular basis against all systems and alert if unauthorized ports are detected on a system.

CIS CONTROL 9: LIMITATION & CONTROL OF NETWORK

9.4: Apply Host-based Firewalls or Port Filtering

- Apply host-based firewalls or port filtering tools on end systems, with a default-deny rule that drops all traffic except those services and ports that are explicitly allowed.

CIS CONTROL 9: LIMITATION & CONTROL OF NETWORK

9.5: Implement Application Firewalls

- Place application firewalls in front of any critical servers to verify and validate the traffic going to the server. Any unauthorized traffic should be blocked and logged.

CIS CONTROL 9: LIMITATION & CONTROL OF NETWORK

PROCEDURES & TOOLS:

- Port scanning tools are used to determine which services are listening on the network for a range of target systems. In addition to determining which ports are open, effective port scanners can be configured to identify the version of the protocol and service

CIS CONTROL 9: LIMITATION & CONTROL OF NETWORK

- ...listening on each discovered port. This list of services and their versions are compared against an inventory of services required by the organization for each server and workstation in an asset management system.

CIS CONTROL 9: LIMITATION & CONTROL OF NETWORK

- Recently added features in these port scanners are being used to determine the changes in services offered by scanned machines on the network since the previous scan, helping security personnel identify differences over time.

END

CIS CONTROL 10: DATA RECOVERY CAPABILITIES

CIS 20 Critical Security Controls

CIS CONTROL 10: DATA RECOVERY CAPABILITIES



V7

Basic

- 1 Inventory and Control of Hardware Assets
- 2 Inventory and Control of Software Assets
- 3 Continuous Vulnerability Management
- 4 Controlled Use of Administrative Privileges
- 5 Secure Configuration for Hardware and Software on Mobile Devices, Laptops, Workstations and Servers
- 6 Maintenance, Monitoring and Analysis of Audit Logs

Foundational

- 7 Email and Web Browser Protections
- 8 Malware Defenses
- 9 Limitation and Control of Network Ports, Protocols, and Services
- 10 Data Recovery Capabilities
- 11 Secure Configuration for Network Devices, such as Firewalls, Routers and Switches
- 12 Boundary Defense
- 13 Data Protection
- 14 Controlled Access Based on the Need to Know
- 15 Wireless Access Control
- 16 Account Monitoring and Control

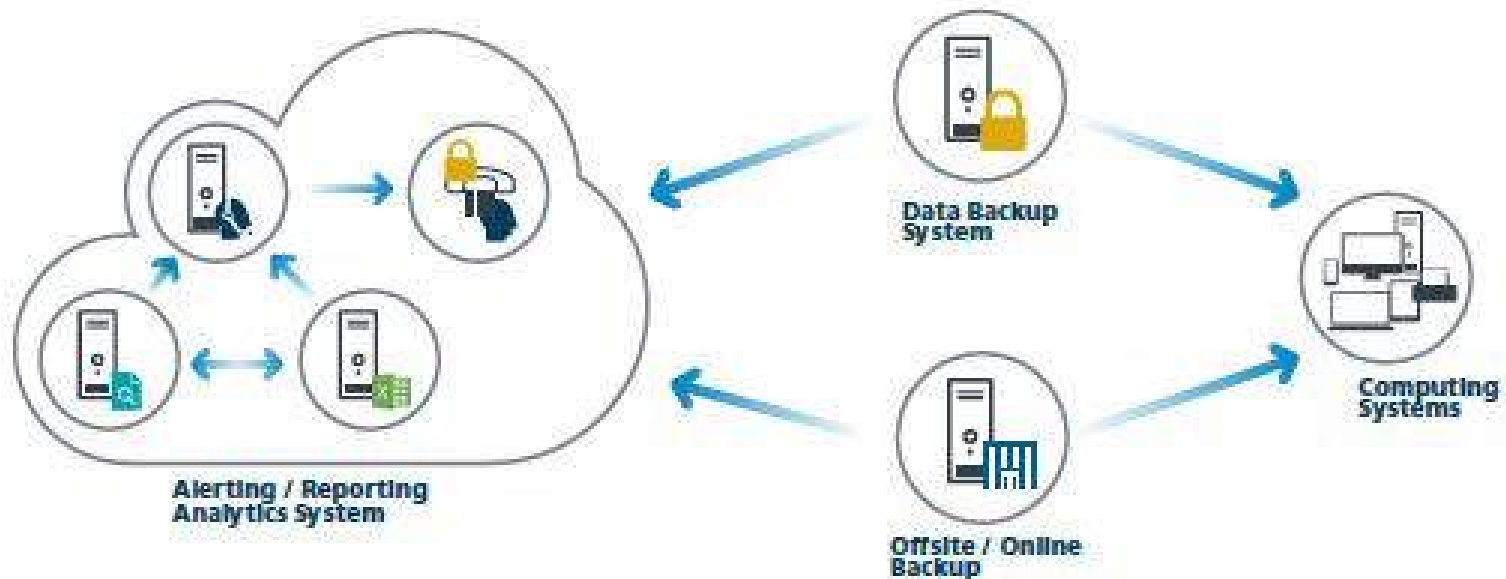
Organizational

- 17 Implement a Security Awareness and Training Program
- 18 Application Software Security
- 19 Incident Response and Management
- 20 Penetration Tests and Red Team Exercises

<https://www.cisecurity.org/controls/>

CIS CONTROL 10: DATA RECOVERY CAPABILITIES

CIS Control 10: System Entity Relationship Diagram



<https://www.cisecurity.org/controls/>

CIS CONTROL 10: DATA RECOVERY CAPABILITIES

10.1: **Ensure Regular Automated Back Ups**

- Ensure that all system data is automatically backed up on regular basis.

CIS CONTROL 10: DATA RECOVERY CAPABILITIES

10.2: Perform Complete System Backups

- Ensure that each of the organization's key systems are backed up as a complete system, through processes such as imaging, to enable the quick recovery of an entire system.

CIS CONTROL 10: DATA RECOVERY CAPABILITIES

10.3: Test Data on Backup Media

- Test data integrity on backup media on a regular basis by performing a data restoration process to ensure that the backup is properly working.

CIS CONTROL 10: DATA RECOVERY CAPABILITIES

10.4: Ensure Protection of Backups

- Ensure that backups are properly protected via physical security or encryption when they are stored, as well as when they are moved across the network. This includes remote backups and cloud services.

CIS CONTROL 10: DATA RECOVERY CAPABILITIES

10.5: Ensure Backups Have At least One Non-Continuously Addressable Destination

- Ensure that all backups have at least one backup destination that is not continuously addressable through operating system calls.

CIS CONTROL 10: DATA RECOVERY CAPABILITIES

Procedures & Tools:

- Once per quarter (or whenever new backup equipment is purchased), a testing team should evaluate a random sample of system backups by attempting to restore them on a test bed environment. The restored systems should

CIS CONTROL 10: DATA RECOVERY CAPABILITIES

- ... be verified to ensure that the operating system, application, and data from the backup are all intact and functional.
- In the event of malware infection, restoration procedures should use a version of the backup that is believed to predate the original infection.

END

CIS CONTROL 11: SECURE CONFIG FOR NETWORK DEVICES

- **SECURE
CONFIGURATION FOR
NETWORK DEVICES
SUCH AS FIREWALLS,
ROUTERS, AND
SWITCHES**

CIS CONTROL 11: SECURE CONFIG FOR NETWORK DEVICES



V7

Basic

- 1 Inventory and Control of Hardware Assets
- 2 Inventory and Control of Software Assets
- 3 Continuous Vulnerability Management
- 4 Controlled Use of Administrative Privileges
- 5 Secure Configuration for Hardware and Software on Mobile Devices, Laptops, Workstations and Servers
- 6 Maintenance, Monitoring and Analysis of Audit Logs

Foundational

- 7 Email and Web Browser Protections
- 8 Malware Defenses
- 9 Limitation and Control of Network Ports, Protocols, and Services
- 10 Data Recovery Capabilities
- 11 Secure Configuration for Network Devices, such as Firewalls, Routers and Switches
- 12 Boundary Defense
- 13 Data Protection
- 14 Controlled Access Based on the Need to Know
- 15 Wireless Access Control
- 16 Account Monitoring and Control

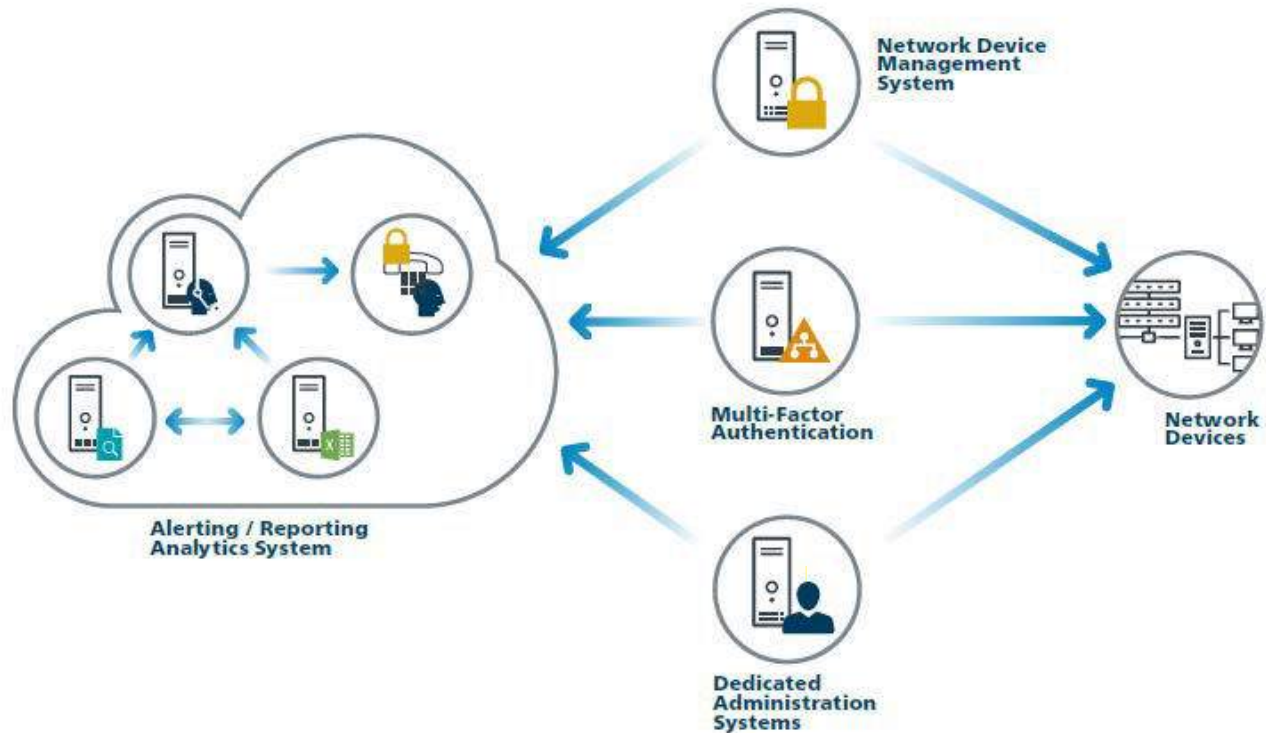
Organizational

- 17 Implement a Security Awareness and Training Program
- 18 Application Software Security
- 19 Incident Response and Management
- 20 Penetration Tests and Red Team Exercises

<https://www.cisecurity.org/controls/>

CIS CONTROL 11: SECURE CONFIG FOR NETWORK DEVICES

CIS Control 11: System Entity Relationship Diagram



<https://www.cisecurity.org/controls/>

CIS CONTROL 11: SECURE CONFIG FOR NETWORK DEVICES

11.1: Maintain Standard Security Configurations for Network Devices

- Maintain standard, documented security configuration standards for all authorized network devices.

CIS CONTROL 11: SECURE CONFIG FOR NETWORK DEVICES

11.2: Document Traffic Configuration Rules

- All configuration rules that allow traffic to flow through network devices should be documented in a configuration management system with a specific business reason for each rule,

CIS CONTROL 11: SECURE CONFIG FOR NETWORK DEVICES

11.2: Document Traffic Configuration Rules

- ... a specific individual's name responsible for that business need, and an expected duration of the need.

CIS CONTROL 11: SECURE CONFIG FOR NETWORK DEVICES

11.3: Use Automated Tools to Verify Standard Device Configurations and Detect Changes

- Compare all network device configuration against approved security configurations defined for each network device in use and alert when any deviation is discovered

CIS CONTROL 11: SECURE CONFIG FOR NETWORK DEVICES

11.4: Install the Latest Stable Version of Any Security-related Updates on All Network Devices

- Install the latest stable version of any security-related updates on all network devices.

END

CIS CONTROL 11: SECURE CONFIG FOR NETWORK DEVICES-II

- **SECURE
CONFIGURATION FOR
NETWORK DEVICES
SUCH AS FIREWALLS,
ROUTERS, AND
SWITCHES**

CIS CONTROL 11: SECURE CONFIG FOR NETWORK DEVICES-II



V7

Basic

- 1 Inventory and Control of Hardware Assets
- 2 Inventory and Control of Software Assets
- 3 Continuous Vulnerability Management
- 4 Controlled Use of Administrative Privileges
- 5 Secure Configuration for Hardware and Software on Mobile Devices, Laptops, Workstations and Servers
- 6 Maintenance, Monitoring and Analysis of Audit Logs

Foundational

- 7 Email and Web Browser Protections
- 8 Malware Defenses
- 9 Limitation and Control of Network Ports, Protocols, and Services
- 10 Data Recovery Capabilities
- 11 Secure Configuration for Network Devices, such as Firewalls, Routers and Switches
- 12 Boundary Defense
- 13 Data Protection
- 14 Controlled Access Based on the Need to Know
- 15 Wireless Access Control
- 16 Account Monitoring and Control

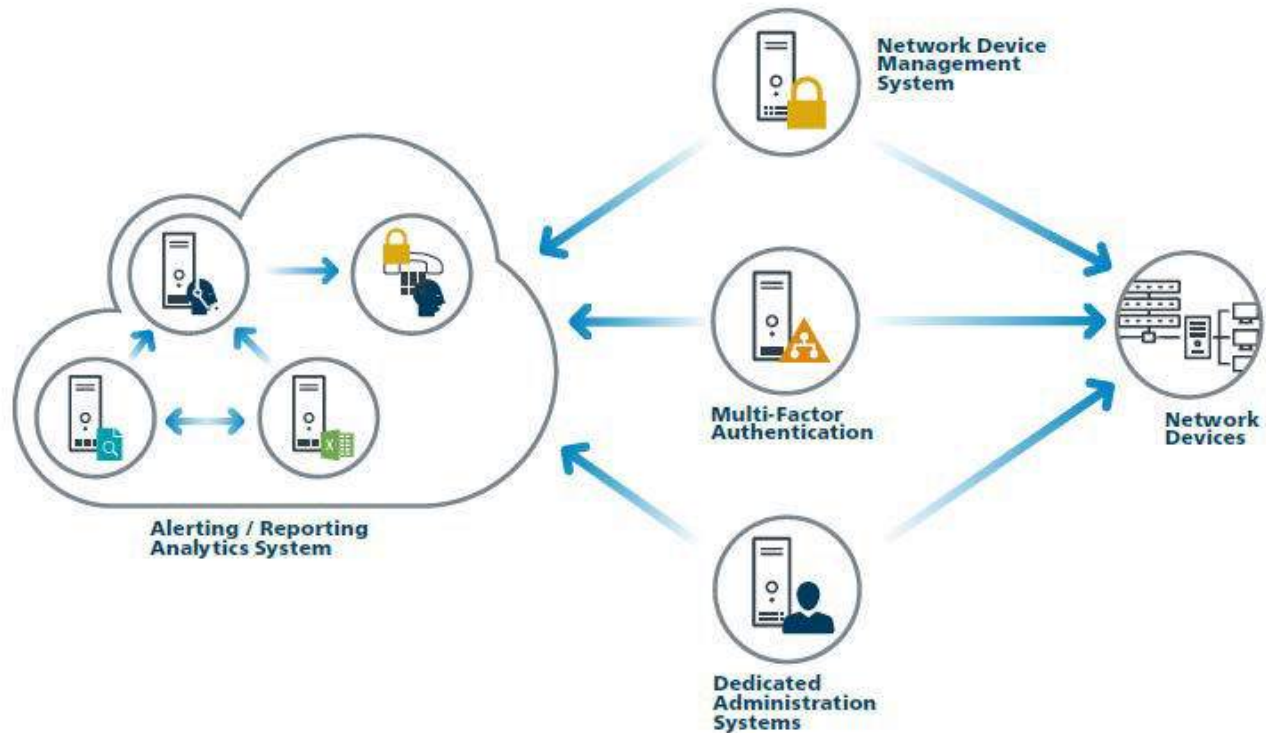
Organizational

- 17 Implement a Security Awareness and Training Program
- 18 Application Software Security
- 19 Incident Response and Management
- 20 Penetration Tests and Red Team Exercises

<https://www.cisecurity.org/controls/>

CIS CONTROL 11: SECURE CONFIG FOR NETWORK DEVICES-II

CIS Control 11: System Entity Relationship Diagram



<https://www.cisecurity.org/controls/>

CIS CONTROL 11: SECURE CONFIG FOR NETWORK DEVICES

11.5: Manage Network Devices Using Multi-Factor Authentication and Encrypted Sessions

- Manage all network devices using multi-factor authentication and encrypted sessions.

CIS CONTROL 11: SECURE CONFIG FOR NETWORK DEVICES

11.6: Use Dedicated Machines For All Network Administrative Tasks

- Ensure network engineers use a dedicated machine for all administrative tasks or tasks requiring elevated access. This machine shall be segmented from the...

CIS CONTROL 11: SECURE CONFIG FOR NETWORK DEVICES

11.6: Use Dedicated Machines For All Network Administrative Tasks

- ...organization's primary network and not be allowed Internet access. This machine shall not be used for reading e-mail, composing documents, or surfing the Internet.

CIS CONTROL 11: SECURE CONFIG FOR NETWORK DEVICES

11.7: Manage Network Infrastructure Through a Dedicated Network

- Manage the network infrastructure across network connections that are separated from the business use of that network, relying on separate VLANs or, preferably, on entirely different physical...

CIS CONTROL 11: SECURE CONFIG FOR NETWORK DEVICES

11.7: Manage Network Infrastructure Through a Dedicated Network

- ... connectivity for management sessions for network devices.

END

CIS CONTROL 12: BOUNDARY DEFENSE - I

- **BOUNDARY DEFENSE**

CIS CONTROL 12: BOUNDARY DEFENSE - I



V7

Basic

- 1 Inventory and Control of Hardware Assets
- 2 Inventory and Control of Software Assets
- 3 Continuous Vulnerability Management
- 4 Controlled Use of Administrative Privileges
- 5 Secure Configuration for Hardware and Software on Mobile Devices, Laptops, Workstations and Servers
- 6 Maintenance, Monitoring and Analysis of Audit Logs

Foundational

- 7 Email and Web Browser Protections
- 8 Malware Defenses
- 9 Limitation and Control of Network Ports, Protocols, and Services
- 10 Data Recovery Capabilities
- 11 Secure Configuration for Network Devices, such as Firewalls, Routers and Switches
- 12 Boundary Defense
- 13 Data Protection
- 14 Controlled Access Based on the Need to Know
- 15 Wireless Access Control
- 16 Account Monitoring and Control

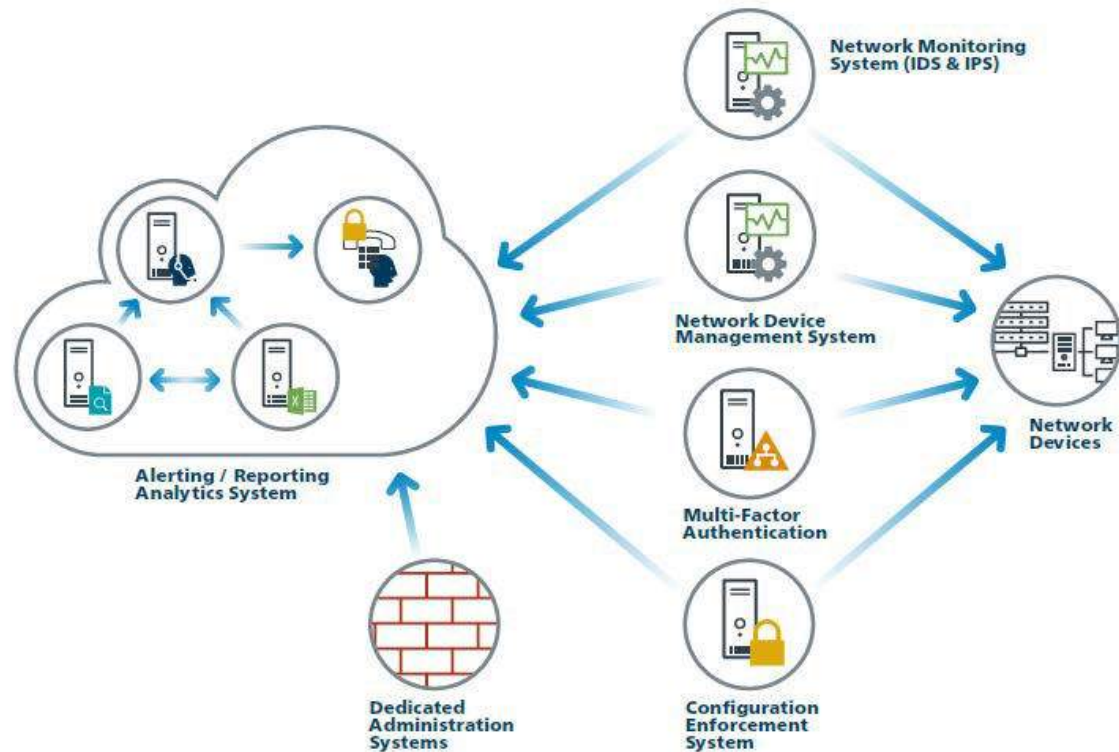
Organizational

- 17 Implement a Security Awareness and Training Program
- 18 Application Software Security
- 19 Incident Response and Management
- 20 Penetration Tests and Red Team Exercises

<https://www.cisecurity.org/controls/>

CIS CONTROL 12: BOUNDARY DEFENSE - I

CIS Control 12: System Entity Relationship Diagram



<https://www.cisecurity.org/controls/>

CIS CONTROL 12: BOUNDARY DEFENSE - I

12.1: Maintain an Inventory of Network Boundaries

- Maintain an up-to-date inventory of all of the organization's network boundaries.

CIS CONTROL 12: BOUNDARY DEFENSE - I

12.2: Scan for Unauthorized Connections across Trusted Network Boundaries

- Perform regular scans from outside each trusted network boundary to detect any unauthorized connections which are accessible across the boundary.

CIS CONTROL 12: BOUNDARY DEFENSE - I

12.3: Deny Communications with Known Malicious IP Addresses

- Deny communications with known malicious or unused Internet IP addresses and limit access only to trusted and necessary IP address ranges at each...

CIS CONTROL 12: BOUNDARY DEFENSE - I

12.3: Deny Communications with Known Malicious IP Addresses

- ...of the organization's network boundaries.

CIS CONTROL 12: BOUNDARY DEFENSE - I

12.4: Deny Communication over Unauthorized Ports

- Deny communication over unauthorized TCP or UDP ports or application traffic to ensure that only authorized protocols are allowed to cross the network boundary in or out of the network at...

CIS CONTROL 12: BOUNDARY DEFENSE - I

12.4: Deny Communication over Unauthorized Ports

- ...each of the organization's network boundaries.

END

CIS CONTROL 12: BOUNDARY DEFENSE - II

- **BOUNDARY DEFENSE**

CIS CONTROL 12: BOUNDARY DEFENSE - II



V7

Basic

- 1 Inventory and Control of Hardware Assets
- 2 Inventory and Control of Software Assets
- 3 Continuous Vulnerability Management
- 4 Controlled Use of Administrative Privileges
- 5 Secure Configuration for Hardware and Software on Mobile Devices, Laptops, Workstations and Servers
- 6 Maintenance, Monitoring and Analysis of Audit Logs

Foundational

- 7 Email and Web Browser Protections
- 8 Malware Defenses
- 9 Limitation and Control of Network Ports, Protocols, and Services
- 10 Data Recovery Capabilities
- 11 Secure Configuration for Network Devices, such as Firewalls, Routers and Switches
- 12 Boundary Defense
- 13 Data Protection
- 14 Controlled Access Based on the Need to Know
- 15 Wireless Access Control
- 16 Account Monitoring and Control

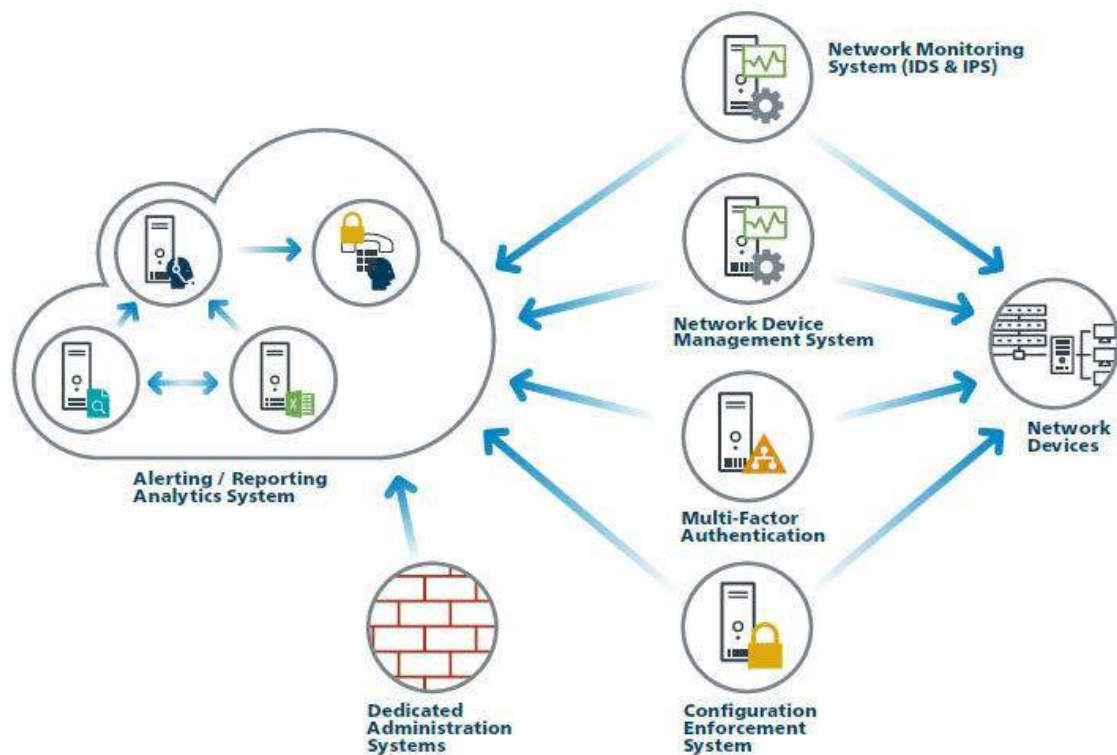
Organizational

- 17 Implement a Security Awareness and Training Program
- 18 Application Software Security
- 19 Incident Response and Management
- 20 Penetration Tests and Red Team Exercises

<https://www.cisecurity.org/controls/>

CIS CONTROL 12: BOUNDARY DEFENSE - II

CIS Control 12: System Entity Relationship Diagram



<https://www.cisecurity.org/controls/>

CIS CONTROL 12: BOUNDARY DEFENSE - II

12.5: Configure Monitoring Systems to Record Network Packets

- Configure monitoring systems to record network packets passing through the boundary at each of the organization's network boundaries.

CIS CONTROL 12: BOUNDARY DEFENSE - II

12.6: Deploy Network-based IDS Sensor

- Deploy network-based Intrusion Detection Systems (IDS) sensors to look for unusual attack mechanisms and detect compromise of these systems at each of the organization's network boundaries.

CIS CONTROL 12: BOUNDARY DEFENSE - II

12.7: Deploy Network-Based Intrusion Prevention Systems

- Deploy network-based Intrusion Prevention Systems (IPS) to block malicious network traffic at each of the organization's network boundaries.

CIS CONTROL 12: BOUNDARY DEFENSE - II

12.8: Deploy NetFlow Collection on Networking Boundary Devices

- Enable the collection of NetFlow and logging data on all network boundary devices.

END

CIS CONTROL 12: BOUNDARY DEFENSE - III

- **BOUNDARY DEFENSE**

CIS CONTROL 12: BOUNDARY DEFENSE - III



V7

Basic

- 1 Inventory and Control of Hardware Assets
- 2 Inventory and Control of Software Assets
- 3 Continuous Vulnerability Management
- 4 Controlled Use of Administrative Privileges
- 5 Secure Configuration for Hardware and Software on Mobile Devices, Laptops, Workstations and Servers
- 6 Maintenance, Monitoring and Analysis of Audit Logs

Foundational

- 7 Email and Web Browser Protections
- 8 Malware Defenses
- 9 Limitation and Control of Network Ports, Protocols, and Services
- 10 Data Recovery Capabilities
- 11 Secure Configuration for Network Devices, such as Firewalls, Routers and Switches
- 12 Boundary Defense
- 13 Data Protection
- 14 Controlled Access Based on the Need to Know
- 15 Wireless Access Control
- 16 Account Monitoring and Control

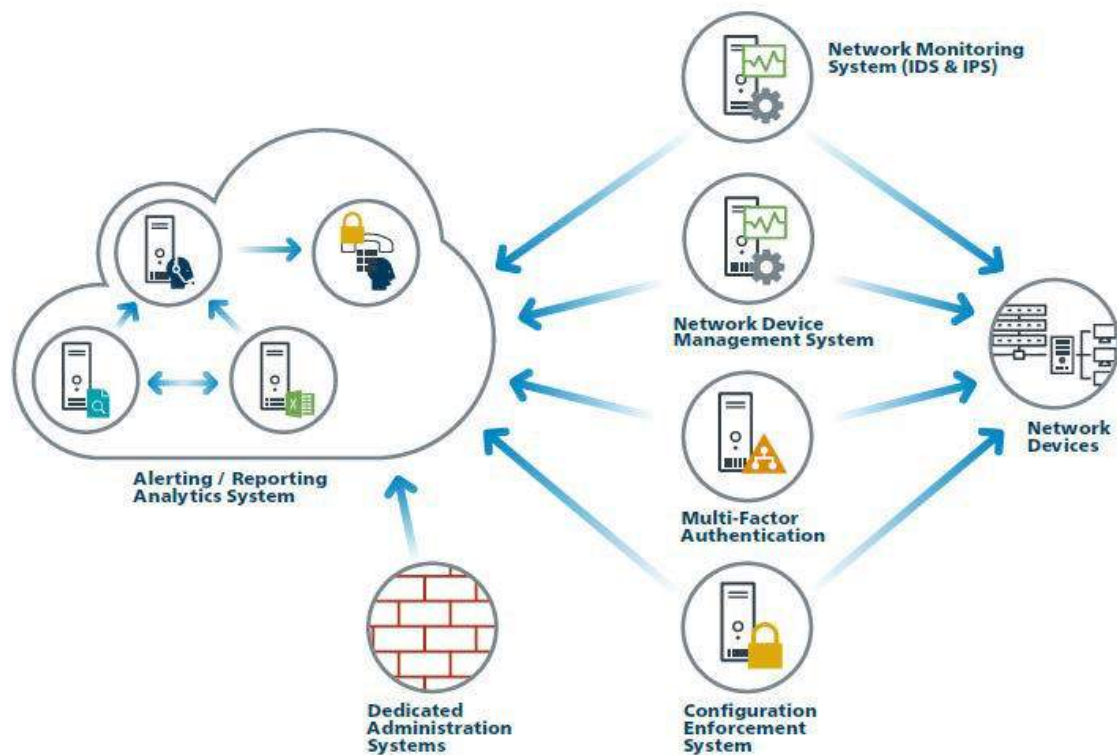
Organizational

- 17 Implement a Security Awareness and Training Program
- 18 Application Software Security
- 19 Incident Response and Management
- 20 Penetration Tests and Red Team Exercises

<https://www.cisecurity.org/controls/>

CIS CONTROL 12: BOUNDARY DEFENSE - III

CIS Control 12: System Entity Relationship Diagram



<https://www.cisecurity.org/controls/>

CIS CONTROL 12: BOUNDARY DEFENSE - III

12.9: Deploy Application Layer Filtering Proxy Server

- Ensure that all network traffic to or from the Internet passes through an authenticated application layer proxy that is configured to filter unauthorized connections.

CIS CONTROL 12: BOUNDARY DEFENSE - III

12.10: Decrypt Network Traffic at Proxy

- Decrypt all encrypted network traffic at the boundary proxy prior to analyzing the content. However, the organization may use whitelists of allowed sites that can be...

CIS CONTROL 12: BOUNDARY DEFENSE - III

12.10: Decrypt Network Traffic at Proxy

- ...accessed through the proxy without decrypting the traffic.

CIS CONTROL 12: BOUNDARY DEFENSE - III

12.11: Require All Remote Login to Use Multi-factor Authentication

- Require all remote login access to the organization's network to encrypt data in transit and use multi-factor authentication..

CIS CONTROL 12: BOUNDARY DEFENSE - III

12.12: Manage All Devices Remotely Logging into Internal Network

- Scan all enterprise devices remotely logging into the organization's network prior to accessing the network to ensure that each of the organization's security...

CIS CONTROL 12: BOUNDARY DEFENSE - III

12.12: Manage All Devices Remotely Logging into Internal Network

- ... policies has been enforced in the same manner as local network devices.

END

CIS CONTROL 13: DATA PROTECTION-I

- DATA PROTECTION

CIS CONTROL 13: DATA PROTECTION-I



V7

Basic

- 1 Inventory and Control of Hardware Assets
- 2 Inventory and Control of Software Assets
- 3 Continuous Vulnerability Management
- 4 Controlled Use of Administrative Privileges
- 5 Secure Configuration for Hardware and Software on Mobile Devices, Laptops, Workstations and Servers
- 6 Maintenance, Monitoring and Analysis of Audit Logs

Foundational

- 7 Email and Web Browser Protections
- 8 Malware Defenses
- 9 Limitation and Control of Network Ports, Protocols, and Services
- 10 Data Recovery Capabilities
- 11 Secure Configuration for Network Devices, such as Firewalls, Routers and Switches
- 12 Boundary Defense
- 13 Data Protection
- 14 Controlled Access Based on the Need to Know
- 15 Wireless Access Control
- 16 Account Monitoring and Control

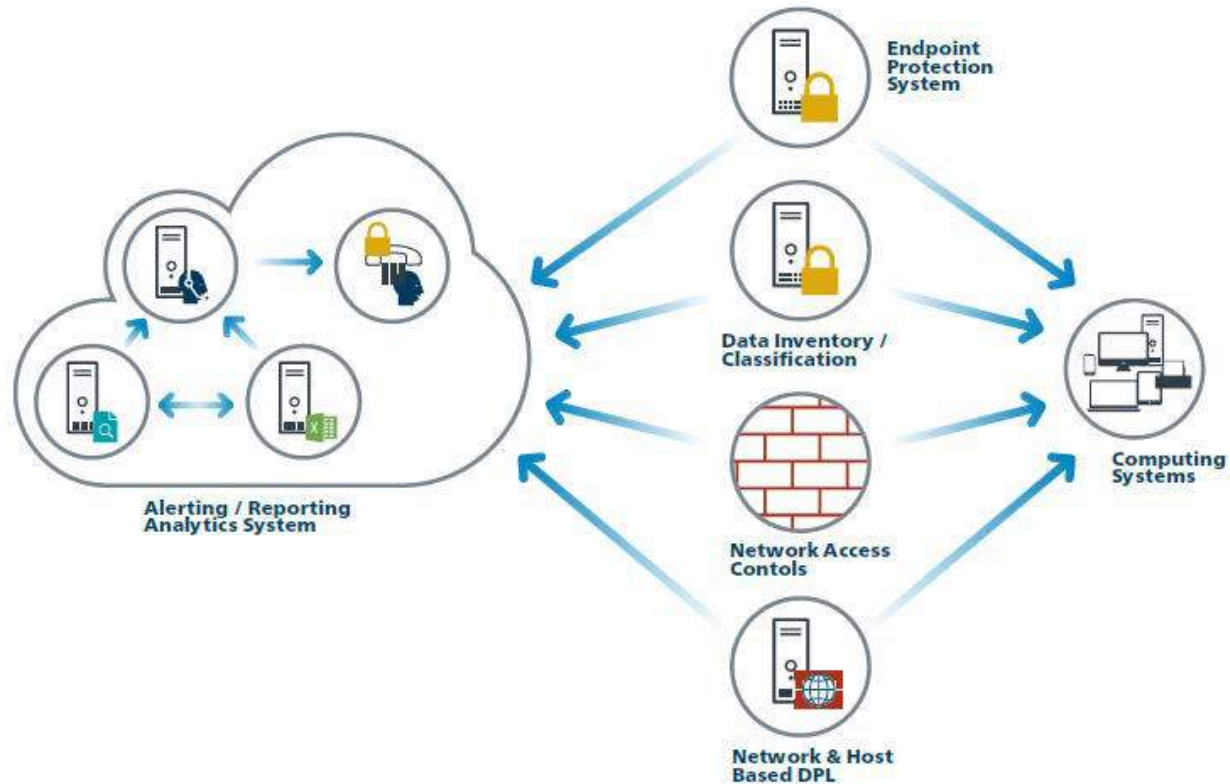
Organizational

- 17 Implement a Security Awareness and Training Program
- 18 Application Software Security
- 19 Incident Response and Management
- 20 Penetration Tests and Red Team Exercises

<https://www.cisecurity.org/controls/>

CIS CONTROL 13: DATA PROTECTION-I

CIS Control 13: System Entity Relationship Diagram



<https://www.cisecurity.org/controls/>

CIS CONTROL 13: DATA PROTECTION-I

13.1: Maintain an Inventory of Sensitive Information

- Maintain an inventory of all sensitive information stored, processed, or transmitted by the organization's technology systems, including those located onsite or at a remote service provider.

CIS CONTROL 13: DATA PROTECTION-I

13.2: Remove Sensitive Data or Systems Not Regularly Accessed by Organization

- Remove sensitive data or systems not regularly accessed by the organization from the network. These systems shall only be used as stand alone systems...

CIS CONTROL 13: DATA PROTECTION-I

13.2: Remove Sensitive Data or Systems Not Regularly Accessed by Organization

- ... (disconnected from the network) by the business unit needing to occasionally use the system or completely virtualized and powered off until needed.

CIS CONTROL 13: DATA PROTECTION-I

13.3: Monitor and Block Unauthorized Network Traffic

- Deploy an automated tool on network perimeters that monitors for unauthorized transfer of sensitive information and blocks such transfers while alerting...

CIS CONTROL 13: DATA PROTECTION-I

13.3: Monitor and Block Unauthorized Network Traffic

- ...information security professionals.

END

CIS CONTROL 13: DATA PROTECTION-II

- DATA PROTECTION

CIS CONTROL 13: DATA PROTECTION-II



V7

Basic

- 1 Inventory and Control of Hardware Assets
- 2 Inventory and Control of Software Assets
- 3 Continuous Vulnerability Management
- 4 Controlled Use of Administrative Privileges
- 5 Secure Configuration for Hardware and Software on Mobile Devices, Laptops, Workstations and Servers
- 6 Maintenance, Monitoring and Analysis of Audit Logs

Foundational

- 7 Email and Web Browser Protections
- 8 Malware Defenses
- 9 Limitation and Control of Network Ports, Protocols, and Services
- 10 Data Recovery Capabilities
- 11 Secure Configuration for Network Devices, such as Firewalls, Routers and Switches
- 12 Boundary Defense
- 13 Data Protection
- 14 Controlled Access Based on the Need to Know
- 15 Wireless Access Control
- 16 Account Monitoring and Control

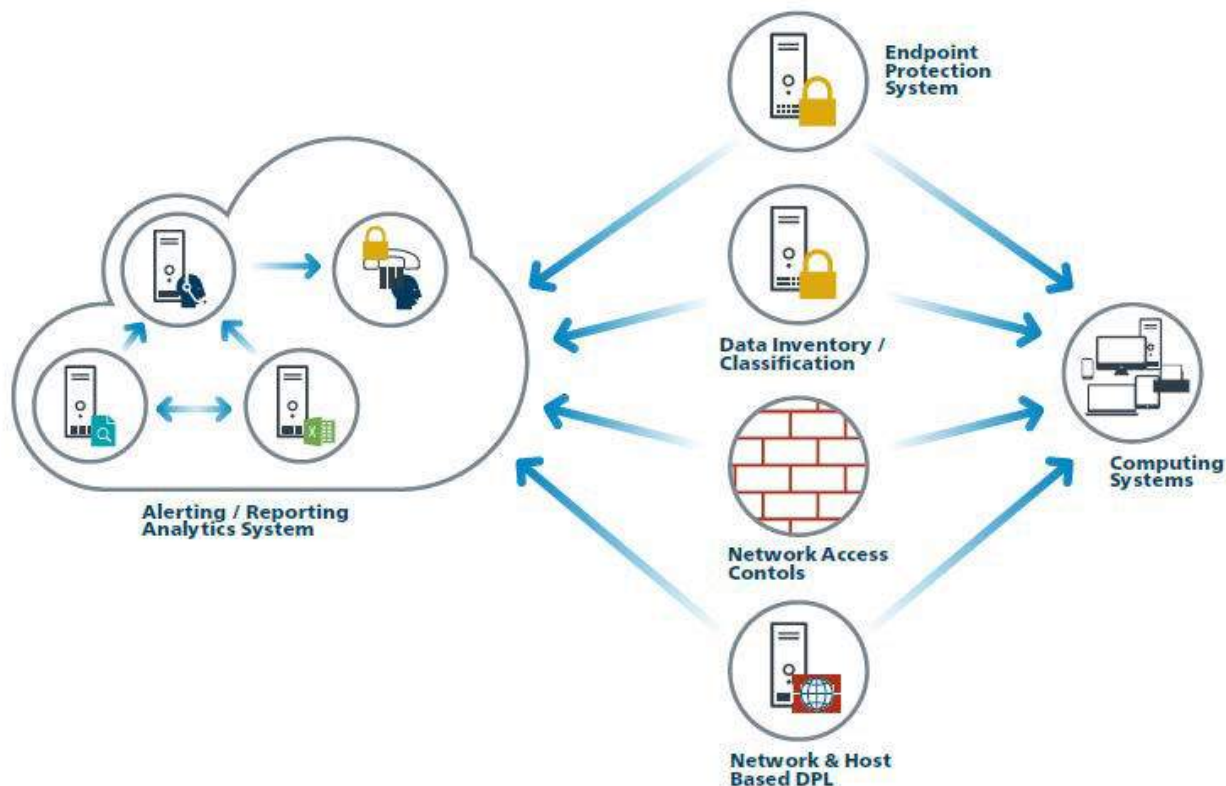
Organizational

- 17 Implement a Security Awareness and Training Program
- 18 Application Software Security
- 19 Incident Response and Management
- 20 Penetration Tests and Red Team Exercises

<https://www.cisecurity.org/controls/>

CIS CONTROL 13: DATA PROTECTION-II

CIS Control 13: System Entity Relationship Diagram



<https://www.cisecurity.org/controls/>

CIS CONTROL 13: DATA PROTECTION-II

13.4: Only Allow Access to Authorized Cloud Storage or Email Providers

- Only allow access to authorized cloud storage or email providers.

CIS CONTROL 13: DATA PROTECTION-II

13.5: Monitor and Detect Any Unauthorized Use of Encryption

- Monitor all traffic leaving the organization and detect any unauthorized use of encryption.

CIS CONTROL 13: DATA PROTECTION-II

13.6: Encrypt the Hard Drive of All Mobile Devices.

- Utilize approved whole disk encryption software to encrypt the hard drive of all mobile devices.

END

CIS CONTROL 13: DATA PROTECTION-III

- DATA PROTECTION

CIS CONTROL 13: DATA PROTECTION-III



V7

Basic

- 1 Inventory and Control of Hardware Assets
- 2 Inventory and Control of Software Assets
- 3 Continuous Vulnerability Management
- 4 Controlled Use of Administrative Privileges
- 5 Secure Configuration for Hardware and Software on Mobile Devices, Laptops, Workstations and Servers
- 6 Maintenance, Monitoring and Analysis of Audit Logs

Foundational

- 7 Email and Web Browser Protections
- 8 Malware Defenses
- 9 Limitation and Control of Network Ports, Protocols, and Services
- 10 Data Recovery Capabilities
- 11 Secure Configuration for Network Devices, such as Firewalls, Routers and Switches
- 12 Boundary Defense
- 13 Data Protection
- 14 Controlled Access Based on the Need to Know
- 15 Wireless Access Control
- 16 Account Monitoring and Control

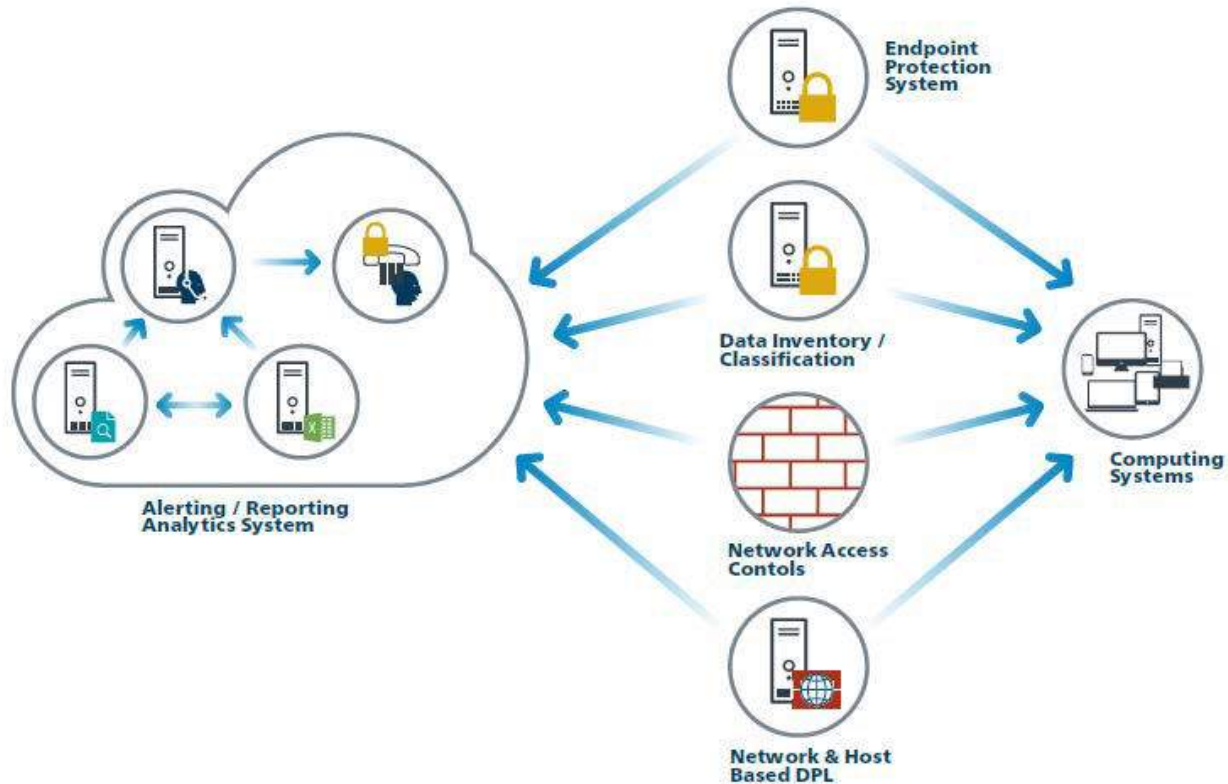
Organizational

- 17 Implement a Security Awareness and Training Program
- 18 Application Software Security
- 19 Incident Response and Management
- 20 Penetration Tests and Red Team Exercises

<https://www.cisecurity.org/controls/>

CIS CONTROL 13: DATA PROTECTION-III

CIS Control 13: System Entity Relationship Diagram



<https://www.cisecurity.org/controls/>

CIS CONTROL 13: DATA PROTECTION-III

13.7: Manage USB Devices

- If USB storage devices are required, enterprise software should be used that can configure systems to allow the use of specific devices. An inventory of such devices should be maintained.

CIS CONTROL 13: DATA PROTECTION-III

13.8: Manage System's External Removable Media's Read/write Configurations

- Configure systems not to write data to external removable media, if there is no business need for supporting such devices.

CIS CONTROL 13: DATA PROTECTION-III

13.9: Encrypt Data on USB Storage Devices

- If USB storage devices are required, all data stored on such devices must be encrypted while at rest.

END

CIS CONTROL 14: CONTROLLED ACCESS-NEED TO KNOW-I

- **CONTROLLED ACCESS
BASED ON THE NEED TO
KNOW**

CIS CONTROL 14: CONTROLLED ACCESS-NEED TO KNOW-I



V7

Basic

- 1 Inventory and Control of Hardware Assets
- 2 Inventory and Control of Software Assets
- 3 Continuous Vulnerability Management
- 4 Controlled Use of Administrative Privileges
- 5 Secure Configuration for Hardware and Software on Mobile Devices, Laptops, Workstations and Servers
- 6 Maintenance, Monitoring and Analysis of Audit Logs

Foundational

- 7 Email and Web Browser Protections
- 8 Malware Defenses
- 9 Limitation and Control of Network Ports, Protocols, and Services
- 10 Data Recovery Capabilities
- 11 Secure Configuration for Network Devices, such as Firewalls, Routers and Switches
- 12 Boundary Defense
- 13 Data Protection
- 14 Controlled Access Based on the Need to Know
- 15 Wireless Access Control
- 16 Account Monitoring and Control

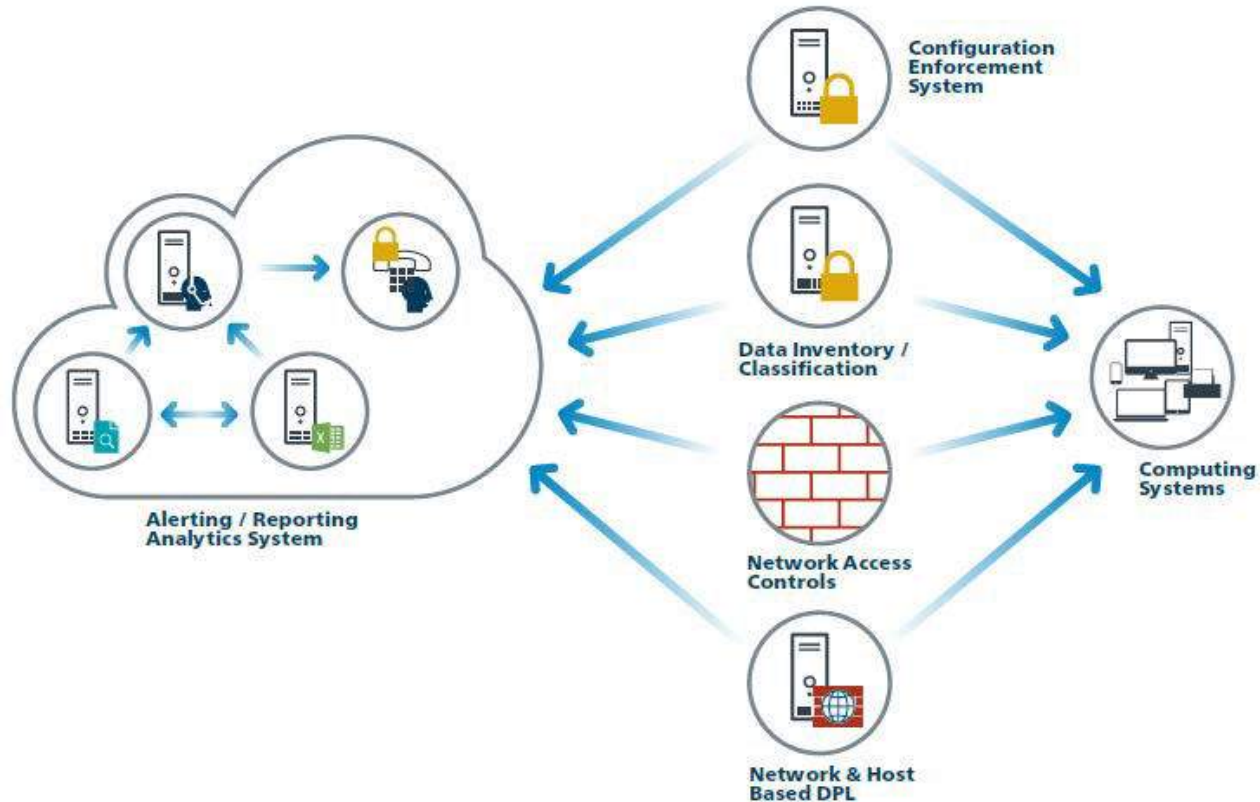
Organizational

- 17 Implement a Security Awareness and Training Program
- 18 Application Software Security
- 19 Incident Response and Management
- 20 Penetration Tests and Red Team Exercises

<https://www.cisecurity.org/controls/>

CIS CONTROL 14: CONTROLLED ACCESS-NEED TO KNOW-I

CIS Control 14: System Entity Relationship Diagram



<https://www.cisecurity.org/controls/>

CIS CONTROL 14: CONTROLLED ACCESS-NEED TO KNOW-I

14.1: Segment the Network Based on Sensitivity

- Segment the network based on the label or classification level of the information stored on the servers, locate all sensitive information on separated Virtual Local Area Networks (VLANs).

CIS CONTROL 14: CONTROLLED ACCESS-NEED TO KNOW-I

14.2: Enable Firewall Filtering Between VLANs

- Enable firewall filtering between VLANs to ensure that only authorized systems are able to communicate with other systems necessary to fulfill their specific responsibilities.

CIS CONTROL 14: CONTROLLED ACCESS-NEED TO KNOW-I

14.3: Disable Workstation to Workstation Communication

- Disable all workstation to workstation communication to limit an attacker's ability to move laterally and compromise neighboring systems, ...

CIS CONTROL 14: CONTROLLED ACCESS-NEED TO KNOW-I

14.3: Disable Workstation to Workstation Communication

- ...through technologies such as Private VLANs or microsegmentation.

CIS CONTROL 14: CONTROLLED ACCESS-NEED TO KNOW-I

14.4: Encrypt All Sensitive Information in Transit

- Encrypt all sensitive information in transit.

CIS CONTROL 14: CONTROLLED ACCESS-NEED TO KNOW-I

14.5: Utilize an Active Discovery Tool to Identify Sensitive Data

- Utilize an active discovery tool to identify all sensitive information stored, processed, or transmitted by the organization's technology systems, including those located...

CIS CONTROL 14: CONTROLLED ACCESS-NEED TO KNOW-I

14.5: Utilize an Active Discovery Tool to Identify Sensitive Data

- ... onsite or at a remote service provider and update the organization's sensitive information inventory.

END

CIS CONTROL 14: CONTROLLED ACCESS-NEED TO KNOW-II

- **CONTROLLED ACCESS
BASED ON THE NEED TO
KNOW**

CIS CONTROL 14: CONTROLLED ACCESS-NEED TO KNOW-II



V7

Basic

- 1 Inventory and Control of Hardware Assets
- 2 Inventory and Control of Software Assets
- 3 Continuous Vulnerability Management
- 4 Controlled Use of Administrative Privileges
- 5 Secure Configuration for Hardware and Software on Mobile Devices, Laptops, Workstations and Servers
- 6 Maintenance, Monitoring and Analysis of Audit Logs

Foundational

- 7 Email and Web Browser Protections
- 8 Malware Defenses
- 9 Limitation and Control of Network Ports, Protocols, and Services
- 10 Data Recovery Capabilities
- 11 Secure Configuration for Network Devices, such as Firewalls, Routers and Switches
- 12 Boundary Defense
- 13 Data Protection
- 14 Controlled Access Based on the Need to Know
- 15 Wireless Access Control
- 16 Account Monitoring and Control

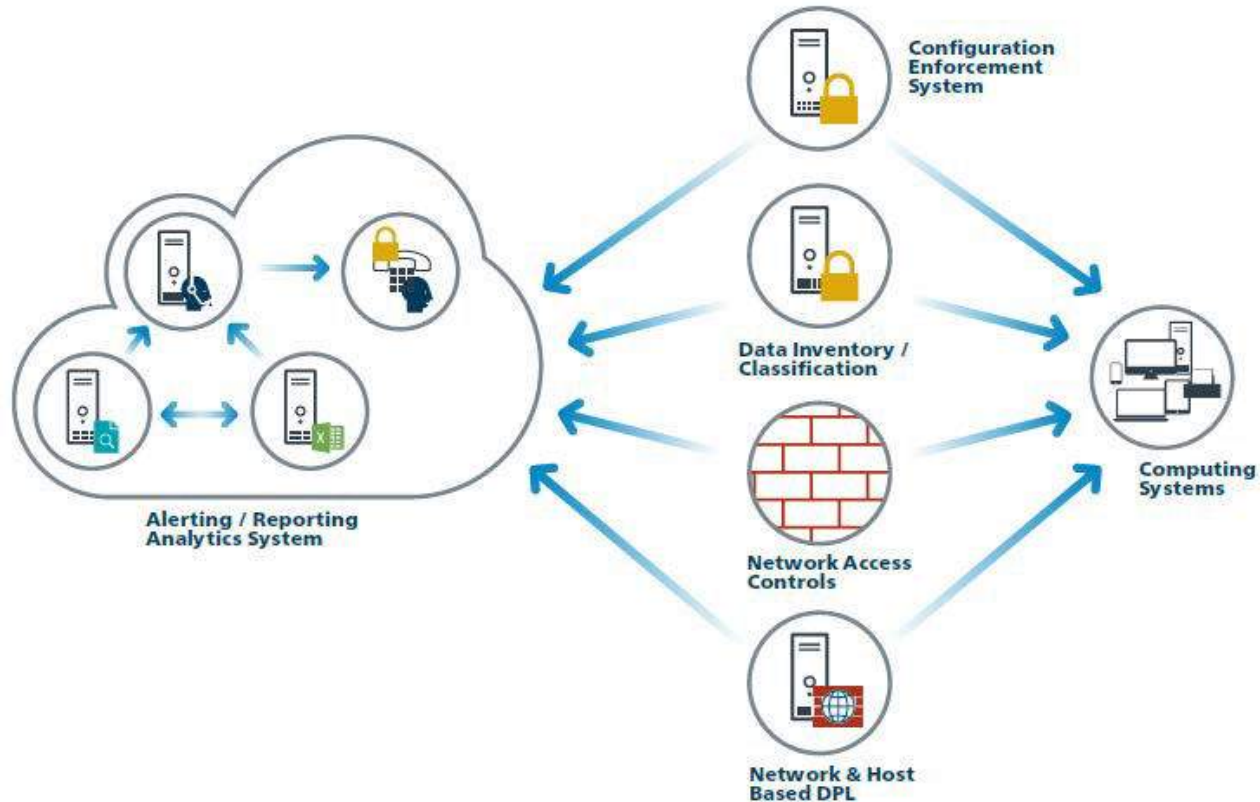
Organizational

- 17 Implement a Security Awareness and Training Program
- 18 Application Software Security
- 19 Incident Response and Management
- 20 Penetration Tests and Red Team Exercises

<https://www.cisecurity.org/controls/>

CIS CONTROL 14: CONTROLLED ACCESS-NEED TO KNOW-II

CIS Control 14: System Entity Relationship Diagram



<https://www.cisecurity.org/controls/>

CIS CONTROL 14: CONTROLLED ACCESS-NEED TO KNOW-II

14.6: Protect Information through Access Control Lists

- Protect all information stored on systems with file system, network share, claims, application, or database specific access control lists. These controls will...

CIS CONTROL 14: CONTROLLED ACCESS-NEED TO KNOW-II

14.6: Protect Information through Access Control Lists

- ...enforce the principle that only authorized individuals should have access to the information based on their need to access the information as a part of their responsibilities.

CIS CONTROL 14: CONTROLLED ACCESS-NEED TO KNOW-II

14.7: Enforce Access Control to Data through Automated Tools

- Use an automated tool, such as host-based Data Loss Prevention, to enforce access controls to data even when data is copied off a system.

14.8: Encrypt Sensitive Information at Rest

- Encrypt all sensitive information at rest using a tool that requires a secondary authentication mechanism not integrated into the operating system, in order to access the information.

CIS CONTROL 14: CONTROLLED ACCESS-NEED TO KNOW-II

14.9: Enforce Detail Logging for Access or Changes to Sensitive Data

- Enforce detailed audit logging for access to sensitive data or changes to sensitive data (utilizing tools such as File Integrity Monitoring or Security Information and Event Monitoring).

END

CIS CONTROL 15: WIRELESS ACCESS CONTROL-I

- **WIRELESS ACCESS CONTROL**

CIS CONTROL 15: WIRELESS ACCESS CONTROL-I



V7

Basic

- 1 Inventory and Control of Hardware Assets
- 2 Inventory and Control of Software Assets
- 3 Continuous Vulnerability Management
- 4 Controlled Use of Administrative Privileges
- 5 Secure Configuration for Hardware and Software on Mobile Devices, Laptops, Workstations and Servers
- 6 Maintenance, Monitoring and Analysis of Audit Logs

Foundational

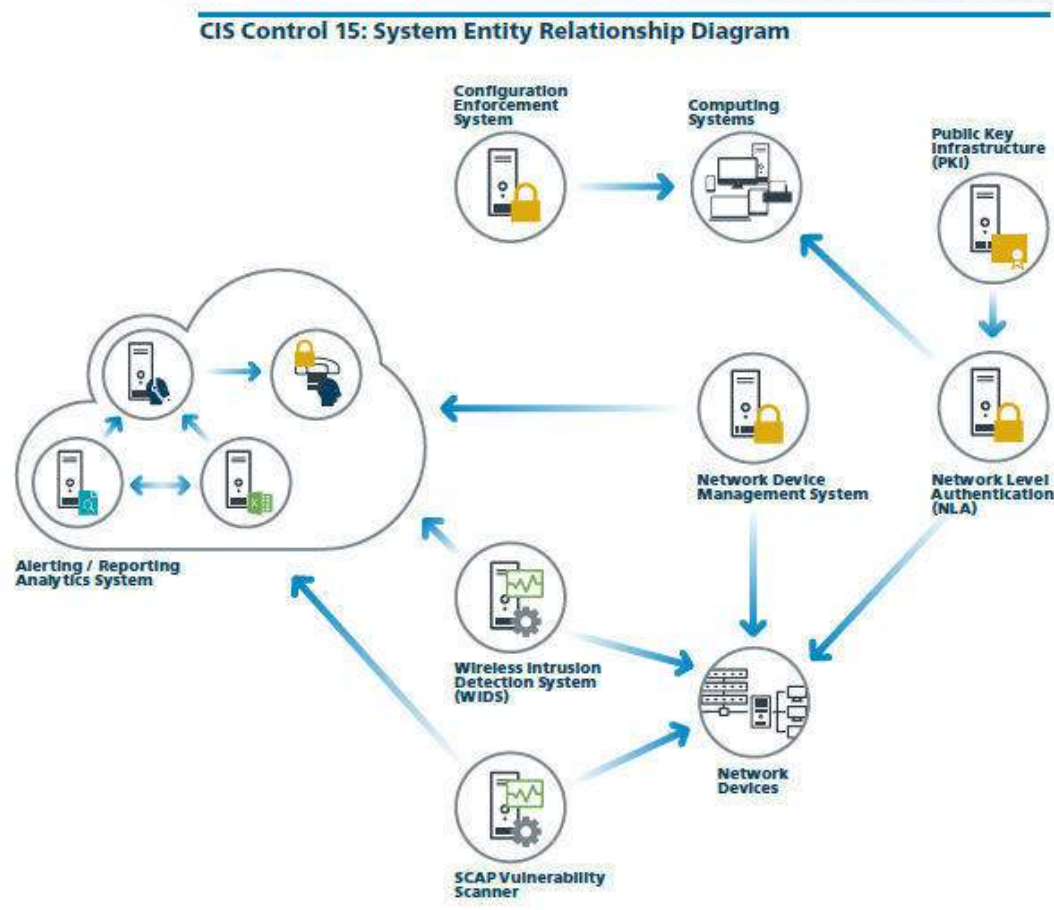
- 7 Email and Web Browser Protections
- 8 Malware Defenses
- 9 Limitation and Control of Network Ports, Protocols, and Services
- 10 Data Recovery Capabilities
- 11 Secure Configuration for Network Devices, such as Firewalls, Routers and Switches
- 12 Boundary Defense
- 13 Data Protection
- 14 Controlled Access Based on the Need to Know
- 15 Wireless Access Control
- 16 Account Monitoring and Control

Organizational

- 17 Implement a Security Awareness and Training Program
- 18 Application Software Security
- 19 Incident Response and Management
- 20 Penetration Tests and Red Team Exercises

<https://www.cisecurity.org/controls/>

CIS CONTROL 15: WIRELESS ACCESS CONTROL-I



<https://www.cisecurity.org/controls/>

CIS CONTROL 15: WIRELESS ACCESS CONTROL-I

15.1: Maintain an Inventory of Authorized Wireless Access Points

- Maintain an inventory of authorized wireless access points connected to the wired network.

CIS CONTROL 15: WIRELESS ACCESS CONTROL-I

15.2: Detect Wireless Access Points Connected to the Wired Network

- Configure network vulnerability scanning tools to detect and alert on unauthorized wireless access points connected to the wired network.

CIS CONTROL 15: WIRELESS ACCESS CONTROL-I

15.3: Use a Wireless Intrusion Detection System

- Use a wireless intrusion detection system (WIDS) to detect and alert on unauthorized wireless access points connected to the network.

CIS CONTROL 15: WIRELESS ACCESS CONTROL-II

- **WIRELESS ACCESS CONTROL**

CIS CONTROL 15: WIRELESS ACCESS CONTROL-II



V7

Basic

- 1 Inventory and Control of Hardware Assets
- 2 Inventory and Control of Software Assets
- 3 Continuous Vulnerability Management
- 4 Controlled Use of Administrative Privileges
- 5 Secure Configuration for Hardware and Software on Mobile Devices, Laptops, Workstations and Servers
- 6 Maintenance, Monitoring and Analysis of Audit Logs

Foundational

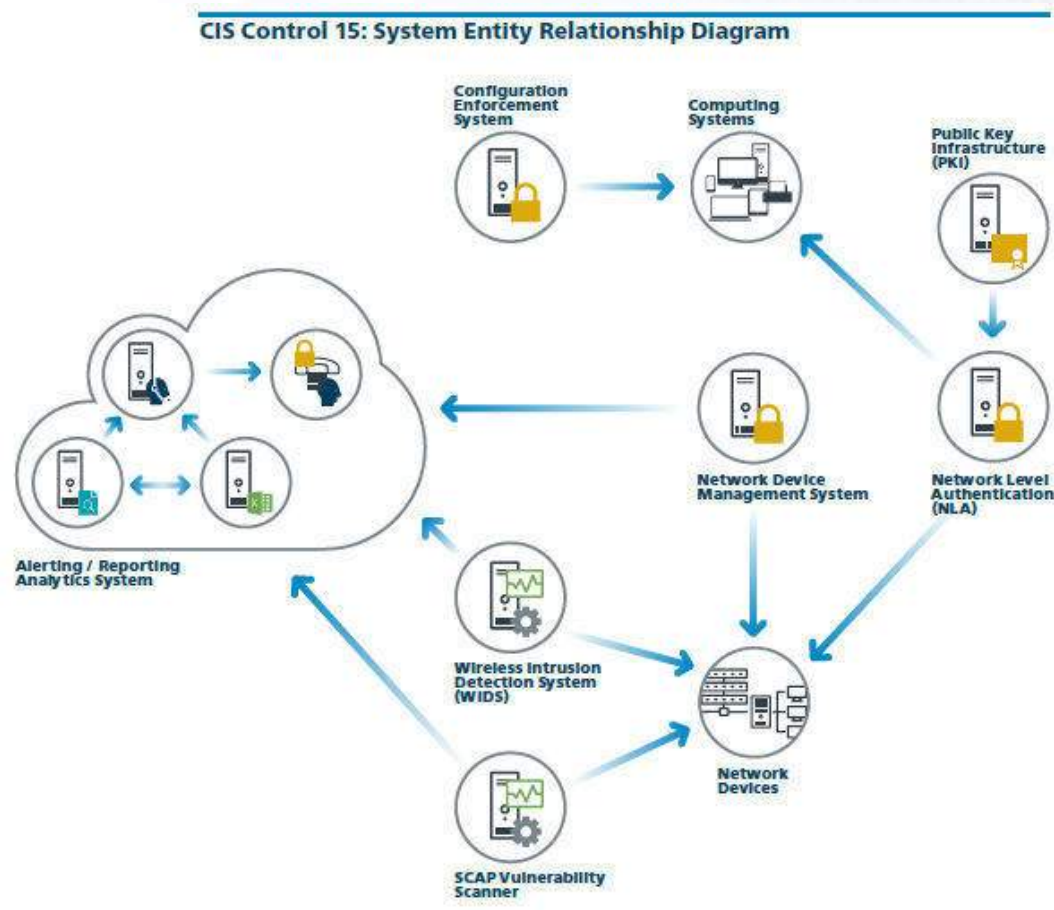
- 7 Email and Web Browser Protections
- 8 Malware Defenses
- 9 Limitation and Control of Network Ports, Protocols, and Services
- 10 Data Recovery Capabilities
- 11 Secure Configuration for Network Devices, such as Firewalls, Routers and Switches
- 12 Boundary Defense
- 13 Data Protection
- 14 Controlled Access Based on the Need to Know
- 15 Wireless Access Control
- 16 Account Monitoring and Control

Organizational

- 17 Implement a Security Awareness and Training Program
- 18 Application Software Security
- 19 Incident Response and Management
- 20 Penetration Tests and Red Team Exercises

<https://www.cisecurity.org/controls/>

CIS CONTROL 15: WIRELESS ACCESS CONTROL-II



<https://www.cisecurity.org/controls/>

CIS CONTROL 15: WIRELESS ACCESS CONTROL-II

15.4: Disable Wireless Access on Devices if Not Required

- Disable wireless access on devices that do not have a business purpose for wireless access.

CIS CONTROL 15: WIRELESS ACCESS CONTROL-II

15.5: Limit Wireless Access on Client Devices

- Configure wireless access on client machines that do have an essential wireless business purpose, to allow access only to authorized wireless networks and to restrict access to other wireless networks.

CIS CONTROL 15: WIRELESS ACCESS CONTROL-II

15.6: Disable Peer-to-peer Wireless Network Capabilities on Wireless Clients

- Disable peer-to-peer (adhoc) wireless network capabilities on wireless clients.

END

CIS CONTROL 15: WIRELESS ACCESS CONTROL-III

- **WIRELESS ACCESS CONTROL**

CIS CONTROL 15: WIRELESS ACCESS CONTROL-III



V7

Basic

- 1 Inventory and Control of Hardware Assets
- 2 Inventory and Control of Software Assets
- 3 Continuous Vulnerability Management
- 4 Controlled Use of Administrative Privileges
- 5 Secure Configuration for Hardware and Software on Mobile Devices, Laptops, Workstations and Servers
- 6 Maintenance, Monitoring and Analysis of Audit Logs

Foundational

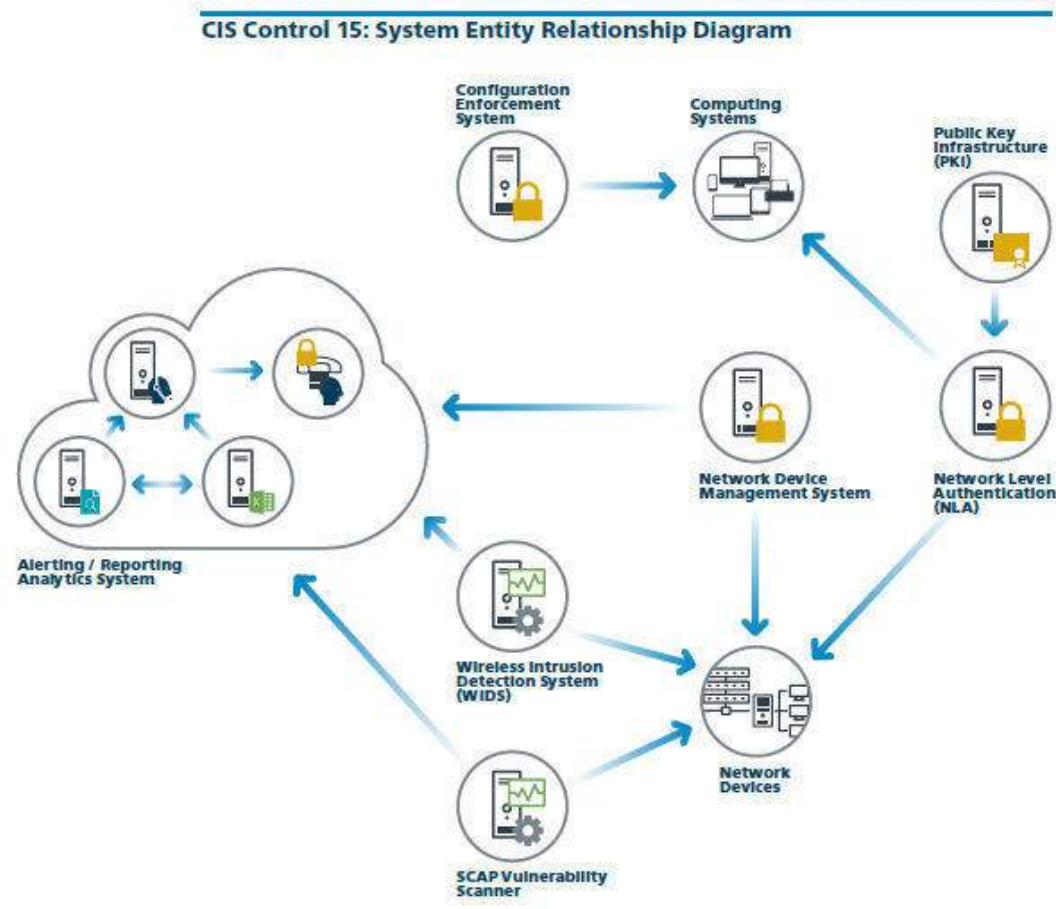
- 7 Email and Web Browser Protections
- 8 Malware Defenses
- 9 Limitation and Control of Network Ports, Protocols, and Services
- 10 Data Recovery Capabilities
- 11 Secure Configuration for Network Devices, such as Firewalls, Routers and Switches
- 12 Boundary Defense
- 13 Data Protection
- 14 Controlled Access Based on the Need to Know
- 15 Wireless Access Control
- 16 Account Monitoring and Control

Organizational

- 17 Implement a Security Awareness and Training Program
- 18 Application Software Security
- 19 Incident Response and Management
- 20 Penetration Tests and Red Team Exercises

<https://www.cisecurity.org/controls/>

CIS CONTROL 15: WIRELESS ACCESS CONTROL-III



<https://www.cisecurity.org/controls/>

CIS CONTROL 15: WIRELESS ACCESS CONTROL-III

15.7: Leverage the Advanced Encryption Standard (AES) to Encrypt Wireless Data

- Leverage the Advanced Encryption Standard (AES) to encrypt wireless data in transit.

CIS CONTROL 15: WIRELESS ACCESS CONTROL-III

15.8: Use Wireless Authentication Protocols that Require Mutual, Multi-Factor Authentication

- Ensure that wireless networks use authentication protocols such as Extensible Authentication Protocol-Transport Layer Security (EAP/TLS), ...

CIS CONTROL 15: WIRELESS ACCESS CONTROL-III

15.8: Use Wireless Authentication Protocols that Require Mutual, Multi-Factor Authentication

- ... that requires mutual, multi-factor authentication.

CIS CONTROL 16: ACCOUNT MONITORING & CONTROL-I

- ACCOUNT MONITORING & CONTROL

CIS CONTROL 16: ACCOUNT MONITORING & CONTROL-I



V7

Basic

- 1 Inventory and Control of Hardware Assets
- 2 Inventory and Control of Software Assets
- 3 Continuous Vulnerability Management
- 4 Controlled Use of Administrative Privileges
- 5 Secure Configuration for Hardware and Software on Mobile Devices, Laptops, Workstations and Servers
- 6 Maintenance, Monitoring and Analysis of Audit Logs

Foundational

- 7 Email and Web Browser Protections
- 8 Malware Defenses
- 9 Limitation and Control of Network Ports, Protocols, and Services
- 10 Data Recovery Capabilities
- 11 Secure Configuration for Network Devices, such as Firewalls, Routers and Switches
- 12 Boundary Defense
- 13 Data Protection
- 14 Controlled Access Based on the Need to Know
- 15 Wireless Access Control
- 16 Account Monitoring and Control

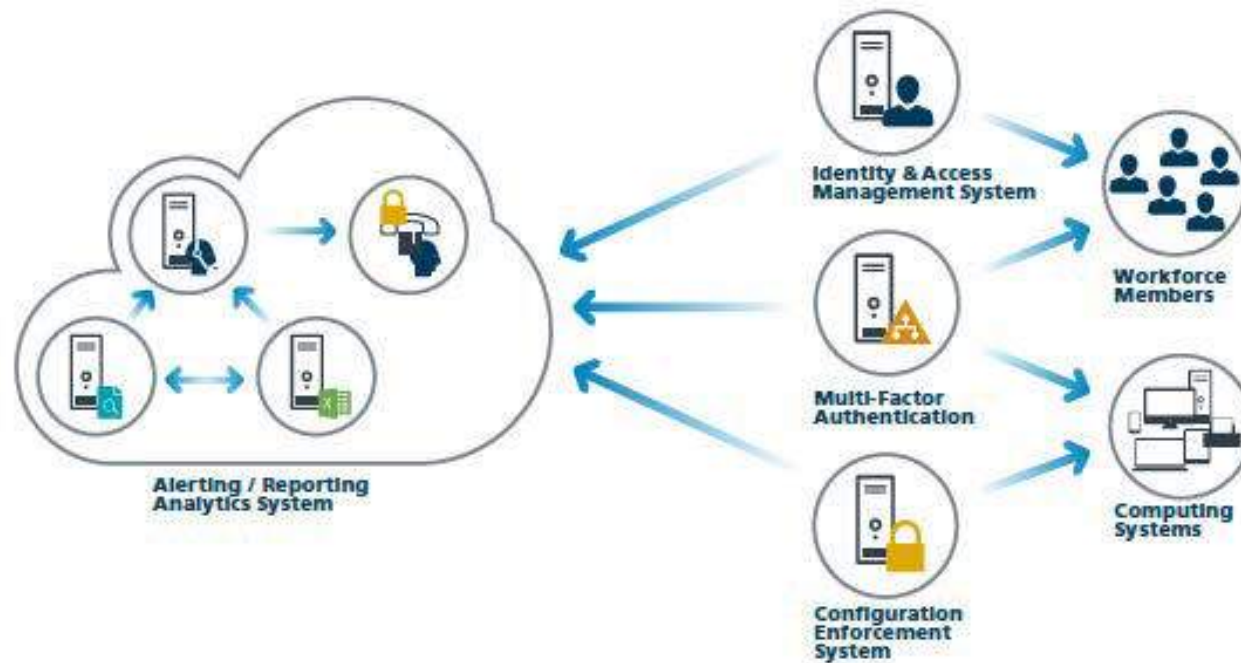
Organizational

- 17 Implement a Security Awareness and Training Program
- 18 Application Software Security
- 19 Incident Response and Management
- 20 Penetration Tests and Red Team Exercises

<https://www.cisecurity.org/controls/>

CIS CONTROL 16: ACCOUNT MONITORING & CONTROL-I

CIS Control 16: System Entity Relationship Diagram



<https://www.cisecurity.org/controls/>

CIS CONTROL 16: ACCOUNT MONITORING & CONTROL-I

16.1: Maintain an Inventory of Authentication Systems

- Maintain an inventory of each of the organization's authentication systems, including those located onsite or at a remote service provider.

CIS CONTROL 16: ACCOUNT MONITORING & CONTROL-I

16.2: Configure Centralized Point of Authentication

- Configure access for all accounts through as few centralized points of authentication as possible, including network, security, and cloud systems.

CIS CONTROL 16: ACCOUNT MONITORING & CONTROL-I

16.3: Require Multi-factor Authentication

Require multi-factor authentication for all user accounts, on all systems, whether managed onsite or by a third-party provider.

CIS CONTROL 16: ACCOUNT MONITORING & CONTROL-I

16.4: Encrypt or Hash all Authentication Credentials

Encrypt or hash with a salt all authentication credentials when stored.

END

CIS CONTROL 16: ACCOUNT MONITORING & CONTROL-II

- **ACCOUNT MONITORING & CONTROL**

CIS CONTROL 16: ACCOUNT MONITORING & CONTROL-II



V7

Basic

- 1 Inventory and Control of Hardware Assets
- 2 Inventory and Control of Software Assets
- 3 Continuous Vulnerability Management
- 4 Controlled Use of Administrative Privileges
- 5 Secure Configuration for Hardware and Software on Mobile Devices, Laptops, Workstations and Servers
- 6 Maintenance, Monitoring and Analysis of Audit Logs

Foundational

- 7 Email and Web Browser Protections
- 8 Malware Defenses
- 9 Limitation and Control of Network Ports, Protocols, and Services
- 10 Data Recovery Capabilities
- 11 Secure Configuration for Network Devices, such as Firewalls, Routers and Switches
- 12 Boundary Defense
- 13 Data Protection
- 14 Controlled Access Based on the Need to Know
- 15 Wireless Access Control
- 16 Account Monitoring and Control

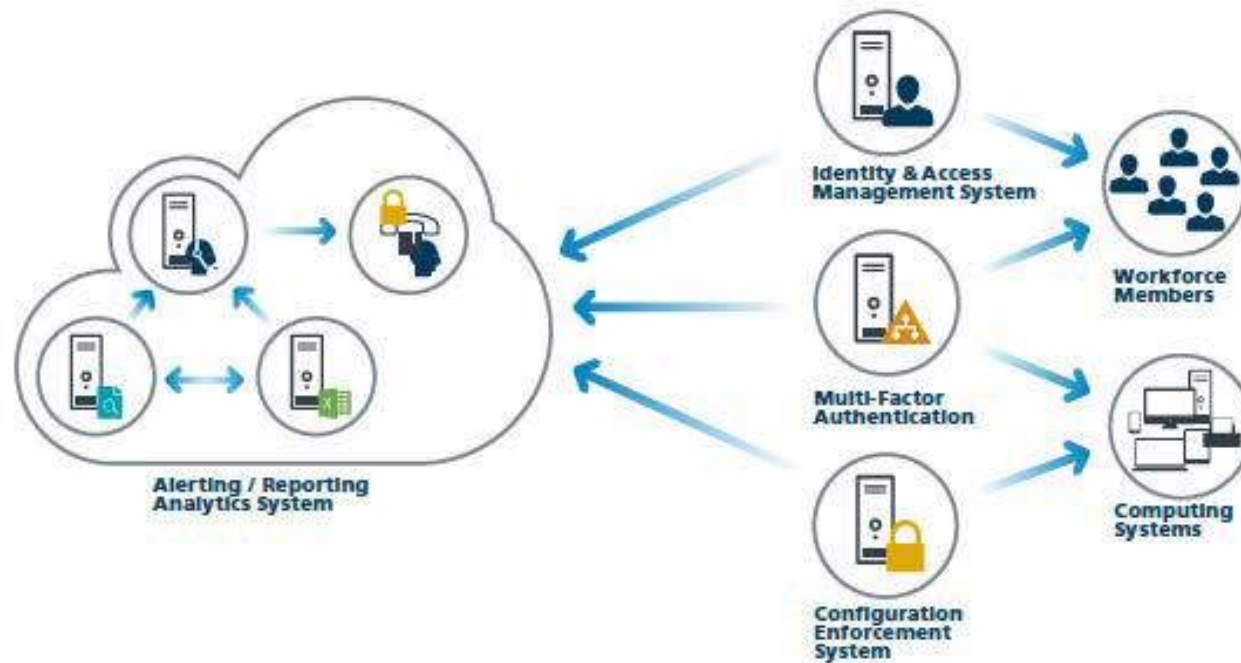
Organizational

- 17 Implement a Security Awareness and Training Program
- 18 Application Software Security
- 19 Incident Response and Management
- 20 Penetration Tests and Red Team Exercises

<https://www.cisecurity.org/controls/>

CIS CONTROL 16: ACCOUNT MONITORING & CONTROL-II

CIS Control 16: System Entity Relationship Diagram



<https://www.cisecurity.org/controls/>

CIS CONTROL 16: ACCOUNT MONITORING & CONTROL-II

16.5: Encrypt Transmittal of Username and Authentication Credentials

- Ensure that all account usernames and authentication credentials are transmitted across networks using encrypted channels.

CIS CONTROL 16: ACCOUNT MONITORING & CONTROL-II

16.6: Maintain an Inventory of Accounts

- Maintain an inventory of all accounts organized by authentication system.

CIS CONTROL 16: ACCOUNT MONITORING & CONTROL-II

16.7: Establish Process for Revoking Access

- Establish and follow an automated process for revoking system access by disabling accounts immediately upon termination or change of responsibilities of an employee or contractor. Disabling these accounts, instead of...

CIS CONTROL 16: ACCOUNT MONITORING & CONTROL-II

16.7: Establish Process for Revoking Access

- ... deleting accounts, allows preservation of audit trails.

CIS CONTROL 16: ACCOUNT MONITORING & CONTROL-II

16.8: Disable Any Unassociated Accounts

- Disable any account that cannot be associated with a business process or business owner.

CIS CONTROL 16: ACCOUNT MONITORING & CONTROL-III

- **ACCOUNT MONITORING & CONTROL**

CIS CONTROL 16: ACCOUNT MONITORING & CONTROL-III



V7

Basic

- 1 Inventory and Control of Hardware Assets
- 2 Inventory and Control of Software Assets
- 3 Continuous Vulnerability Management
- 4 Controlled Use of Administrative Privileges
- 5 Secure Configuration for Hardware and Software on Mobile Devices, Laptops, Workstations and Servers
- 6 Maintenance, Monitoring and Analysis of Audit Logs

Foundational

- 7 Email and Web Browser Protections
- 8 Malware Defenses
- 9 Limitation and Control of Network Ports, Protocols, and Services
- 10 Data Recovery Capabilities
- 11 Secure Configuration for Network Devices, such as Firewalls, Routers and Switches
- 12 Boundary Defense
- 13 Data Protection
- 14 Controlled Access Based on the Need to Know
- 15 Wireless Access Control
- 16 Account Monitoring and Control

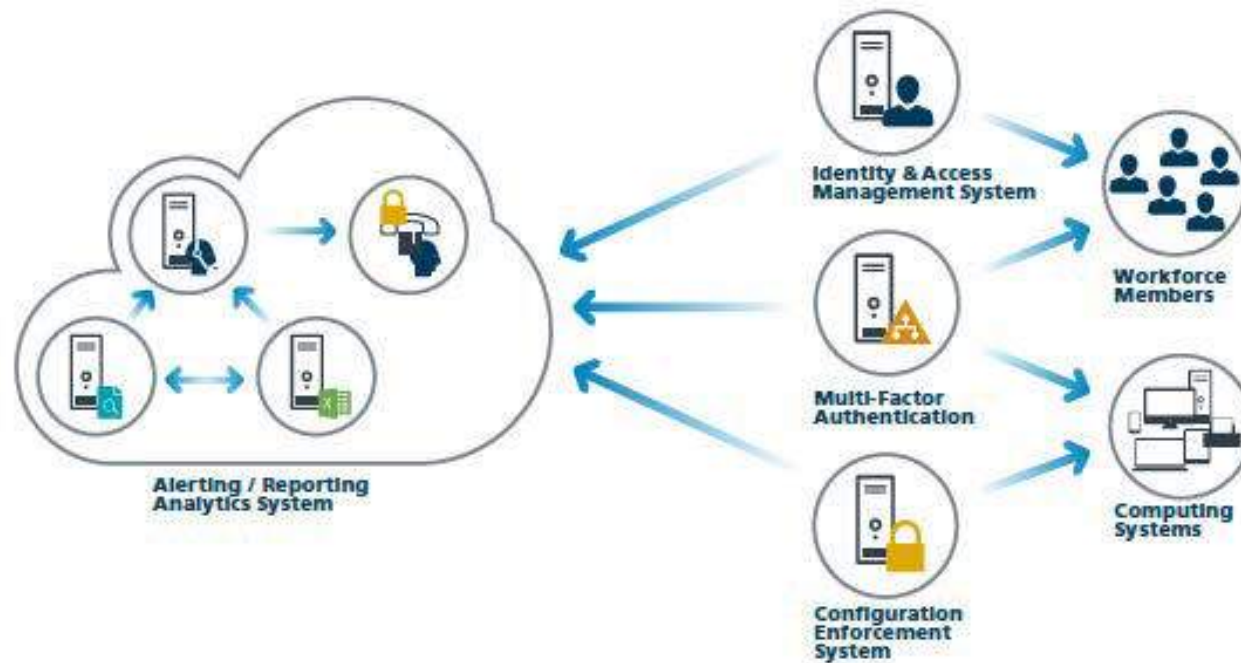
Organizational

- 17 Implement a Security Awareness and Training Program
- 18 Application Software Security
- 19 Incident Response and Management
- 20 Penetration Tests and Red Team Exercises

<https://www.cisecurity.org/controls/>

CIS CONTROL 16: ACCOUNT MONITORING & CONTROL-III

CIS Control 16: System Entity Relationship Diagram



<https://www.cisecurity.org/controls/>

CIS CONTROL 16: ACCOUNT MONITORING & CONTROL-III

16.9: Disable Dormant Accounts

- Automatically disable dormant accounts after a set period of inactivity.

CIS CONTROL 16: ACCOUNT MONITORING & CONTROL-III

16.10: Ensure All Accounts Have An Expiration Date

- Ensure that all accounts have an expiration date that is monitored and enforced.

16.11: Lock Workstation Sessions After Inactivity

- Automatically lock workstation sessions after a standard period of inactivity.

CIS CONTROL 16: ACCOUNT MONITORING & CONTROL-III

16.12: Monitor Attempts to Access Deactivated Accounts

- Monitor attempts to access deactivated accounts through audit logging.

CIS CONTROL 16: ACCOUNT MONITORING & CONTROL-III

16.13: Alert on Account Login Behavior Deviation

- Alert when users deviate from normal login behavior, such as time-of-day, workstation location and duration.

END

CIS CONTROL 17: SECURITY AWARENESS & TRAINING-I

- **IMPLEMENT A
SECURITY AWARENESS
& TRAINING PROGRAM**

CIS CONTROL 17: SECURITY AWARENESS & TRAINING-I



V7

Basic

- 1 Inventory and Control of Hardware Assets
- 2 Inventory and Control of Software Assets
- 3 Continuous Vulnerability Management
- 4 Controlled Use of Administrative Privileges
- 5 Secure Configuration for Hardware and Software on Mobile Devices, Laptops, Workstations and Servers
- 6 Maintenance, Monitoring and Analysis of Audit Logs

Foundational

- 7 Email and Web Browser Protections
- 8 Malware Defenses
- 9 Limitation and Control of Network Ports, Protocols, and Services
- 10 Data Recovery Capabilities
- 11 Secure Configuration for Network Devices, such as Firewalls, Routers and Switches
- 12 Boundary Defense
- 13 Data Protection
- 14 Controlled Access Based on the Need to Know
- 15 Wireless Access Control
- 16 Account Monitoring and Control

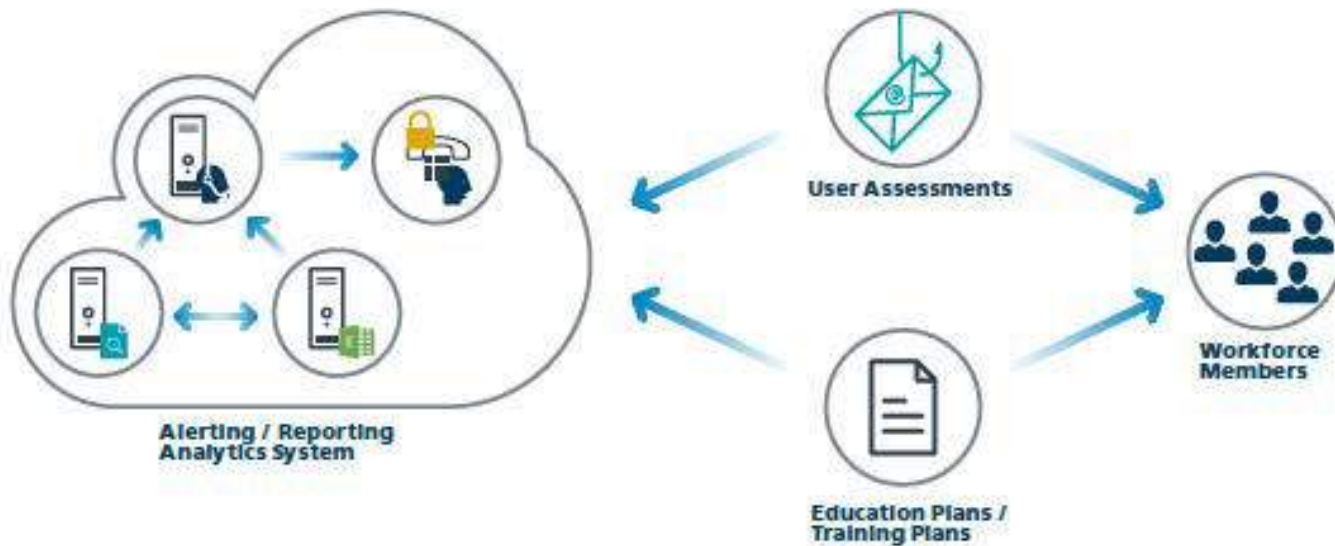
Organizational

- 17 Implement a Security Awareness and Training Program
- 18 Application Software Security
- 19 Incident Response and Management
- 20 Penetration Tests and Red Team Exercises

<https://www.cisecurity.org/controls/>

CIS CONTROL 17: SECURITY AWARENESS & TRAINING-I

CIS Control 17: System Entity Relationship Diagram



<https://www.cisecurity.org/controls/>

CIS CONTROL 17: SECURITY AWARENESS & TRAINING-I

17.1: Perform a Skills Gap Analysis

- Perform a skills gap analysis to understand the skills and behaviors workforce members are not adhering to, using this information to build a baseline education roadmap.

CIS CONTROL 17: SECURITY AWARENESS & TRAINING-I

17.2: Deliver Training to Fill the Skills Gap

- Deliver training to address the skills gap identified to positively impact workforce members' security behavior.

CIS CONTROL 17: SECURITY AWARENESS & TRAINING-I

17.3: Implement a Security Awareness Program

- Create a security awareness program for all workforce members to complete on a regular basis to ensure they understand and exhibit the necessary behaviors and skills to help ensure the security of the organization.

CIS CONTROL 17: SECURITY AWARENESS & TRAINING-I

17.3: Implement a Security Awareness Program

- The organization's security awareness program should be communicated in a continuous and engaging manner...

CIS CONTROL 17: SECURITY AWARENESS & TRAINING-I

17.4: Update Awareness Content Frequently

- ... Ensure that the organization's security awareness program is updated frequently (at least annually) to address new technologies, threats, standards and business requirements.

END

CIS CONTROL 17: SECURITY AWARENESS & TRAINING-II

- **IMPLEMENT A
SECURITY AWARENESS
& TRAINING PROGRAM**

CIS CONTROL 17: SECURITY AWARENESS & TRAINING-II



V7

Basic

- 1 Inventory and Control of Hardware Assets
- 2 Inventory and Control of Software Assets
- 3 Continuous Vulnerability Management
- 4 Controlled Use of Administrative Privileges
- 5 Secure Configuration for Hardware and Software on Mobile Devices, Laptops, Workstations and Servers
- 6 Maintenance, Monitoring and Analysis of Audit Logs

Foundational

- 7 Email and Web Browser Protections
- 8 Malware Defenses
- 9 Limitation and Control of Network Ports, Protocols, and Services
- 10 Data Recovery Capabilities
- 11 Secure Configuration for Network Devices, such as Firewalls, Routers and Switches
- 12 Boundary Defense
- 13 Data Protection
- 14 Controlled Access Based on the Need to Know
- 15 Wireless Access Control
- 16 Account Monitoring and Control

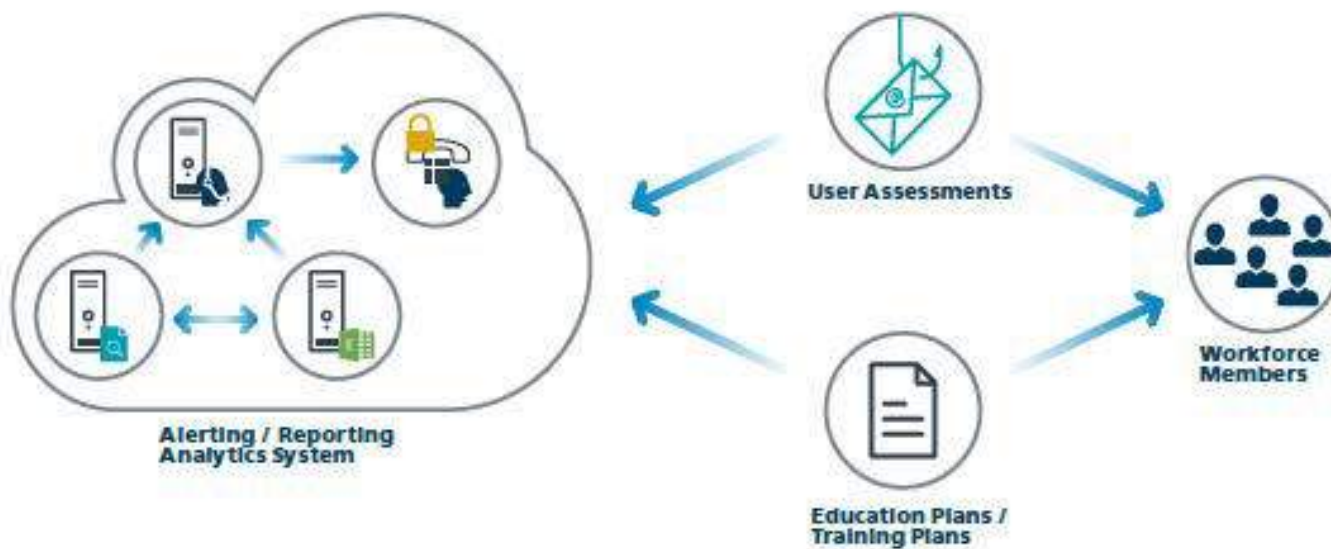
Organizational

- 17 Implement a Security Awareness and Training Program
- 18 Application Software Security
- 19 Incident Response and Management
- 20 Penetration Tests and Red Team Exercises

<https://www.cisecurity.org/controls/>

CIS CONTROL 17: SECURITY AWARENESS & TRAINING-II

CIS Control 17: System Entity Relationship Diagram



<https://www.cisecurity.org/controls/>

CIS CONTROL 17: SECURITY AWARENESS & TRAINING-II

17.5: Train Workforce on Secure Authentication

- Train workforce members on the importance of enabling and utilizing secure authentication.

CIS CONTROL 17: SECURITY AWARENESS & TRAINING-II

17.6: Train Workforce on Identifying Social Engineering Attacks

- Train the workforce on how to identify different forms of social engineering attacks, such as phishing, phone scams and impersonation calls.

CIS CONTROL 17: SECURITY AWARENESS & TRAINING-II

17.7: Train Workforce on Sensitive Data Handling

- Train workforce on how to identify and properly store, transfer, archive and destroy sensitive information.

CIS CONTROL 17: SECURITY AWARENESS & TRAINING-II

17.8: Train Workforce on Causes of Unintentional Data Exposure

- Train workforce members to be aware of causes for unintentional data exposures, such as losing their mobile devices or emailing the wrong person due to autocomplete in email.

CIS CONTROL 17: SECURITY AWARENESS & TRAINING-II

17.9: Train Workforce Members on Identifying and Reporting Incidents

- Train employees to be able to identify the most common indicators of an incident and be able to report such an incident.

END

CIS CONTROL 18: APPLICATION SOFTWARE SECURITY-I

- **APPLICATION
SOFTWARE SECURITY**

CIS CONTROL 18: APPLICATION SOFTWARE SECURITY-I



V7

Basic

- 1 Inventory and Control of Hardware Assets
- 2 Inventory and Control of Software Assets
- 3 Continuous Vulnerability Management
- 4 Controlled Use of Administrative Privileges
- 5 Secure Configuration for Hardware and Software on Mobile Devices, Laptops, Workstations and Servers
- 6 Maintenance, Monitoring and Analysis of Audit Logs

Foundational

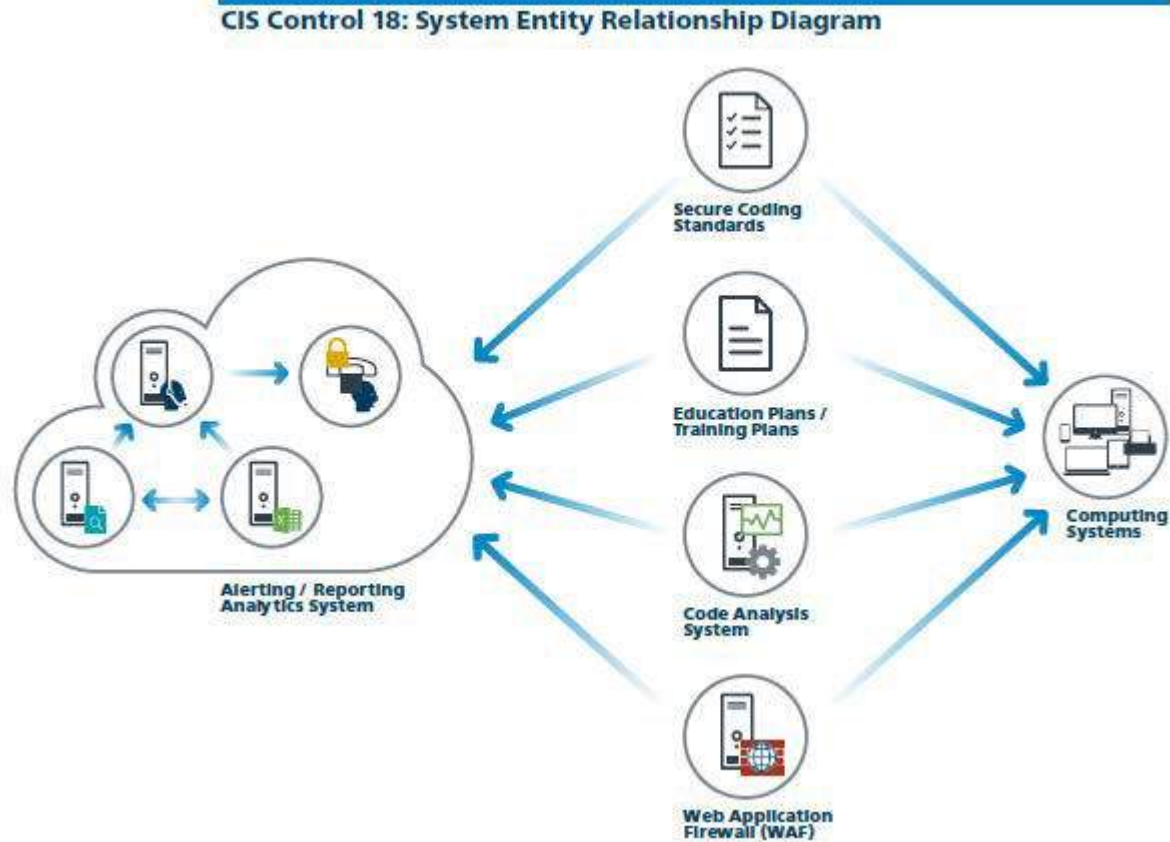
- 7 Email and Web Browser Protections
- 8 Malware Defenses
- 9 Limitation and Control of Network Ports, Protocols, and Services
- 10 Data Recovery Capabilities
- 11 Secure Configuration for Network Devices, such as Firewalls, Routers and Switches
- 12 Boundary Defense
- 13 Data Protection
- 14 Controlled Access Based on the Need to Know
- 15 Wireless Access Control
- 16 Account Monitoring and Control

Organizational

- 17 Implement a Security Awareness and Training Program
- 18 Application Software Security
- 19 Incident Response and Management
- 20 Penetration Tests and Red Team Exercises

<https://www.cisecurity.org/controls/>

CIS CONTROL 18: APPLICATION SOFTWARE SECURITY-I



<https://www.cisecurity.org/controls/>

CIS CONTROL 18: APPLICATION SOFTWARE SECURITY-I

18.1: Establish Secure Coding Practices

- Establish secure coding practices appropriate to the programming language and development environment being used.

CIS CONTROL 18: APPLICATION SOFTWARE SECURITY-I

18.2: Ensure Explicit Error Checking is Performed for All In-house Developed Software

- For in-house developed software, ensure that explicit error checking is performed and documented for all input, including for size, data type, & acceptable ranges or formats.

CIS CONTROL 18: APPLICATION SOFTWARE SECURITY-I

18.3: Verify That Acquired Software is Still Supported

- Verify that the version of all software acquired from outside your organization is still supported by the developer or appropriately hardened based on developer security recommendations.

CIS CONTROL 18: APPLICATION SOFTWARE SECURITY-I

18.4: Only Use Up-to-date And Trusted Third-Party Components

- Only use up-to-date and trusted third-party components for the software developed by the organization.

END

CIS CONTROL 18: APPLICATION SOFTWARE SECURITY-I

- **APPLICATION
SOFTWARE SECURITY**

CIS CONTROL 18: APPLICATION SOFTWARE SECURITY-I



V7

Basic

- 1 Inventory and Control of Hardware Assets
- 2 Inventory and Control of Software Assets
- 3 Continuous Vulnerability Management
- 4 Controlled Use of Administrative Privileges
- 5 Secure Configuration for Hardware and Software on Mobile Devices, Laptops, Workstations and Servers
- 6 Maintenance, Monitoring and Analysis of Audit Logs

Foundational

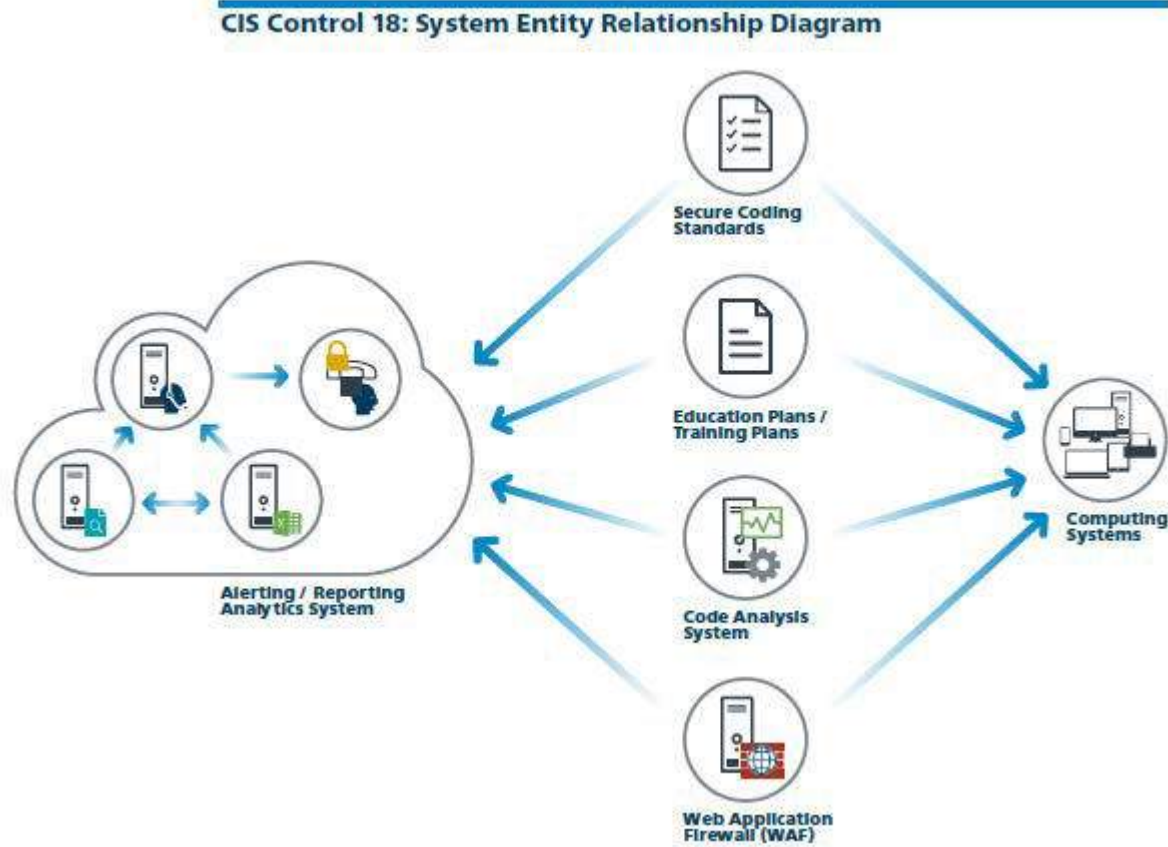
- 7 Email and Web Browser Protections
- 8 Malware Defenses
- 9 Limitation and Control of Network Ports, Protocols, and Services
- 10 Data Recovery Capabilities
- 11 Secure Configuration for Network Devices, such as Firewalls, Routers and Switches
- 12 Boundary Defense
- 13 Data Protection
- 14 Controlled Access Based on the Need to Know
- 15 Wireless Access Control
- 16 Account Monitoring and Control

Organizational

- 17 Implement a Security Awareness and Training Program
- 18 Application Software Security
- 19 Incident Response and Management
- 20 Penetration Tests and Red Team Exercises

<https://www.cisecurity.org/controls/>

CIS CONTROL 18: APPLICATION SOFTWARE SECURITY-I



<https://www.cisecurity.org/controls/>

CIS CONTROL 18: APPLICATION SOFTWARE SECURITY-II

18.5: Use Only Standardized and Extensively Reviewed Encryption Algorithms

Use only standardized and extensively reviewed encryption algorithms.

CIS CONTROL 18: APPLICATION SOFTWARE SECURITY-II

18.6: Ensure Software Development Personnel are Trained in Secure Coding

Ensure that all software development personnel receive training in writing secure code for their specific development environment and responsibilities.

CIS CONTROL 18: APPLICATION SOFTWARE SECURITY-II

18.7: Apply Static and Dynamic Code Analysis Tools

Apply static and dynamic analysis tools to verify that secure coding practices are being adhered to for internally developed software.

CIS CONTROL 18: APPLICATION SOFTWARE SECURITY-II

18.8: Establish a Process to Accept and Address Reports of Software Vulnerabilities

Establish a process to accept and address reports of software vulnerabilities, including providing a means for external entities to contact your security group.

END

CIS CONTROL 18: APPLICATION SOFTWARE SECURITY-III

- **APPLICATION
SOFTWARE SECURITY**

CIS CONTROL 18: APPLICATION SOFTWARE SECURITY-III



V7

Basic

- 1 Inventory and Control of Hardware Assets
- 2 Inventory and Control of Software Assets
- 3 Continuous Vulnerability Management
- 4 Controlled Use of Administrative Privileges
- 5 Secure Configuration for Hardware and Software on Mobile Devices, Laptops, Workstations and Servers
- 6 Maintenance, Monitoring and Analysis of Audit Logs

Foundational

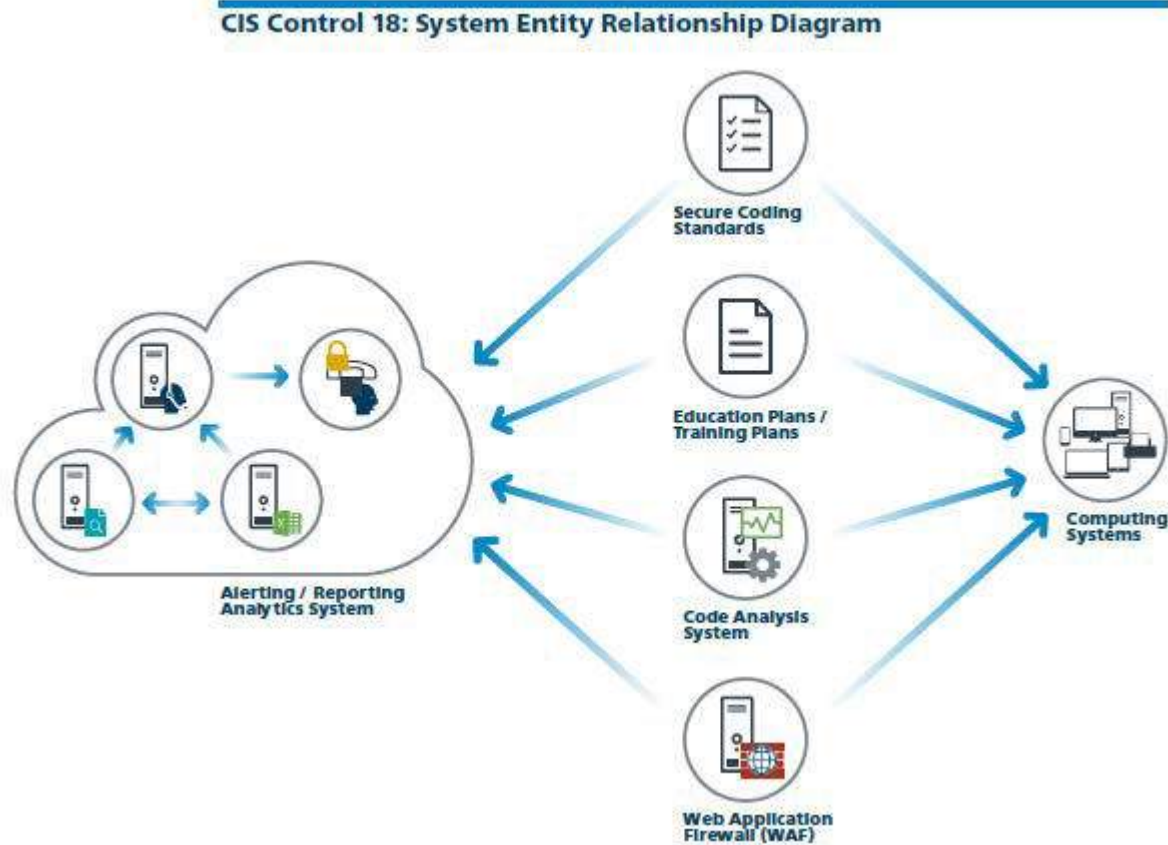
- 7 Email and Web Browser Protections
- 8 Malware Defenses
- 9 Limitation and Control of Network Ports, Protocols, and Services
- 10 Data Recovery Capabilities
- 11 Secure Configuration for Network Devices, such as Firewalls, Routers and Switches
- 12 Boundary Defense
- 13 Data Protection
- 14 Controlled Access Based on the Need to Know
- 15 Wireless Access Control
- 16 Account Monitoring and Control

Organizational

- 17 Implement a Security Awareness and Training Program
- 18 Application Software Security
- 19 Incident Response and Management
- 20 Penetration Tests and Red Team Exercises

<https://www.cisecurity.org/controls/>

CIS CONTROL 18: APPLICATION SOFTWARE SECURITY-III



<https://www.cisecurity.org/controls/>

18.9: Separate Production and Non-Production Systems

- Maintain separate environments for production and nonproduction systems. Developers should not have unmonitored access to production environments.

18.10: Deploy Web Application Firewalls (WAFs)

- Protect web applications by deploying web application firewalls (WAFs) that inspect all traffic flowing to the web application for common web application attacks.

18.10: Deploy Web Application Firewalls (WAFs)

- ... For applications that are not web-based, specific application firewalls should be deployed if such tools are available for the given application type. If the traffic is encrypted, the device should...

18.10: Deploy Web Application Firewalls (WAFs)

- ...either sit behind the encryption or be capable of decrypting the traffic prior to analysis. If neither option is appropriate, a host-based web application firewall should be deployed.

18.11: Use Standard Hardening Configuration Templates for Databases

- For applications that rely on a database, use standard hardening configuration templates. All systems that are part of critical business processes should also be tested.

CIS CONTROL 19: INCIDENT RESPONSE & MANAGEMENT-I

- **INCIDENT RESPONSE & MANAGEMENT**

CIS CONTROL 19: INCIDENT RESPONSE & MANAGEMENT-I



V7

Basic

- 1 Inventory and Control of Hardware Assets
- 2 Inventory and Control of Software Assets
- 3 Continuous Vulnerability Management
- 4 Controlled Use of Administrative Privileges
- 5 Secure Configuration for Hardware and Software on Mobile Devices, Laptops, Workstations and Servers
- 6 Maintenance, Monitoring and Analysis of Audit Logs

Foundational

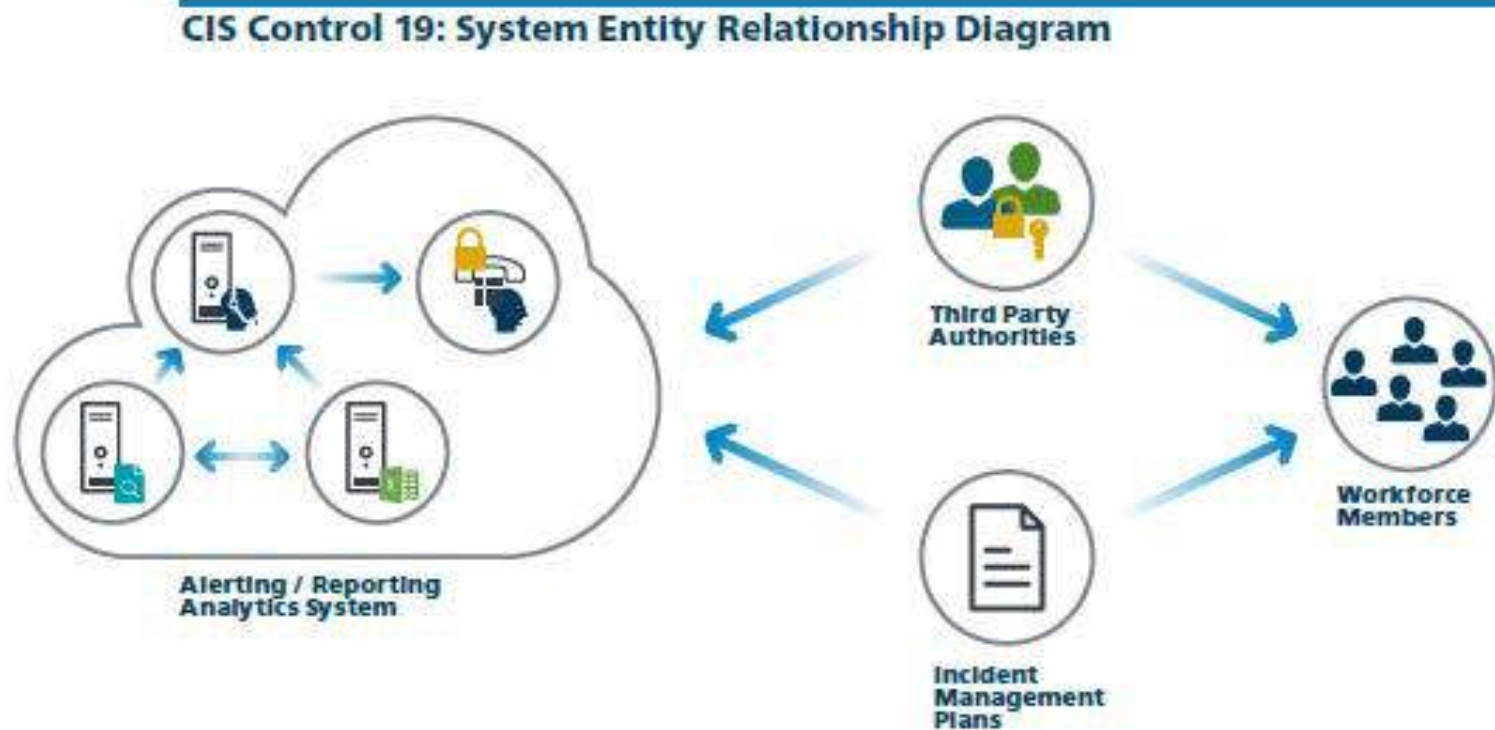
- 7 Email and Web Browser Protections
- 8 Malware Defenses
- 9 Limitation and Control of Network Ports, Protocols, and Services
- 10 Data Recovery Capabilities
- 11 Secure Configuration for Network Devices, such as Firewalls, Routers and Switches
- 12 Boundary Defense
- 13 Data Protection
- 14 Controlled Access Based on the Need to Know
- 15 Wireless Access Control
- 16 Account Monitoring and Control

Organizational

- 17 Implement a Security Awareness and Training Program
- 18 Application Software Security
- 19 Incident Response and Management
- 20 Penetration Tests and Red Team Exercises

<https://www.cisecurity.org/controls/>

CIS CONTROL 19: INCIDENT RESPONSE & MANAGEMENT-I



<https://www.cisecurity.org/controls/>

CIS CONTROL 19: INCIDENT RESPONSE & MANAGEMENT-I

19.1: Document Incident Response Procedures

- Ensure that there are written incident response plans that defines roles of personnel as well as phases of incident handling/management.

CIS CONTROL 19: INCIDENT RESPONSE & MANAGEMENT-I

19.2: Assign Job Titles and Duties for Incident Response

- Assign job titles and duties for handling computer and network incidents to specific individuals and ensure tracking and documentation throughout the incident through resolution.

CIS CONTROL 19: INCIDENT RESPONSE & MANAGEMENT-I

19.3: Designate Management Personnel to Support Incident Handling

- Designate management personnel, as well as backups, who will support the incident handling process by acting in key decision-making roles.

19.4: Devise Organization-wide Standards for Reporting Incidents

- Devise organization-wide standards for the time required for system administrators and other workforce members to report anomalous events to the incident handling team, ...

CIS CONTROL 19: INCIDENT RESPONSE & MANAGEMENT-I

19.4: Devise Organization-wide Standards for Reporting Incidents

- ... the mechanisms for such reporting, and the kind of information that should be included in the incident notification.

CIS CONTROL 19: INCIDENT RESPONSE & MANAGEMENT-II

- **INCIDENT RESPONSE & MANAGEMENT**

CIS CONTROL 19: INCIDENT RESPONSE & MANAGEMENT-II



V7

Basic

- 1 Inventory and Control of Hardware Assets
- 2 Inventory and Control of Software Assets
- 3 Continuous Vulnerability Management
- 4 Controlled Use of Administrative Privileges
- 5 Secure Configuration for Hardware and Software on Mobile Devices, Laptops, Workstations and Servers
- 6 Maintenance, Monitoring and Analysis of Audit Logs

Foundational

- 7 Email and Web Browser Protections
- 8 Malware Defenses
- 9 Limitation and Control of Network Ports, Protocols, and Services
- 10 Data Recovery Capabilities
- 11 Secure Configuration for Network Devices, such as Firewalls, Routers and Switches
- 12 Boundary Defense
- 13 Data Protection
- 14 Controlled Access Based on the Need to Know
- 15 Wireless Access Control
- 16 Account Monitoring and Control

Organizational

- 17 Implement a Security Awareness and Training Program
- 18 Application Software Security
- 19 Incident Response and Management
- 20 Penetration Tests and Red Team Exercises

<https://www.cisecurity.org/controls/>

CIS CONTROL 19: INCIDENT RESPONSE & MANAGEMENT-II

CIS Control 19: System Entity Relationship Diagram



<https://www.cisecurity.org/controls/>

19.5: Maintain Contact Information For Reporting Security Incidents

- Assemble & maintain information on third-party contact information to be used to report a security incident, such as Law Enforcement, relevant govt departments, vendors, etc

19.6: Publish Information Regarding Reporting Computer Anomalies and Incidents

- Publish information for all workforce members, regarding reporting computer anomalies and incidents to the incident handling team. Such information should be...

CIS CONTROL 19: INCIDENT RESPONSE & MANAGEMENT-II

19.6: Publish Information Regarding Reporting Computer Anomalies and Incidents

- ...included in routine employee awareness activities.

19.7: Conduct Periodic Incident Scenario Sessions for Personnel

- Plan and conduct routine incident response exercises and scenarios for the workforce involved in the incident response to maintain awareness and comfort in responding to real world threats.

19.7: Conduct Periodic Incident Scenario Sessions for Personnel

- ... Exercises should test communication channels, decision making, and incident responders technical capabilities using tools and data available to them.

19.8: Create Incident Scoring and Prioritization Schema

- Create incident scoring and prioritization schema based on known or potential impact to your organization. Utilize score to define frequency of status updates and escalation procedures.

CIS CONTROL 20: PEN TESTS & RED TEAM EXERCISES-I

- **PENETRATION TESTS & RED TEAM EXERCISES**

CIS CONTROL 20: PEN TESTS & RED TEAM EXERCISES-I



V7

Basic

- 1 Inventory and Control of Hardware Assets
- 2 Inventory and Control of Software Assets
- 3 Continuous Vulnerability Management
- 4 Controlled Use of Administrative Privileges
- 5 Secure Configuration for Hardware and Software on Mobile Devices, Laptops, Workstations and Servers
- 6 Maintenance, Monitoring and Analysis of Audit Logs

Foundational

- 7 Email and Web Browser Protections
- 8 Malware Defenses
- 9 Limitation and Control of Network Ports, Protocols, and Services
- 10 Data Recovery Capabilities
- 11 Secure Configuration for Network Devices, such as Firewalls, Routers and Switches
- 12 Boundary Defense
- 13 Data Protection
- 14 Controlled Access Based on the Need to Know
- 15 Wireless Access Control
- 16 Account Monitoring and Control

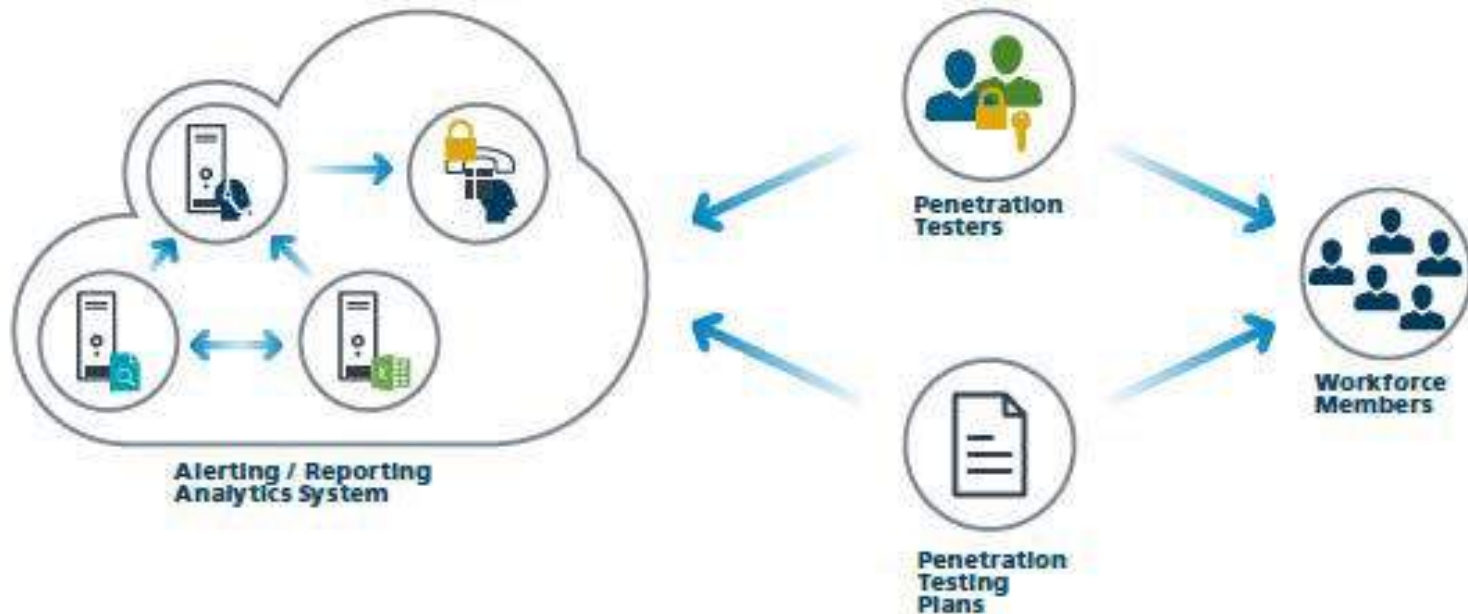
Organizational

- 17 Implement a Security Awareness and Training Program
- 18 Application Software Security
- 19 Incident Response and Management
- 20 Penetration Tests and Red Team Exercises

<https://www.cisecurity.org/controls/>

CIS CONTROL 20: PEN TESTS & RED TEAM EXERCISES-I

CIS Control 20: System Entity Relationship Diagram



<https://www.cisecurity.org/controls/>

20.1: Establish a Penetration Testing Program

- Establish a program for penetration tests that includes a full scope of blended attacks, such as wireless, client-based, and web application attacks.

20.2: Conduct Regular External and Internal Penetration Tests

- Conduct regular external and internal penetration tests to identify vulnerabilities and attack vectors that can be used to exploit enterprise systems successfully.

20.3: Perform Periodic Red Team Exercises

- Perform periodic Red Team exercises to test organizational readiness to identify and stop attacks or to respond quickly and effectively.

20.4: Include Tests for Presence of Unprotected System Information and Artifacts

- Include tests for the presence of unprotected system information and artifacts that would be useful to attackers, including network diagrams, ...

20.4: Include Tests for Presence of Unprotected System Information and Artifacts

- ... configuration files, older penetration test reports, e-mails or documents containing passwords or other information critical to system operation.

CIS CONTROL 20: PEN TESTS & RED TEAM EXERCISES-II

- **PENETRATION TESTS & RED TEAM EXERCISES**

CIS CONTROL 20: PEN TESTS & RED TEAM EXERCISES-II



V7

Basic

- 1 Inventory and Control of Hardware Assets
- 2 Inventory and Control of Software Assets
- 3 Continuous Vulnerability Management
- 4 Controlled Use of Administrative Privileges
- 5 Secure Configuration for Hardware and Software on Mobile Devices, Laptops, Workstations and Servers
- 6 Maintenance, Monitoring and Analysis of Audit Logs

Foundational

- 7 Email and Web Browser Protections
- 8 Malware Defenses
- 9 Limitation and Control of Network Ports, Protocols, and Services
- 10 Data Recovery Capabilities
- 11 Secure Configuration for Network Devices, such as Firewalls, Routers and Switches
- 12 Boundary Defense
- 13 Data Protection
- 14 Controlled Access Based on the Need to Know
- 15 Wireless Access Control
- 16 Account Monitoring and Control

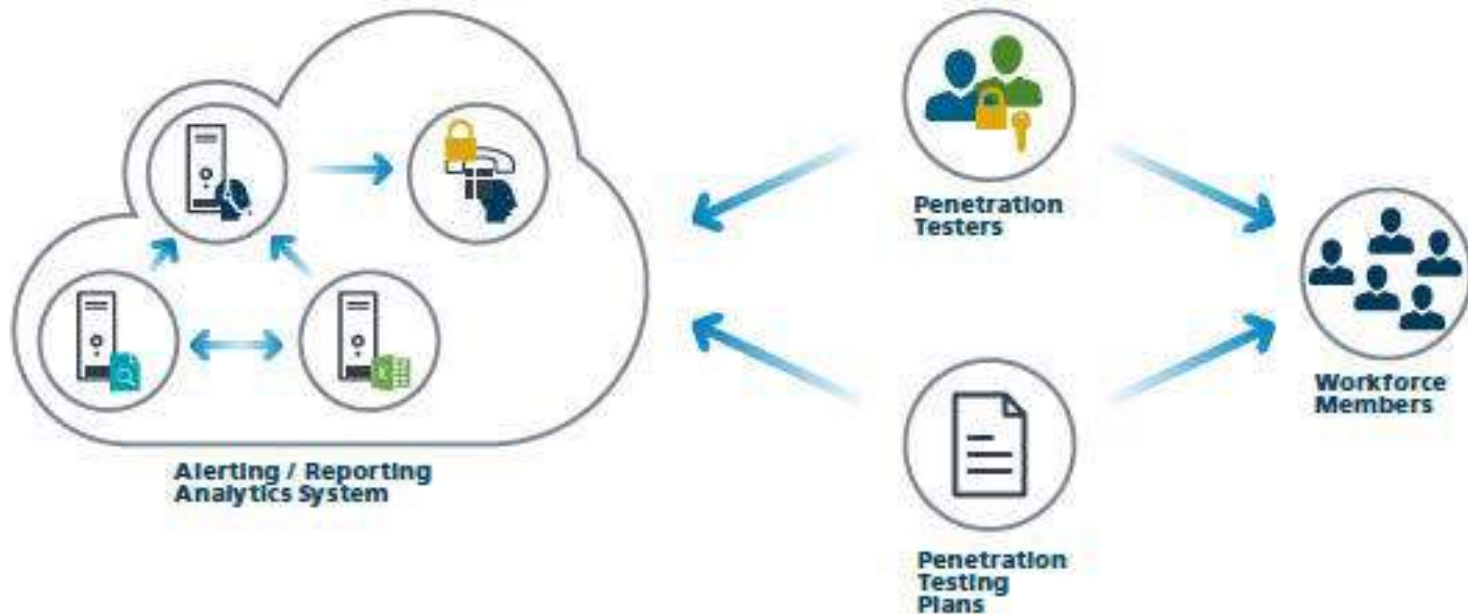
Organizational

- 17 Implement a Security Awareness and Training Program
- 18 Application Software Security
- 19 Incident Response and Management
- 20 Penetration Tests and Red Team Exercises

<https://www.cisecurity.org/controls/>

CIS CONTROL 20: PEN TESTS & RED TEAM EXERCISES-II

CIS Control 20: System Entity Relationship Diagram



<https://www.cisecurity.org/controls/>

20.5: Create Test Bed for Elements Not Typically Tested in Production

- Create a test bed that mimics a production environment for specific penetration tests and Red Team attacks against elements that are not typically tested in production, such as attacks against...

20.5: Create Test Bed for Elements Not Typically Tested in Production

- ...supervisory control and data acquisition and other control systems.

20.6: Use Vulnerability Scanning and Penetration Testing Tools in Concert

- Use vulnerability scanning & penetration testing tools in concert. The results of vulnerability scanning assessments should be used as a starting point to guide & focus pen testing efforts.

20.7: Ensure Results from Penetration Test are Documented Using Open, Machine-readable Standards

- Wherever possible, ensure that Red Teams results are documented using open, machine-readable standards (e.g., SCAP). Devise a scoring ...

CIS CONTROL 20: PEN TESTS & RED TEAM EXERCISES-II

20.7: Ensure Results from Penetration Test are Documented Using Open, Machine-readable Standards

- ...method for determining the results of Red Team exercises so that results can be compared over time.

20.8: Control and Monitor Accounts Associated with Penetration Testing

- Any user or system accounts used to perform penetration testing should be controlled and monitored to make sure they are only being used for legitimate purposes, ...

20.8: Control and Monitor Accounts Associated with Penetration Testing

- ...and are removed or restored to normal function after testing is over.

END

What Is IT Governance ?

- What is IT Governance ?
 - The primary goals of IT Governance are to assure that the investments in IT generate business value, and to mitigate the risks that are associated with IT

http://www.intosaiitaudit.org/intoit_articles/25_p30top35.pdf

What Is IT Governance ?

- What is IT Governance ?
 - Simply put, it's putting structure around how organizations align IT strategy with business strategy, ensuring that companies stay on track to achieve their strategies and goals,

<http://www.cio.com/article/2438931/governance/it-governance-definition-and-solutions.html>

What Is IT Governance ?

- What is IT Governance ?
 - ... and implementing good ways to measure IT's performance.
 - It makes sure that all stakeholders' interests are taken into account and that processes provide measurable results.

<http://www.cio.com/article/2438931/governance/it-governance-definition-and-solutions.html>

What Is IT Governance ?

- What is IT Governance ?
 - An IT governance framework should answer key questions such as how the IT dept is functioning overall, what key metrics management needs and what return IT is giving back to the business from investments

<http://www.cio.com/article/2438931/governance/it-governance-definition-and-solutions.html>

What Is IT Governance?

- Frameworks which cover IT Governance:
 - **ISO27001: 2013**
(Information Security Management System - ISMS)
 - **ITIL** (IT Infrastructure Library)
 - **COBIT** (Control Objectives for Information & Related Technology)

https://www.itgovernance.co.uk/it_governance

What Is IT Governance?



What Is IT Governance ?

- What is COBIT ?
 - Simply stated, COBIT 5 helps enterprises to create optimal value from IT by maintaining a balance between realising benefits and optimising risk levels and resource use.

END



What Is Information Security Governance ?

- What is Information Security governance ?
 - "Security governance is the set of responsibilities and practices exercised by the board and executive management with the goal of providing strategic direction,

IT Governance Institute (ITGI), Guidance
For Boards of Directors & Executive
Management, 2nd Edition

What Is Information Security Governance ?

- What is Information Security governance ?
 - *ensuring that objectives are achieved, ascertaining that risks are managed appropriately and verifying that the enterprise's resources are used responsibly."*

IT Governance Institute (ITGI), Guidance
For Boards of Directors & Executive
Management, 2nd Edition

What Is Information Security Governance ?

- Information Security governance is the mechanism how the information security function is managed by the organization

What Is Information Security Governance?

IT Governance

Information
Security
Governance

Business
Continuity &
DR

IT Service
Management
&
Performance
Management

IT Project
Management

What Is Information Security Governance ?

- The leading framework for Information Security governance is ISO27001:2013 (ISMS)
 - Considered gold standard
 - Most widely deployed Information Security governance framework

What Is Information Security Governance ?

- “Provides a model for establishing, implementing, operating, monitoring, reviewing, maintaining and improving an information security management system.”

ISO27001:2013 (ISMS)

What Is Information Security Governance ?

- **Clauses 4 to 10 of ISO27001:2013**
 - **4: Organization & context, scope**
 - **5: Leadership & commitment, policy, organizational roles & responsibilities**
 - **6: Planning; Infosec objectives and planning to achieve them**

What Is Information Security Governance ?

- Clauses 4 to 10 of ISO27001:2013
 - 7: Support; resources, competence, awareness
 - 8: Operations; risk assessment and risk management

ISO27001:2013 (ISMS)

What Is Information Security Governance ?

- Clauses 4 to 10 of ISO27001:2013
 - 9: Performance evaluation; monitoring, measurement & analysis; internal audit
 - 10: Non-conformities & corrective actions, continual improvement
- ISO27001:2013 (ISMS)

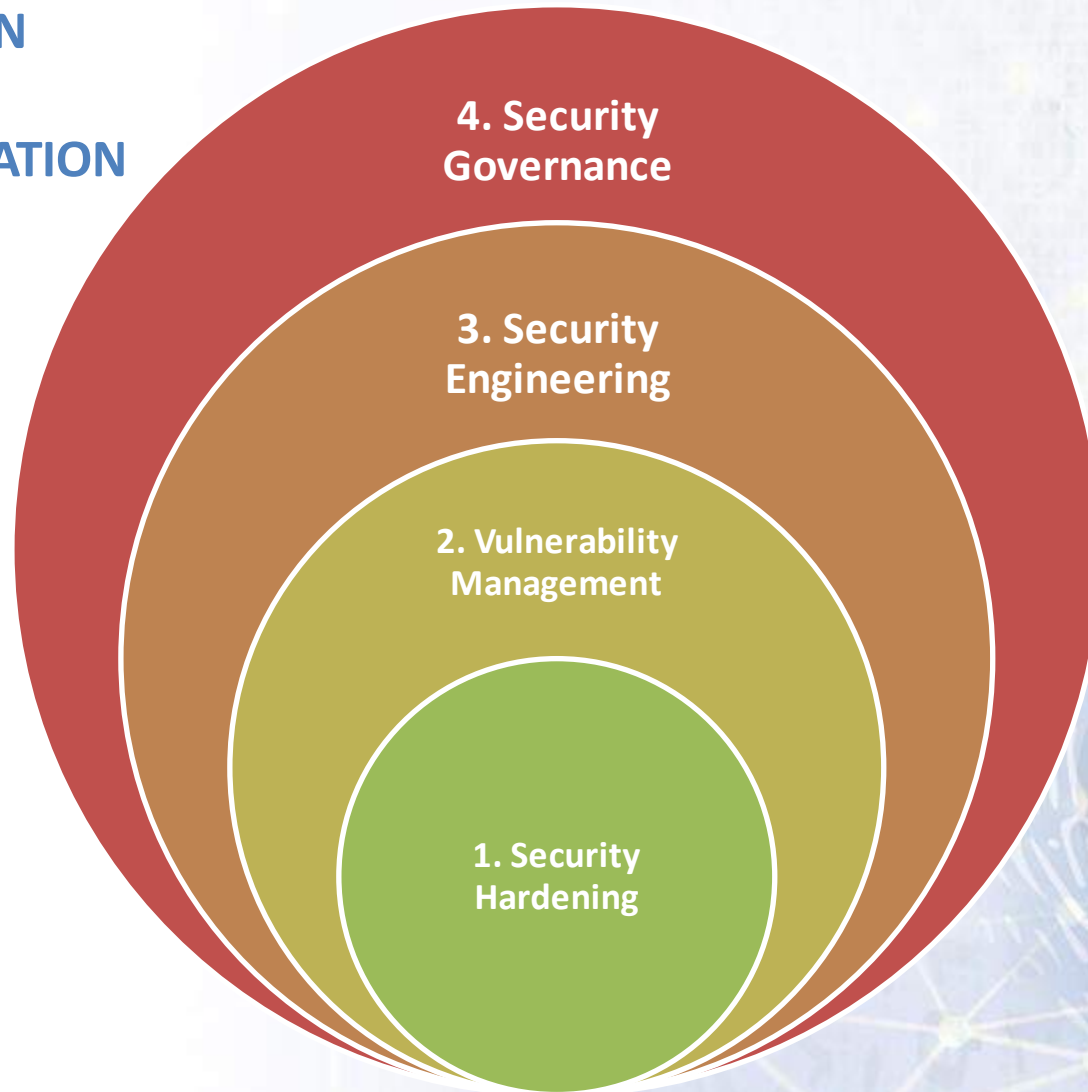
END

Why Is InfoSec Governance At Stage 4 ?

- Lets have a look at the Security Transformation Model

Why Is InfoSec Governance At Stage 4 ?

INFORMATION SECURITY TRANSFORMATION MODEL



Why Is InfoSec Governance At Stage 4 ?

- Why is security governance at stage 4?
 - First build a building and then manage it
 - First 2 stages build up the essential foundation
 - 3rd stage implements advanced security measures
 - Then (4th stage) it is time to manage

Why Is InfoSec Governance At Stage 4 ?

- Limited organizational bandwidth ?
 - Governance is a broad function
 - May get lost in governance if implement at the wrong time
 - Spend limited resources where they count most (in security hardening)

Why Is InfoSec Governance At Stage 4 ?

- Pakistan's InfoSec paradigm –
 - Governance overkill
 - Reactive
 - Superficial
 - Complete absence of underlying security controls
 - ... that is why security transformation is required

Why Is InfoSec Governance At Stage 4 ?

- Once the basic foundations of security hardening, vulnerability management, and security engineering are in place it is time to manage the “system”
- If we try to establish governance first, our entire energies will be consumed in managing a system that has not yet been built....

Why Is InfoSec Governance At Stage 4 ?

- Organizational security maturity... when does governance make sense ?
- Governance is important but only after security hardening & controls (stage 1, 2, and 3) are in place...

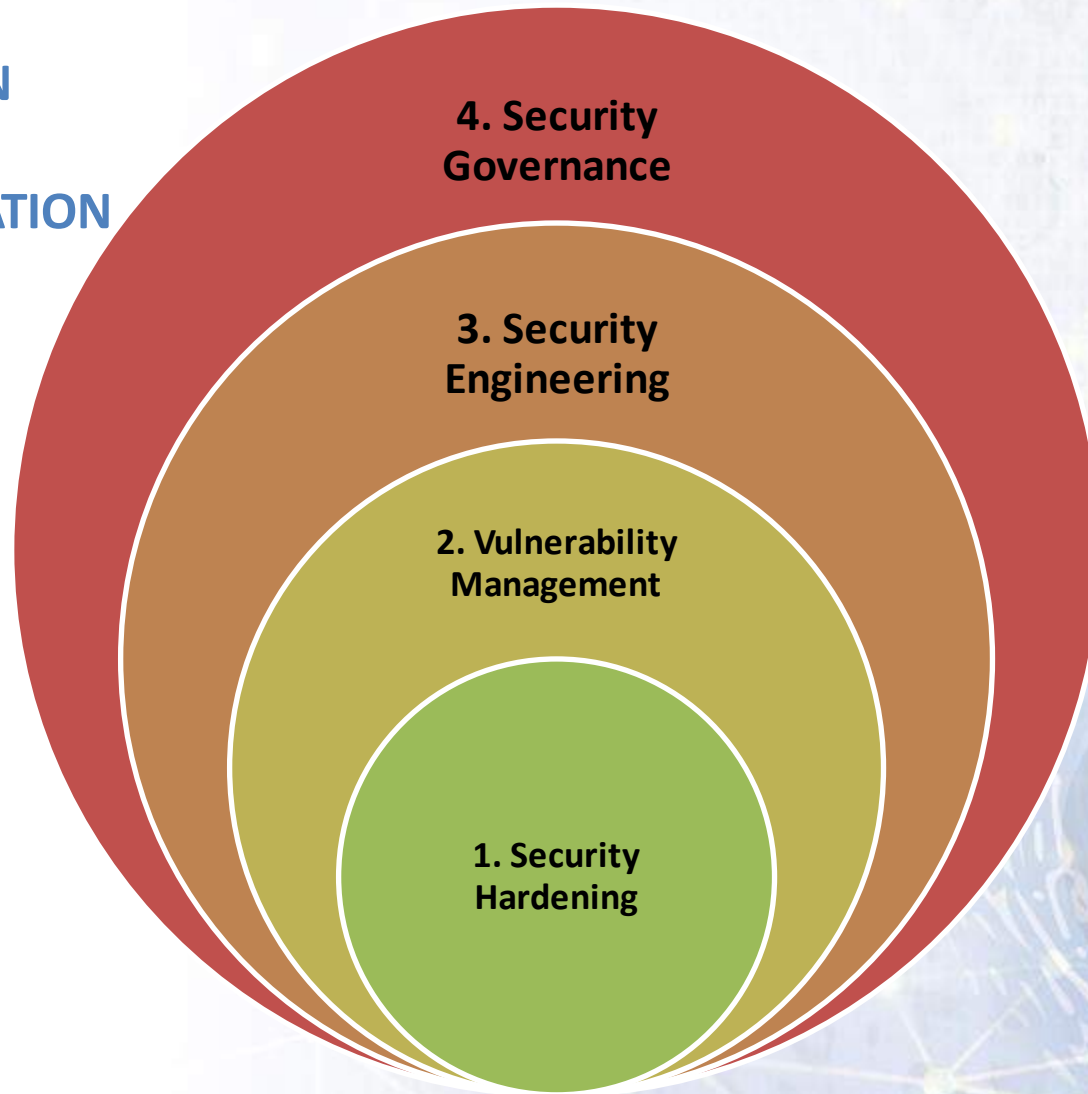
END

Can InfoSec Governance Be Before Stage 4 ?

- Lets have a look at the Security Transformation Model

Can InfoSec Governance Be Before Stage 4 ?

INFORMATION SECURITY TRANSFORMATION MODEL



Can InfoSec Governance Be Before Stage 4 ?

- Implications of implementing Stage 4 before first 3 stages:
 - Expending project energy, resources, and time in governance whereas they should have been spent on building fundamental security foundation (which later requires management)

Can InfoSec Governance Be Before Stage 4 ?

- Implications of implementing Stage 4 before first 3 stages:
 - Getting caught up in intangible “governance” activity
 - Getting caught up in policy & management without essential and fundamental underlying security controls

Can InfoSec Governance Be Before Stage 4 ?

- Implications of implementing Stage 4 before first 3 stages:
 - Setting unrealistic expectations
 - **Note that governance consists of documentation and process which tends to bog down and dis-interest tech resources**

Can InfoSec Governance Be Before Stage 4 ?

- Security controls (Stage 1-3) once they are implemented by following security hardening & vulnerability management international best-practices can be better documented and regulated through governance (policy, SOP)...

Can InfoSec Governance Be Before Stage 4 ?

- Why ?
 - We know what works and is implementable in terms of security controls
 - Controls are implemented incrementally (practical)
 - Minimal policy in place at initial stages as a starting point

Can InfoSec Governance Be Before Stage 4 ?

- However:
 - Certain projects may have governance stipulations by the regulator/customers
 - Deadline to achieve certain governance or security milestones
 - In such cases tailor security transformation project

Can InfoSec Governance Be Before Stage 4 ?

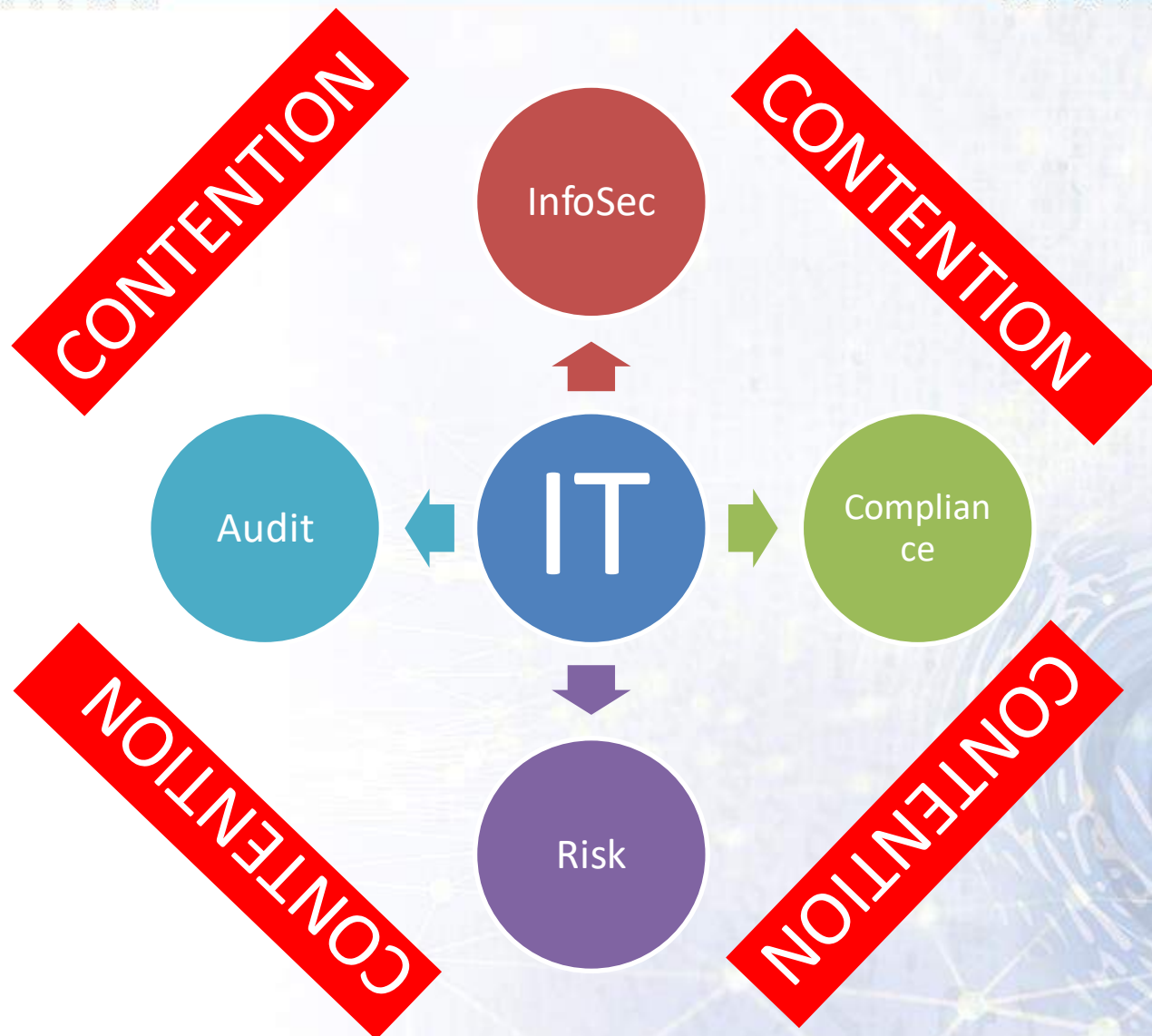
- The sequence of the security transformation model (stages 1 through 4) should be followed wherever possible as it is a tried and tested model
- The security transformation model may be tailored as per your unique requirements

END

Pakistan's InfoSecurity Posture & Challenges

- Lets have a look at the typical IT & Information Security challenges

Pakistan's InfoSecurity Posture & Challenges



Pakistan's InfoSecurity Posture & Challenges

IT CHALLENGES SUMMARY

- ▶ IT is **complex** and difficult to manage
- ▶ IT under **pressure** from **business** groups
- ▶ **Lack of** sufficient (trained) **resources**
- ▶ Lack of **process culture**

IT IS CLEARLY NOT ALIGNED TO PERFORM
DILIGENT SECURITY WORK

Pakistan's InfoSecurity Posture & Challenges

INFORMATION SECURITY CHALLENGES

- ▶ Silos and **lack of** Security **ownership**
- ▶ **Time & energy wasted** in traversing **depts**
- ▶ InfoSecurity is **tough work** –
enabling environment missing

**Fundamental security hardening of IT assets
“in the trenches” is glaringly absent**

Pakistan's InfoSecurity Posture & Challenges

PAKISTAN INDUSTRY CHARACTERISTICS

- ▶ **Wavering** management **commitment**
- ▶ **"Superficial dressing"** security
- ▶ **Reactive** to regulator/audit/compliance
- ▶ **Security hardening** largely **"untouched"**



Industry (has been) in denial

Pakistan's InfoSecurity Posture & Challenges

PAKISTAN INDUSTRY CHARACTERISTICS



Security
Harden ?

Manage
Security ?

Pakistan's InfoSecurity Posture & Challenges

- Pakistan is now almost one entire technology generation behind in Information Security
- IT progressed during the last 10-12 years but InfoSec was ignored
- Information Security Transformation Model is the only way to catch up

END

InfoSec Governance Building Blocks

- Lets have a look at the Information Security governance building blocks

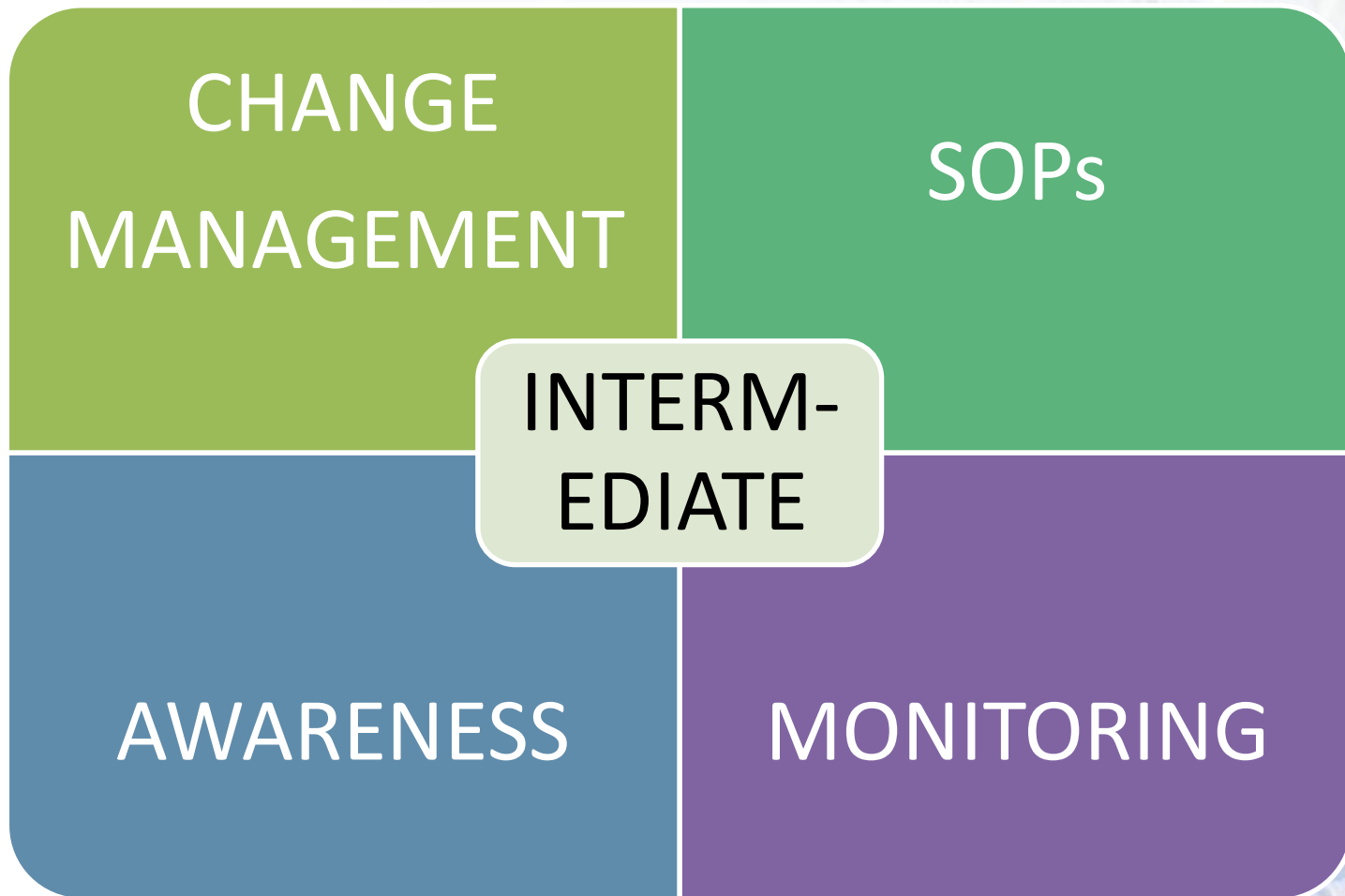
InfoSec Governance Building Blocks

INITIAL GOVERNANCE BUILDING BLOCKS



InfoSec Governance Building Blocks

INTERMEDIATE GOVERNANCE BUILDING BLOCKS



InfoSec Governance Building Blocks

MATURE GOVERNANCE BUILDING BLOCKS

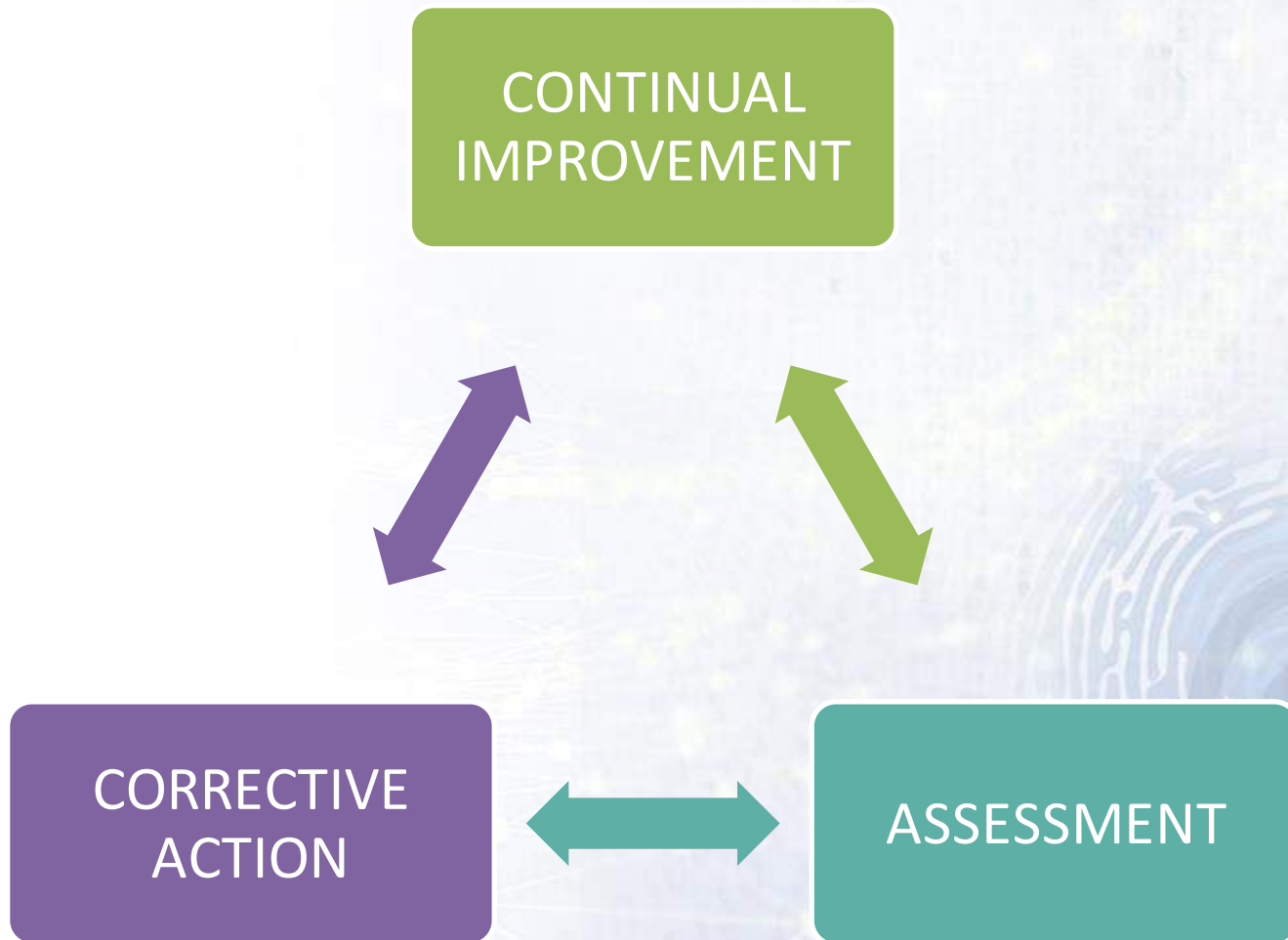
RISK
MANAGEMENT

INTERNAL AUDIT

INCIDENT
MANAGEMENT

InfoSec Governance Building Blocks

CONTINUAL IMPROVEMENT CYCLE



InfoSec Governance Building Blocks

- Governance implementation should be broken up into phases
 - Essential (initial) activities first
 - Gradually progress with activities that match organizational readiness & maturity

END

Whose Responsibility Is InfoSec Governance ?

- Information security governance has responsibilities at different layers of the organization
- In Pakistan, the governance functions are slightly different than practice in more mature markets

Whose Responsibility Is InfoSec Governance ?

TYPICAL ORGANIZATIONAL TIERS AND MEMBERS

TIER	MEMBERS
BOARD (STEERING COMMITTEE)	BOARD MEMBER, CIO, CISO, IT MANAGEMENT, (SOME KEY BUSINESS MEMBERS)
IT MANAGEMENT (CIO)	GMs BELONGING TO IT MANAGEMENT, CISO
CISO/SECURITY HEAD	CISO AND ISMC
IT & SECURITY TEAMS	IT TEAMS AND PROJECT TEAMS

Whose Responsibility Is InfoSec Governance ?

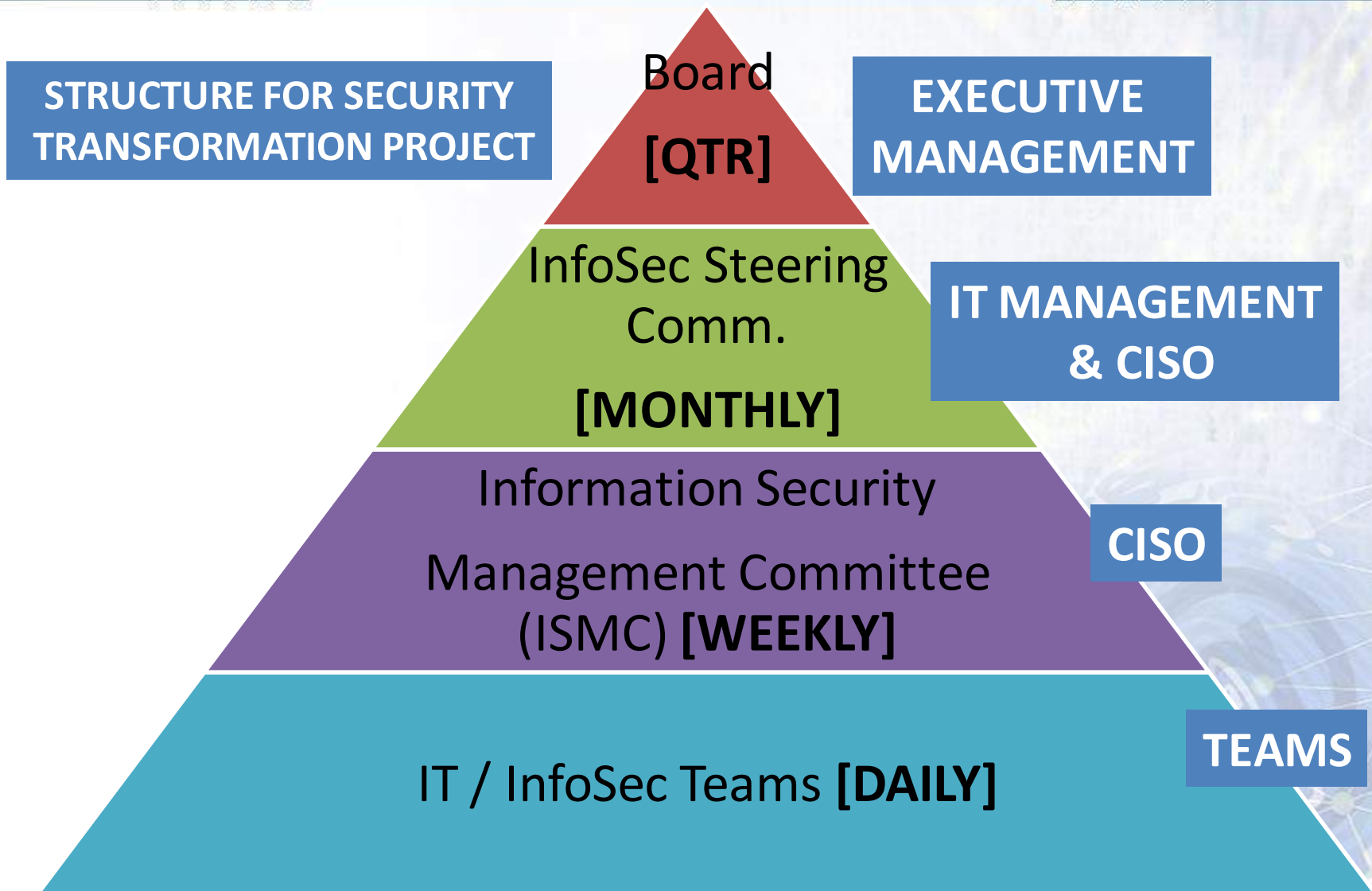
TYPICAL ORGANIZATIONAL TIERS AND RESPONSIBILITIES

TIER	RESPONSIBILITY
BOARD (STEERING COMMITTEE)	ORGANIZATIONAL COMMITMENT, APPROVE BUDGET, DIRECT
IT MANAGEMENT (CIO)	REVIEW, MONITOR, PROPOSE
CISO/SECURITY HEAD	PLAN, BUILD, RUN
IT & SECURITY TEAMS	IMPLEMENT/EXECUTE

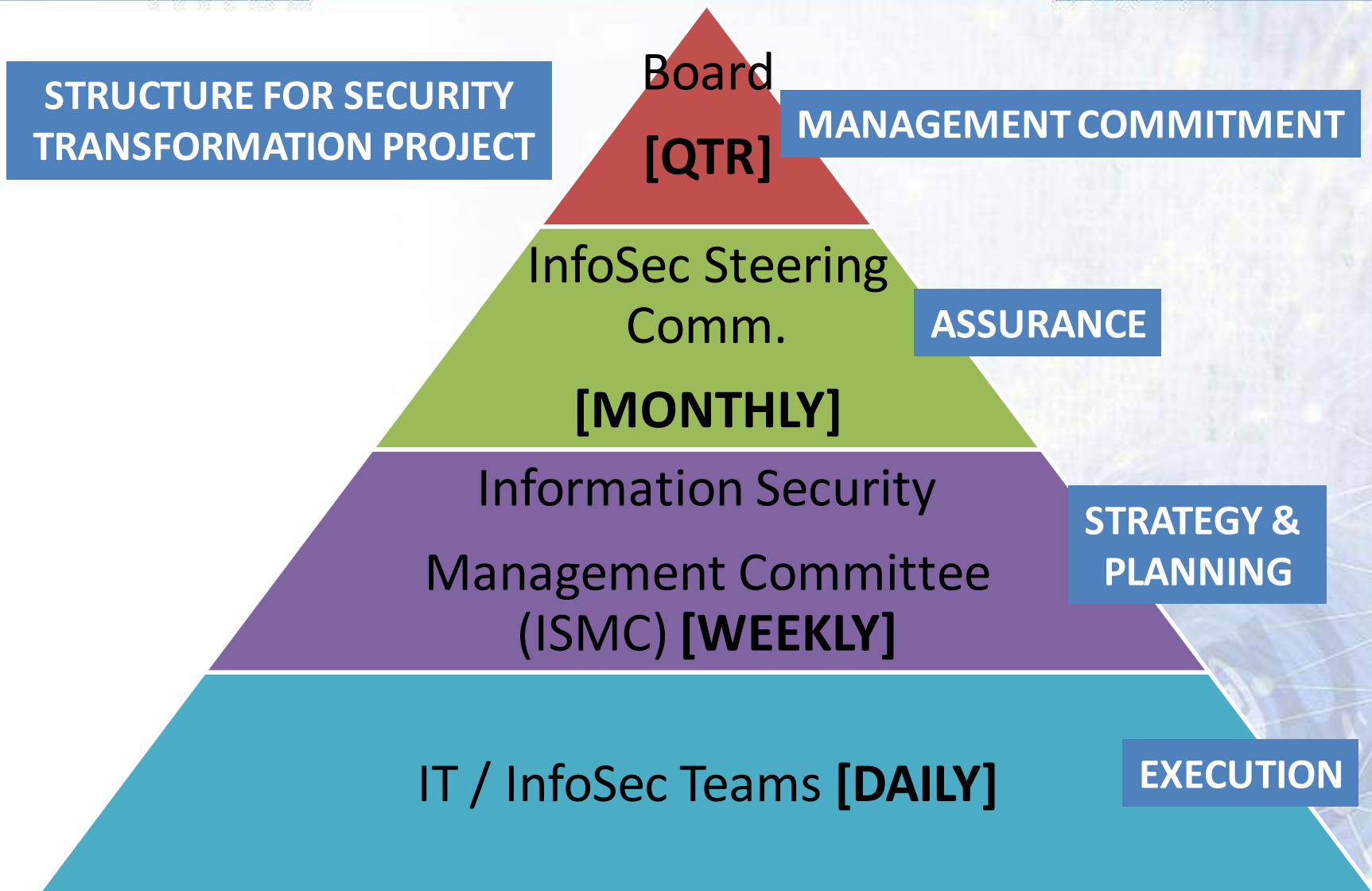
Whose Responsibility Is InfoSec Governance ?

- Based on experience with real Information Security Transformation projects in the Pakistan industry, we have set a more practical structure as shown in the following slides
- Well-suited to drive the Security Transformation project successfully

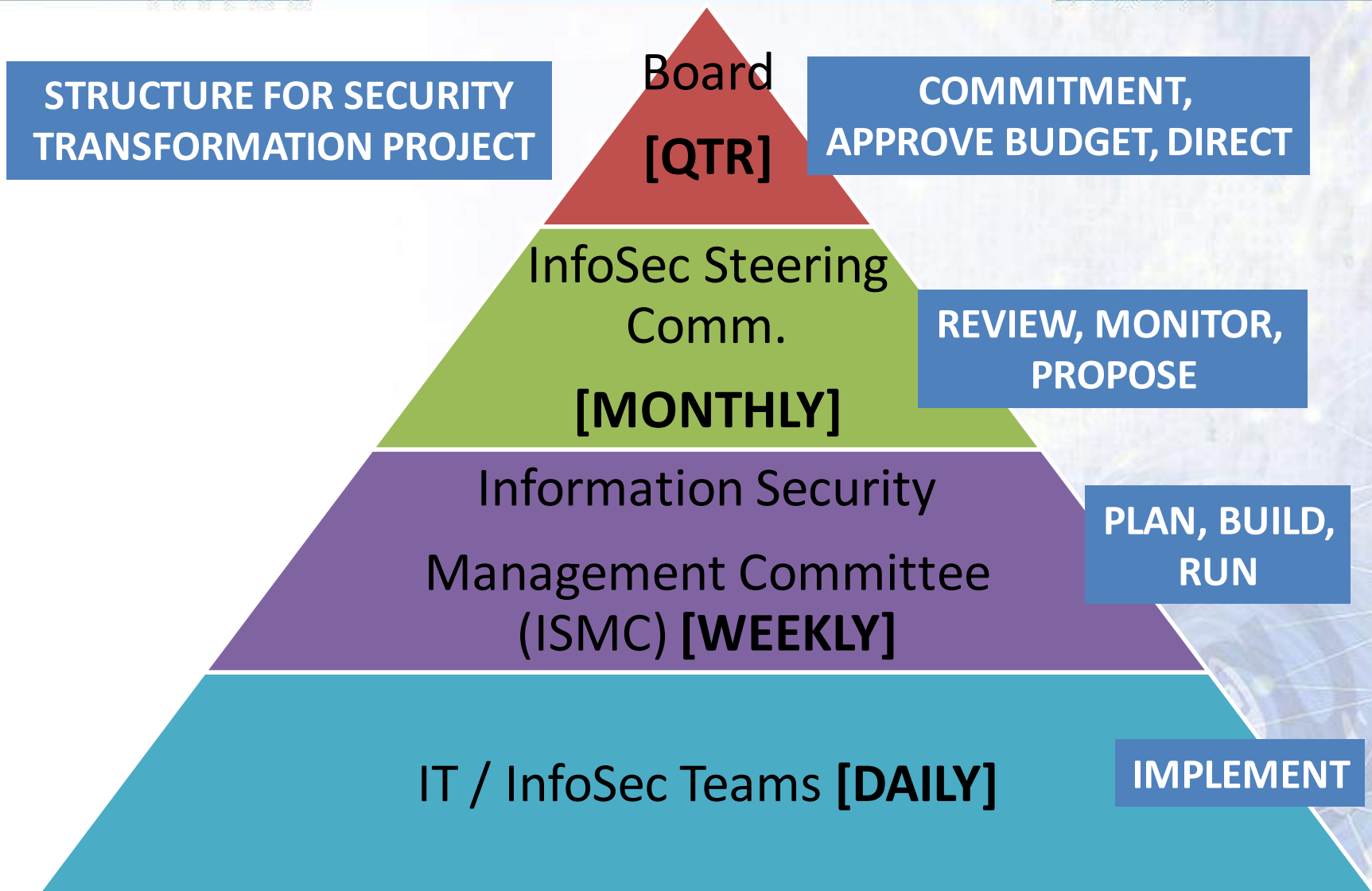
Whose Responsibility Is InfoSec Governance ?



Whose Responsibility Is InfoSec Governance ?



Whose Responsibility Is InfoSec Governance ?



Whose Responsibility Is InfoSec Governance ?

- When working in the practical industry in a market where the security posture is sub-par, we should be open to adopt structures and strategies relevant for such a level of market
- ISACA and other frameworks propose mechanisms that do not always make sense in an unprepared market

END

How Is InfoSec Governance Implemented?

- Lets have a look at the Information Security governance building blocks

How Is InfoSec Governance Implemented?

INITIAL GOVERNANCE BUILDING BLOCKS



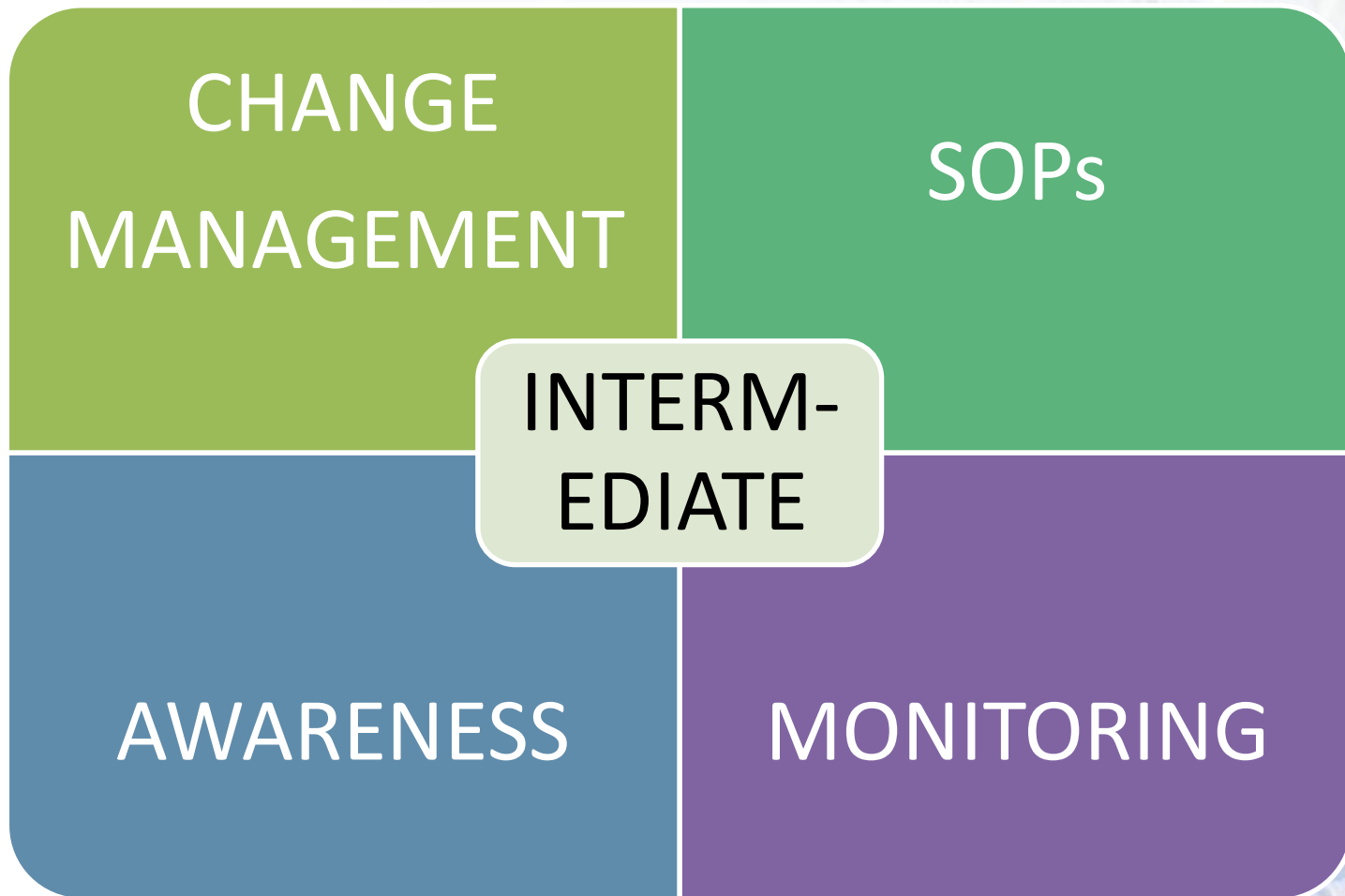
How Is InfoSec Governance Implemented?

INITIAL GOVERNANCE BUILDING BLOCKS

ACTIVITY	RESPONSIBLE	DETAIL
POLICY	DEVELOPED BY CISO SIGNED OFF BY BOARD/EXECUTIVE	SETS THE SCOPE, OBJECTIVES, FRAMEWORK, REQUIREMENTS
RESPONSIBILITY & AUTHORITY	BOARD/EXECUTIVE	ASSIGNS ROLES, RESPONSIBILITIES, AND AUTHORITY FOR INFOSEC PROGRAM
RESOURCE ASSIGNMENT & PRIORITY SETTING	BOARD/EXECUTIVE	ALLOCATION OF RESOURCES AND BUDGET FOR THE INFOSEC FUNCTIONS
PERIODIC REVIEW	BOARD/EXECUTIVE	MONITOR AND REVIEW THAT THE GOALS OF THE INFOSEC PROGRAM ARE BEING MET

How Is InfoSec Governance Implemented?

INTERMEDIATE GOVERNANCE BUILDING BLOCKS



How Is InfoSec Governance Implemented?

INTERMEDIATE GOVERNANCE BUILDING BLOCKS

ACTIVITY	RESPONSIBLE	DETAIL
CHANGE MANAGEMENT	IT MANAGEMENT	ESTABLISHING AND ENFORCING A CHANGE MANAGEMENT PROCESS
SOPs	IT MANAGEMENT	DEVELOPING STANDARD OPERATING PROCEDURES BASED ON ACTUAL PRACTICE
AWARENESS	CISO/ SECURITY TEAMS	CONDUCTING SECURITY AWARENESS TRAINING
MONITORING/ REVIEW	IT MANAGEMENT	GAUGING THE PERFORMANCE AND PROGRESS OF THE INFOSEC PROGRAM AGAINST AGREED PROJECT PLAN/MILESTONES

How Is InfoSec Governance Implemented?

MATURE GOVERNANCE BUILDING BLOCKS



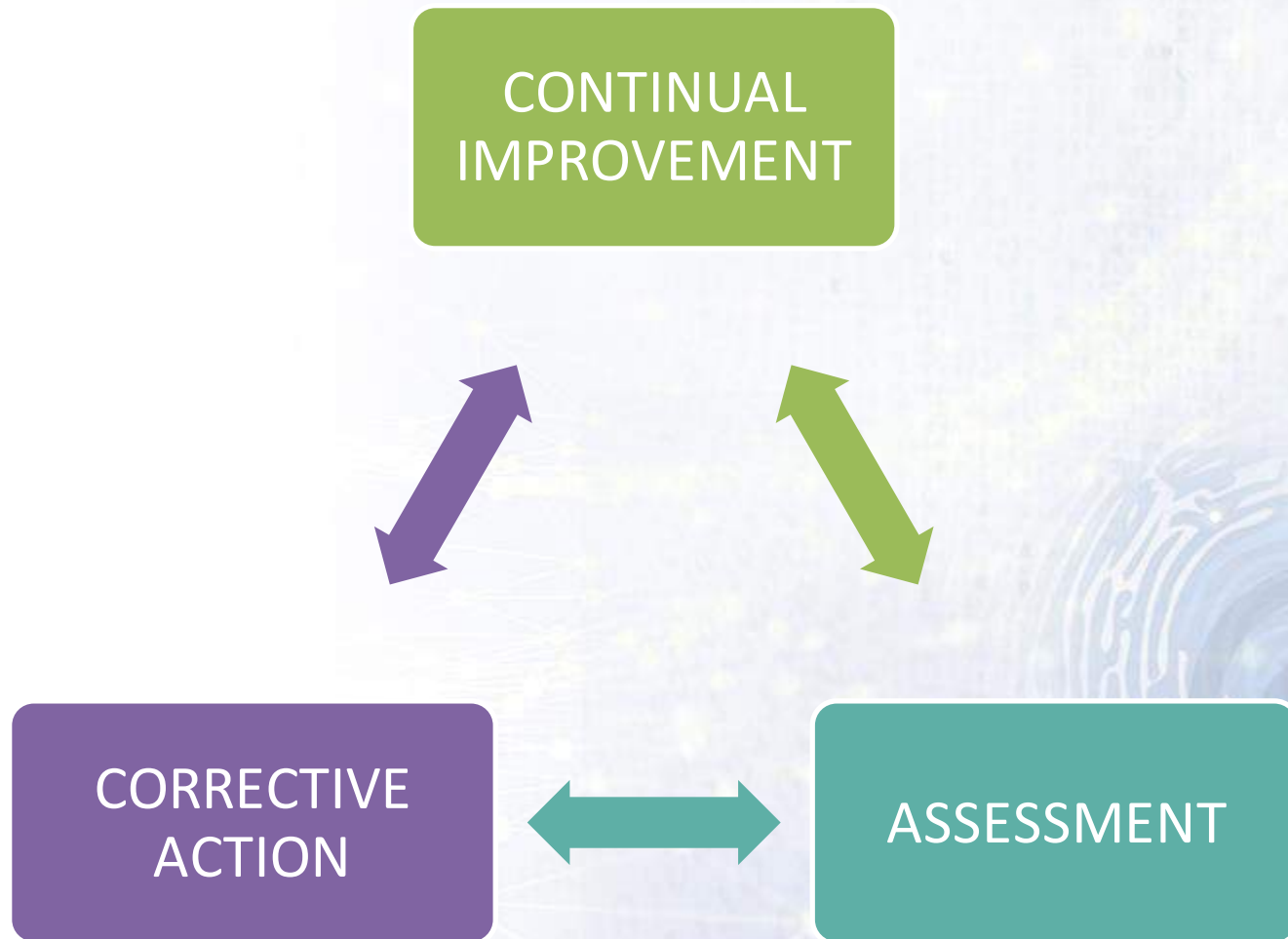
How Is InfoSec Governance Implemented?

MATURE GOVERNANCE BUILDING BLOCKS

ACTIVITY	RESPONSIBLE	DETAIL
RISK MANAGEMENT	DRIVEN BY INFOSEC SUPPORTED BY IT MANAGEMENT	RISK ASSESSMENT, RISK TREATMENT & RISK MANAGEMENT LIFECYCLE
INTERNAL AUDIT	INTERNAL AUDIT DEPT, OR INFOSEC	IMPLEMENT PERIODIC AUDIT PROGRAM
INCIDENT MANAGEMENT	IT MANAGEMENT & INFOSEC	INCIDENT MANAGEMENT LIFECYCLE

How Is InfoSec Governance Implemented?

CONTINUAL IMPROVEMENT CYCLE



How Is InfoSec Governance Implemented?

CONTINUAL IMPROVEMENT CYCLE

ACTIVITY	RESPONSIBLE	DETAIL
CONTINUAL IMPROVEMENT	BOARD/ EXECUTIVE	CONTINUAL STEPS FOR THE EFFECTIVENESS OF INFOSEC PROGRAM
CORRECTIVE ACTIONS	IT MANAGEMENT / INFOSEC	CORRECTIVE ACTIONS FOR NON-CONFORMITIES AND GAPS
THIRD-PARTY ASSESSMENTS	BOARD/INFOSEC	CONDUCT THIRD-PARTY ASSESSMENTS SUCH AS VA/PT, GAP ANALYSIS

How Is InfoSec Governance Implemented?

- Information Security governance can quickly become a challenge as governance is considered an intangible
 - How do you achieve governance?
 - When do you know you have achieved it?
 - How you drive process and documentation in IT?

How Is InfoSec Governance Implemented?

- The key is to align Information Security governance as closely as possible with ISO27001:2013 (ISMS), and to go for crisp clear actions which are always measurable
- Certify against ISO27001:2013 (ISMS) for best-practices implementation

END

How To Build Effective InfoSec Governance ?

- Key success factors:
 - Leadership
 - Strategy
 - Structure
 - Reporting
 - Project management
 - Culture

How To Build Effective InfoSec Governance ?



How To Build Effective InfoSec Governance ?

- Leadership:
 - Executive management role
 - Tone at the top
 - Drive pressing priority
 - Approves budgets and resources
 - Periodic review of progress

How To Build Effective InfoSec Governance ?

- Strategy:
 - How the objectives will be practically achieved while achieving the technical, governance, and performance goals
 - How the organization will gear up and focus for the security transformation

How To Build Effective InfoSec Governance ?

- Structure:
 - What hierarchies, team structures, reporting lines, and resources will come together
 - How will different teams work together to achieve the common goals?

How To Build Effective InfoSec Governance ?

- Reporting:
 - What will be reported?
 - What will be the frequency of reports?
 - Who will perform review and assurance?
 - Who will monitor and track progress?

How To Build Effective InfoSec Governance ?

- Project Management:
 - How will an exceptional execution discipline be built ?
 - How will milestones and performance be tracked ?
 - How will project management best-practices be utilized?

How To Build Effective InfoSec Governance ?

- Culture:
 - How will an open, cooperative, authentic, and committed culture be built ?
 - How will contention and conflict be eliminated?
 - How will a performance driven culture be promoted?

How To Build Effective InfoSec Governance ?

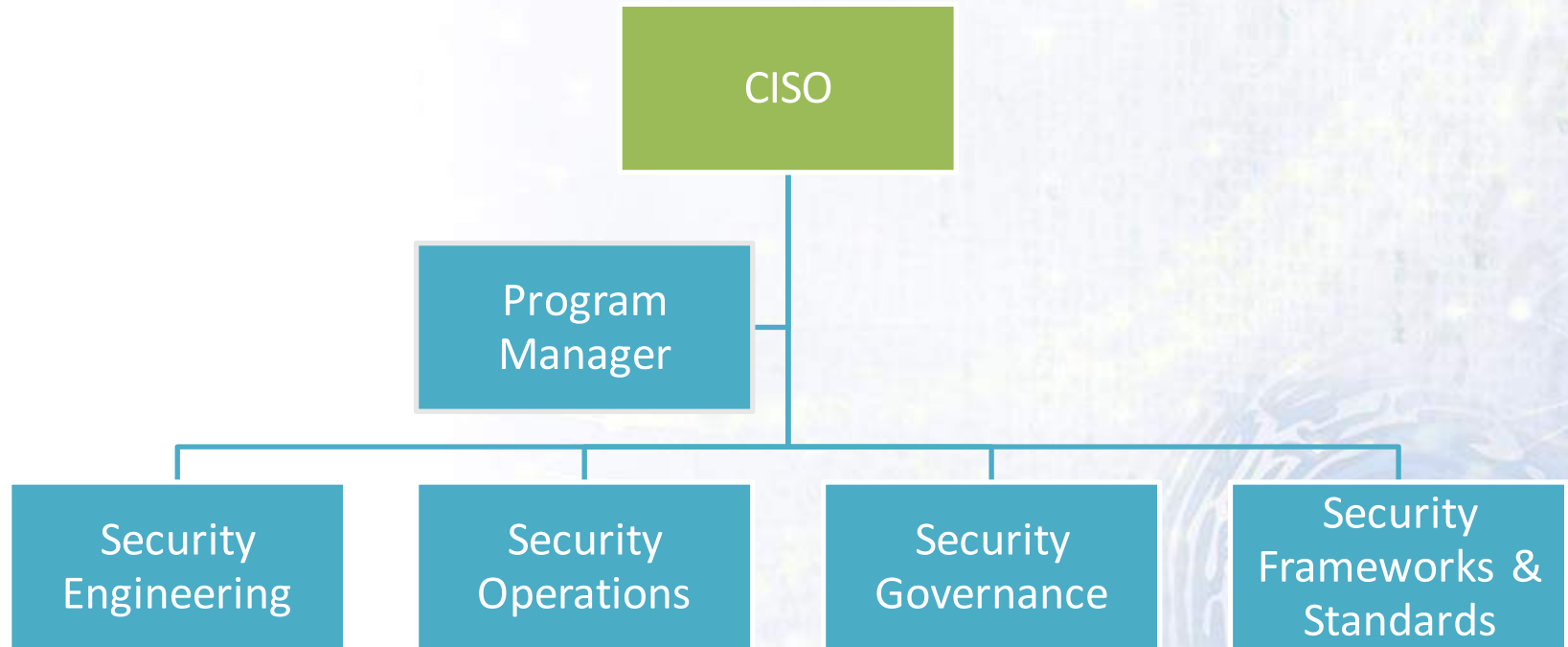
- Building effective information security governance or an effective information security transformation project are based on good management, execution and project management skills

END

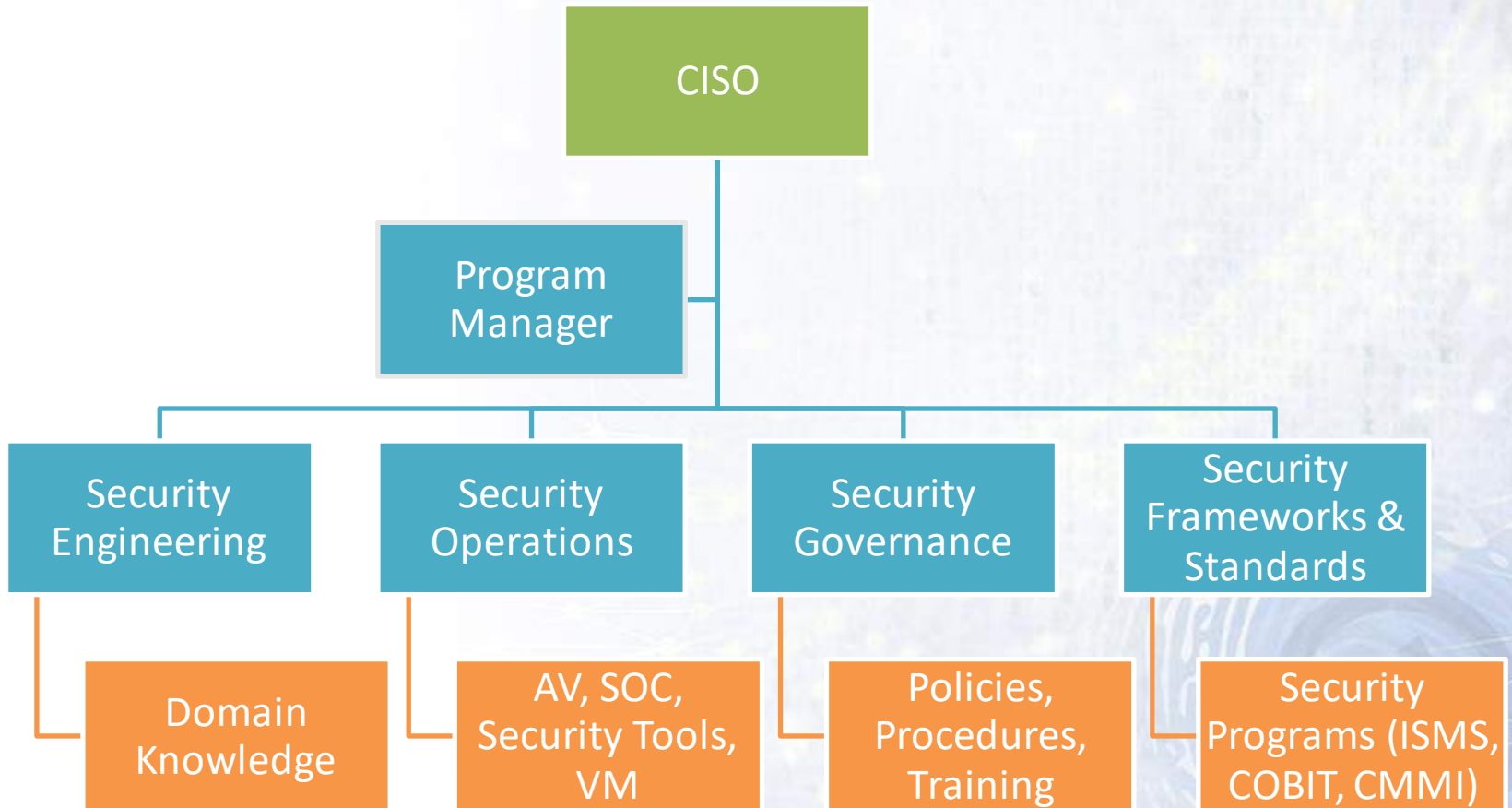
InfoSec Dept Structure (Large-Sized Org)

- Lets look at the recommended structure for a large organization

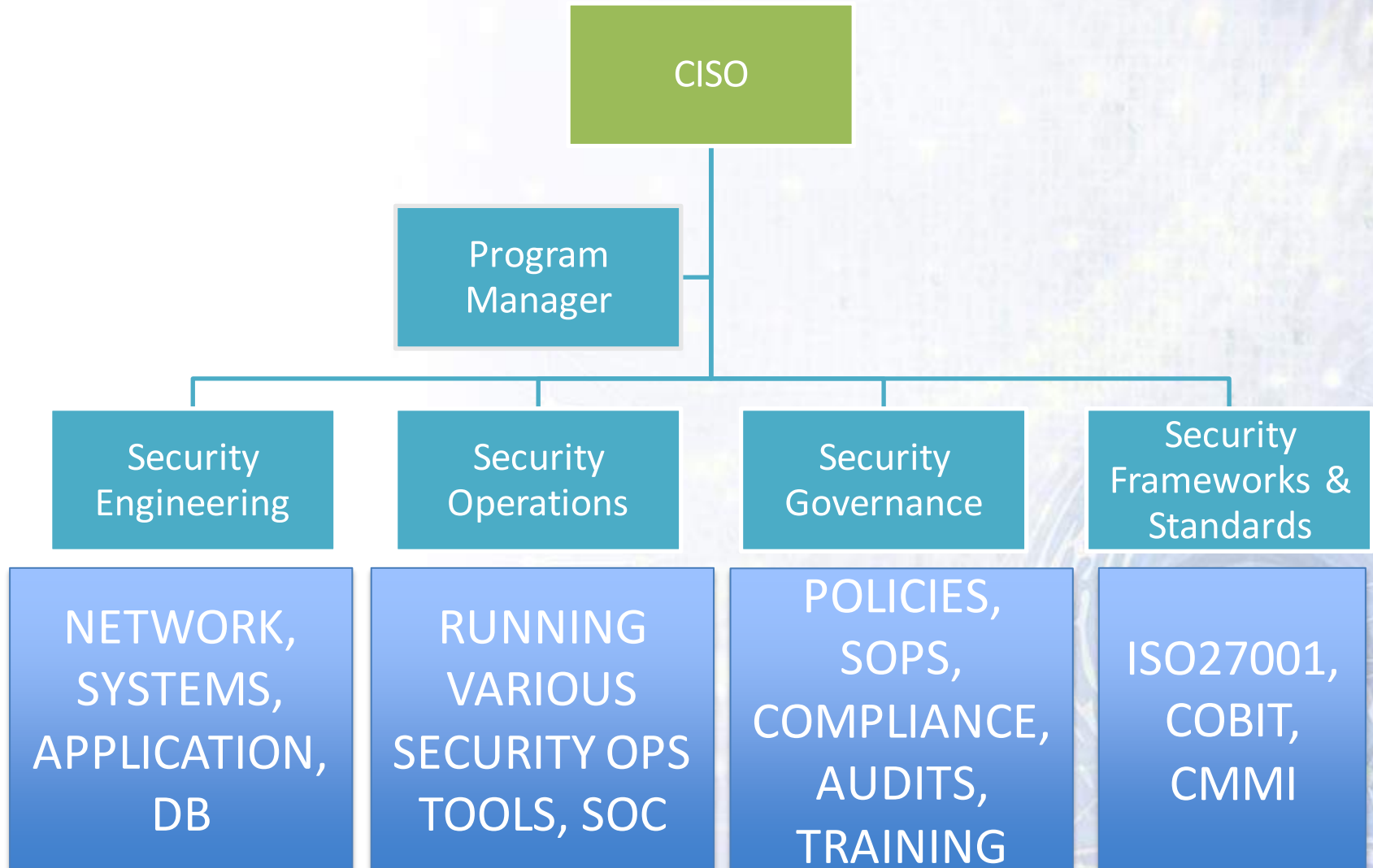
InfoSec Dept Structure (Large-Sized Org)



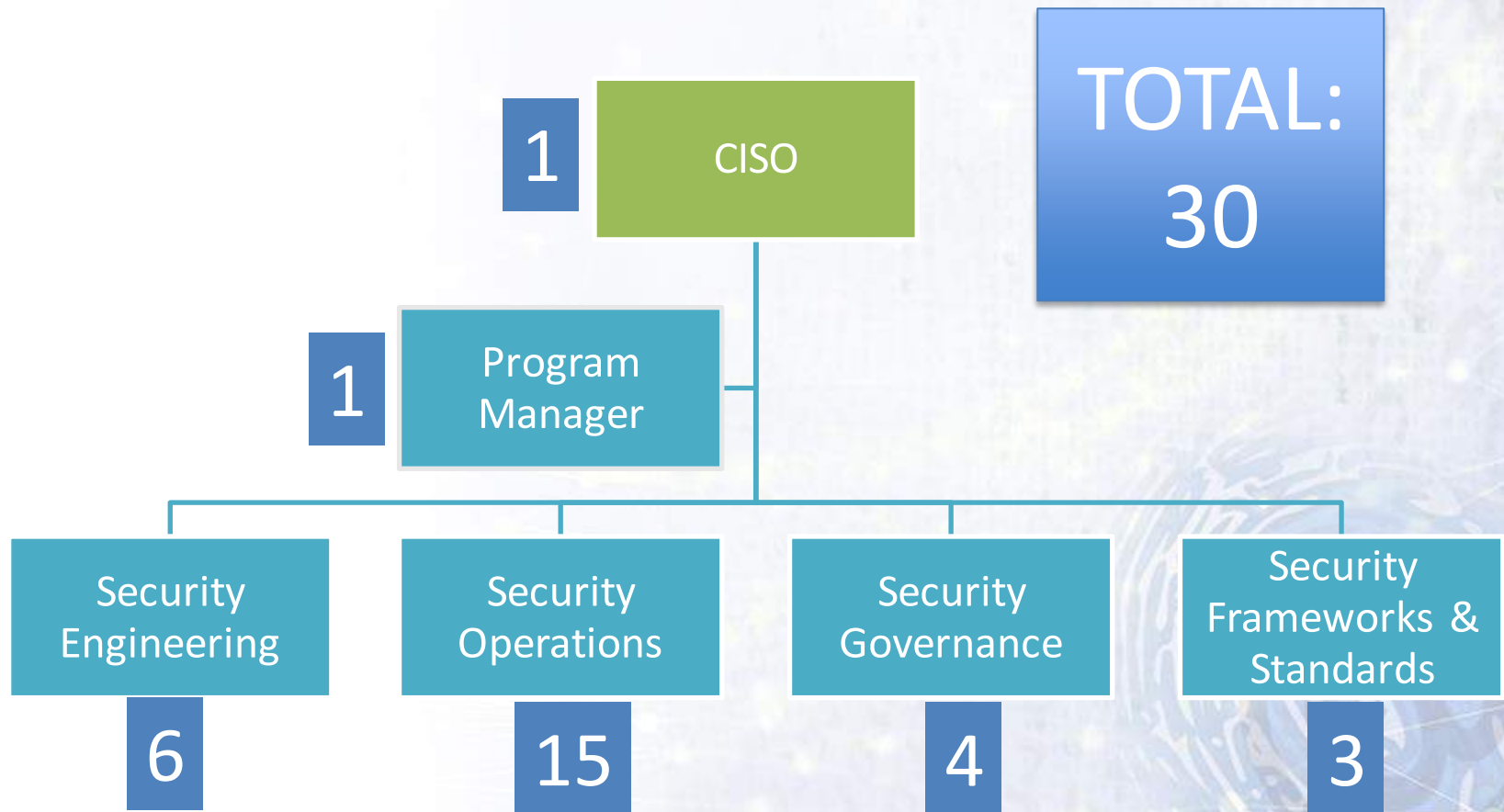
InfoSec Dept Structure (Large-Sized Org)



InfoSec Dept Structure (Large-Sized Org)



InfoSec Dept Structure (Large-Sized Org)



InfoSec Dept Structure (Large-Sized Org)

- A large organization can have an Infosec team ranging between 25-30 staff
- 10% of IT (250 to 300 IT staff)

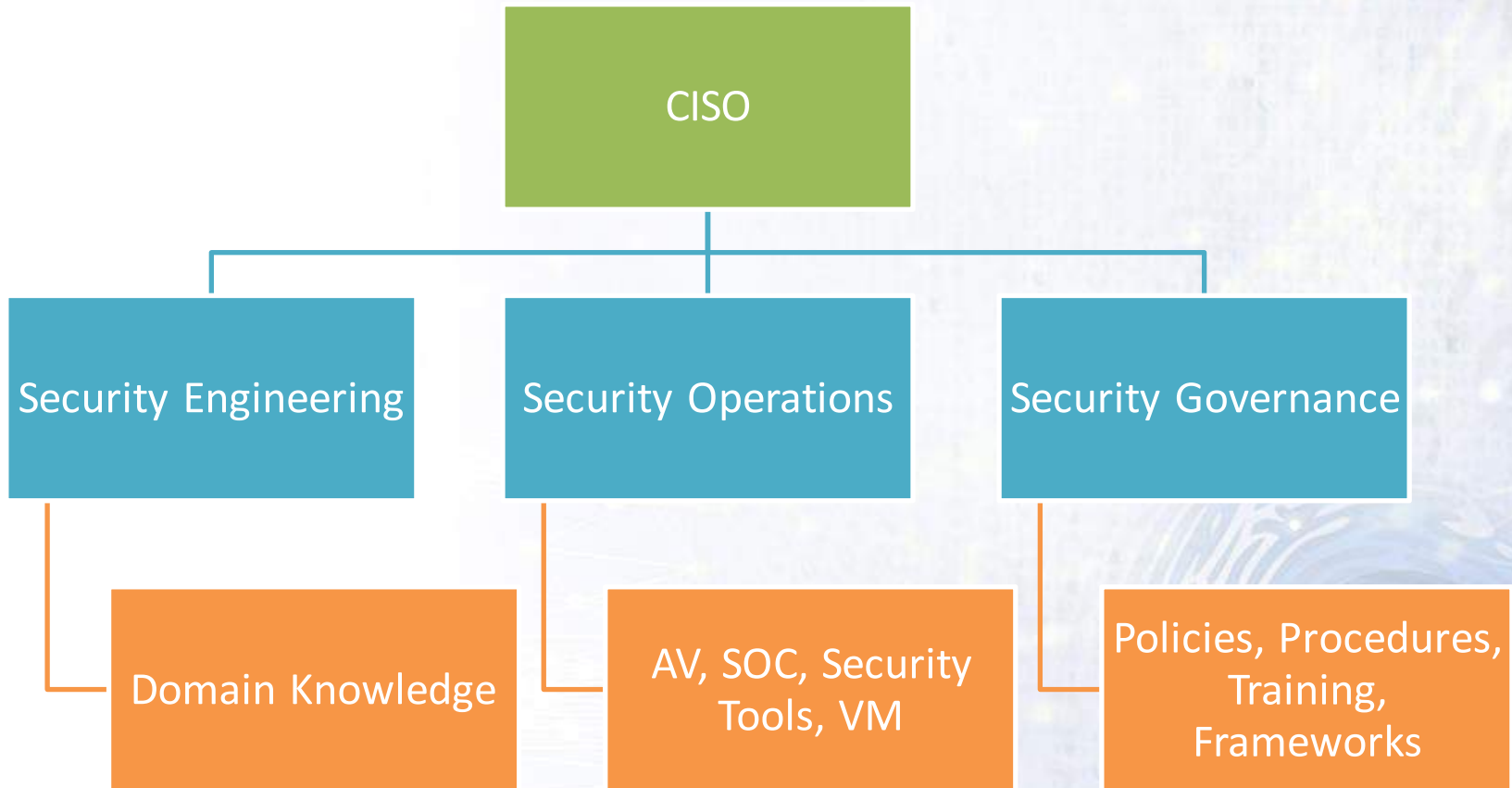
InfoSec Dept Structure (Mid-Sized Org)

- Lets look at the recommended structure for a mid-sized organization

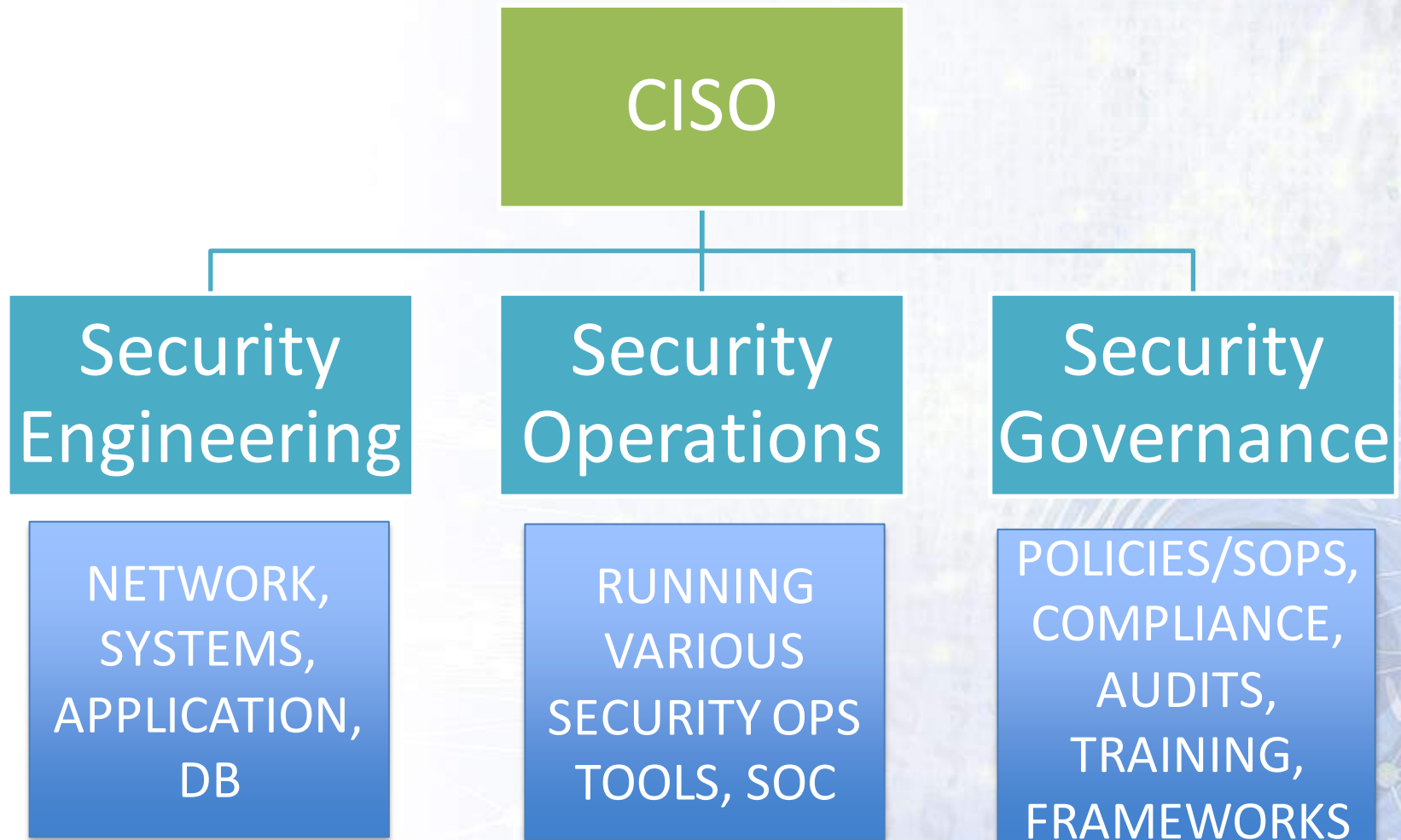
InfoSec Dept Structure (Mid-Sized Org)



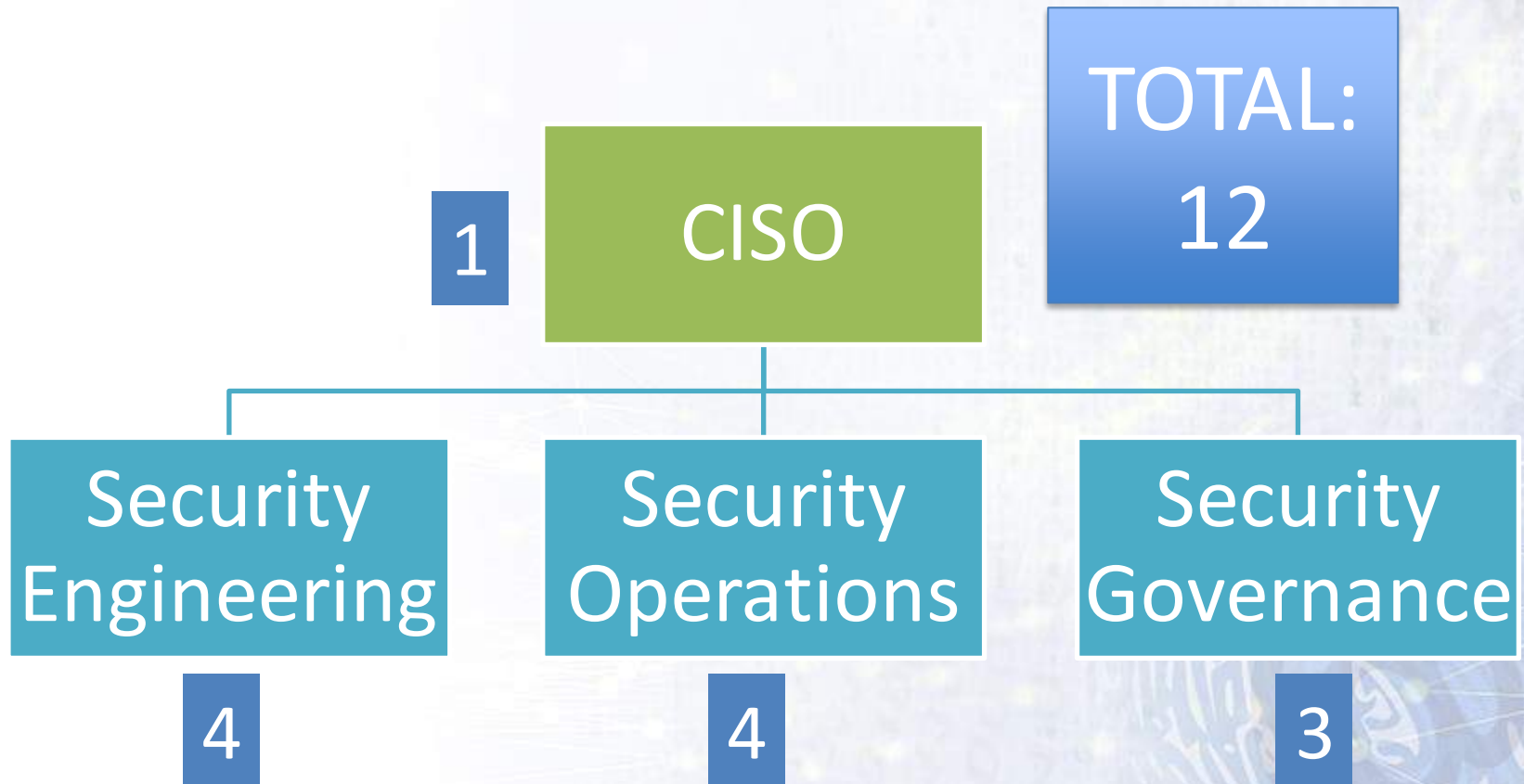
InfoSec Dept Structure (Mid-Sized Org)



InfoSec Dept Structure (Mid-Sized Org)



InfoSec Dept Structure (Mid-Sized Org)



InfoSec Dept Structure (Mid-Sized Org)

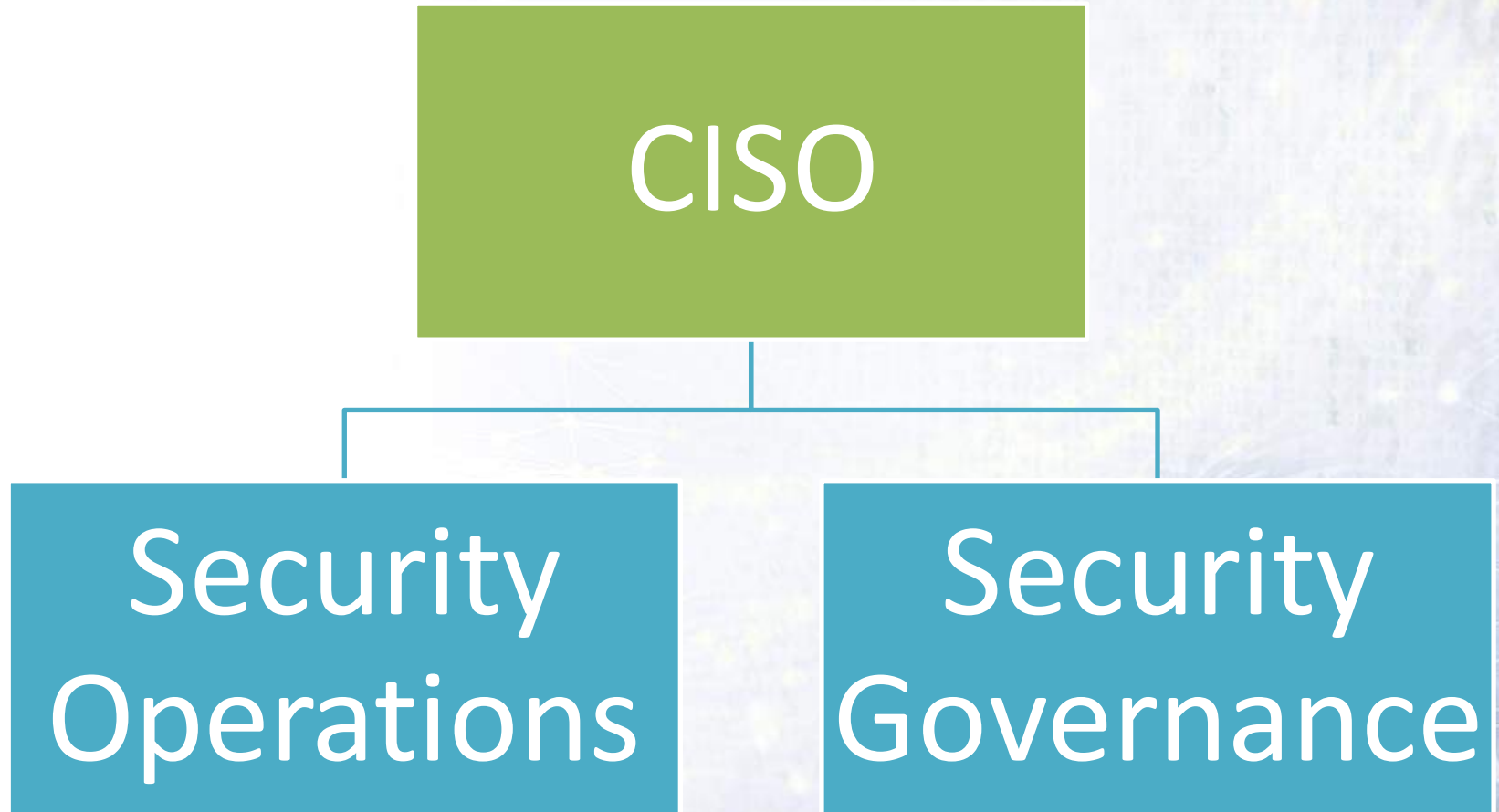
- A mid-sized organization can have an Infosec team ranging between 10-15 staff
- 10% of IT (100 to 150 IT staff)

END

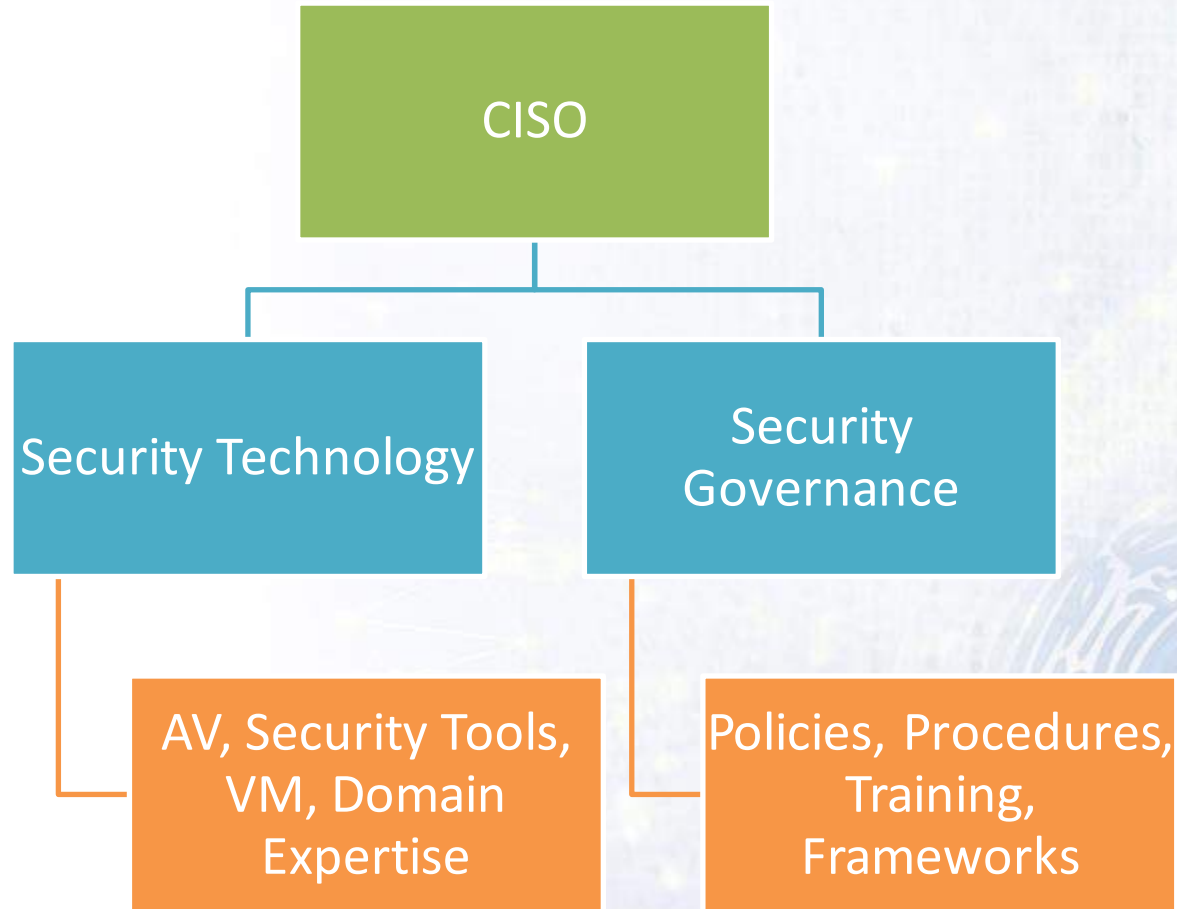
InfoSec Dept Structure (Small Org)

- Lets look at the recommended structure for a small organization

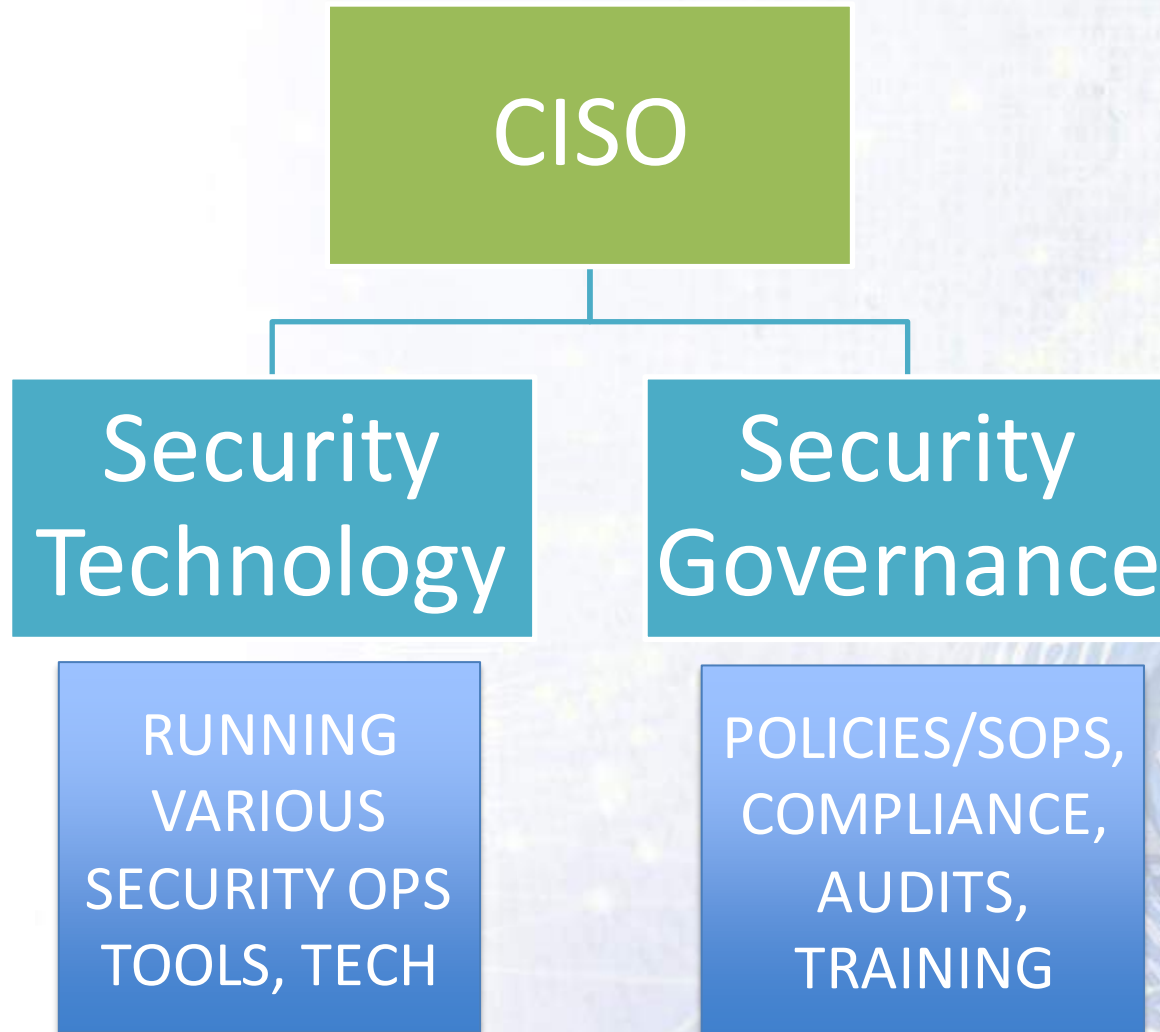
InfoSec Dept Structure (Small Org)



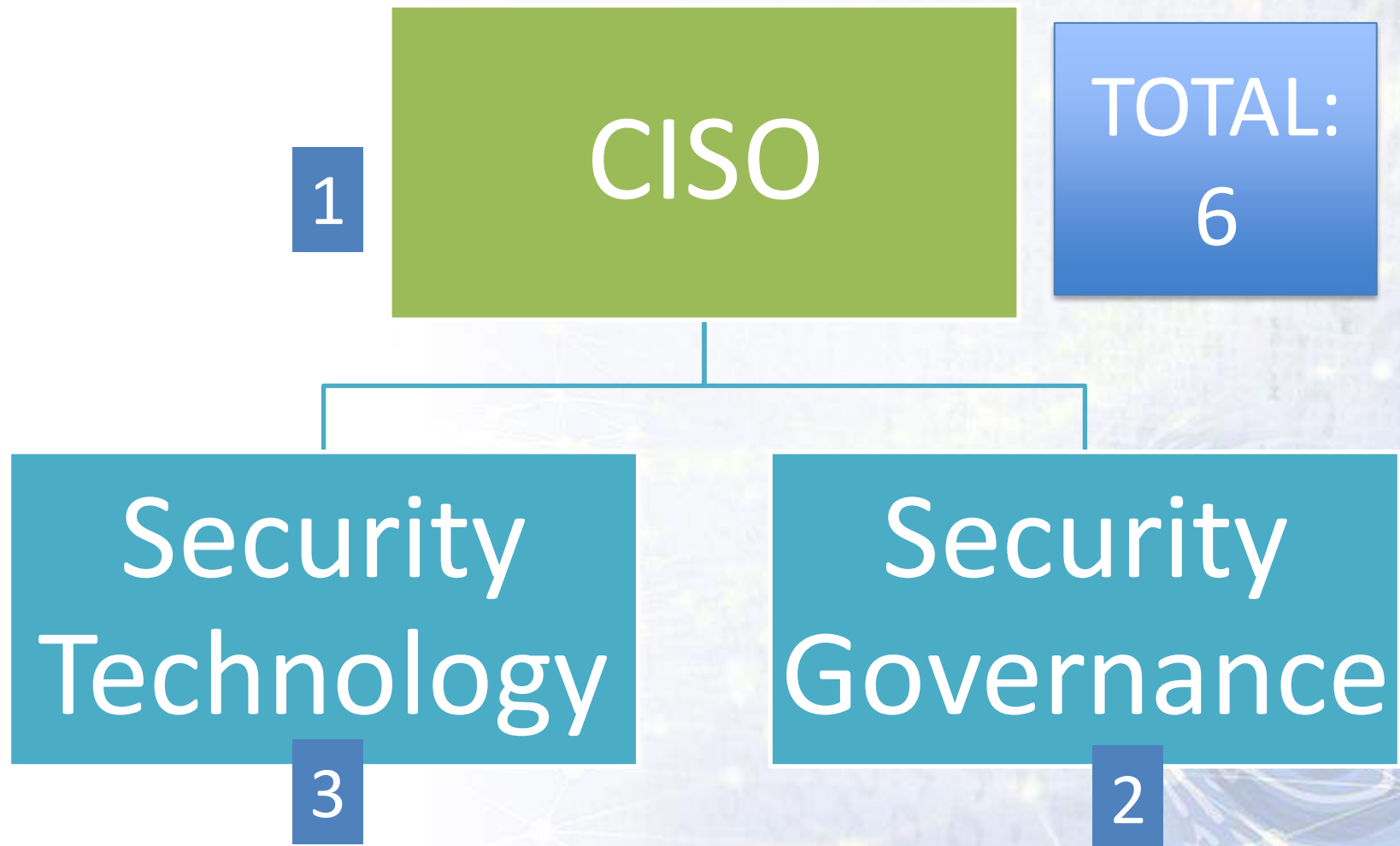
InfoSec Dept Structure (Small Org)



InfoSec Dept Structure (Small Org)



InfoSec Dept Structure (Small Org)



InfoSec Dept Structure (Small Org)

- A small-sized organization can have an Infosec team ranging between 2-4 staff
- 10% of IT (15 to 50 IT staff)

END

Role Of CISO In Driving Infosec Program

- The CISO plays a crucial role in successfully driving the Information Security program
- Two factors:
 - CISO skills
 - Placement in organizational hierarchy

Role Of CISO In Driving Infosec Program



Role Of CISO In Driving Infosec Program

- Leadership & strategy:
 - Good understanding of IT & Information security challenges
 - Experience of driving critical projects in organizations

Role Of CISO In Driving Infosec Program

- Leadership & strategy:
 - Ability to build program strategy, structure, reporting mechanism, and execution discipline to achieve results
 - Ability to work with Board and senior executive management to drive program

Role Of CISO In Driving Infosec Program

- Leadership & strategy:
 - Ability to motivate and communicate security vision to team
 - Ability to infuse credibility & authenticity in IT environment
 - Ability to build team work & cooperation culture

Role Of CISO In Driving Infosec Program

- Technology Domain Knowledge
 - CISOs or security heads usually have 5-10 years experience in IT followed by 3-5 years in Information Security
 - CISOs are typically strong in 2-3 domain areas such as...

Role Of CISO In Driving Infosec Program

- Technology Domain Knowledge
 - ... networking + infrastructure OR software + databases OR software QA & process engineering
 - A good CISO is able to build a good team to cover all major domain areas and all functional reqmts

Role Of CISO In Driving Infosec Program

- Technology Domain Knowledge
 - Having a solid technical base, good CISOs are able to easily build a security competence layer on top of it

Role Of CISO In Driving Infosec Program

- Governance domain knowledge:
 - Working with regulators & compliance
 - Policies & SOPs
 - Frameworks & standards
 - A passion for training & awareness

Role Of CISO In Driving Infosec Program

- Governance domain knowledge:
 - A process oriented mindset to successfully build a strong InfoSec program
 - Ability to balance people, process, and technology

Role Of CISO In Driving Infosec Program

- Good people skills:
 - A CISO requires good people management skills as the security transformation project is all about motivating, directing, and organizing people to achieve a focused goal
 - Personal discipline & commitment

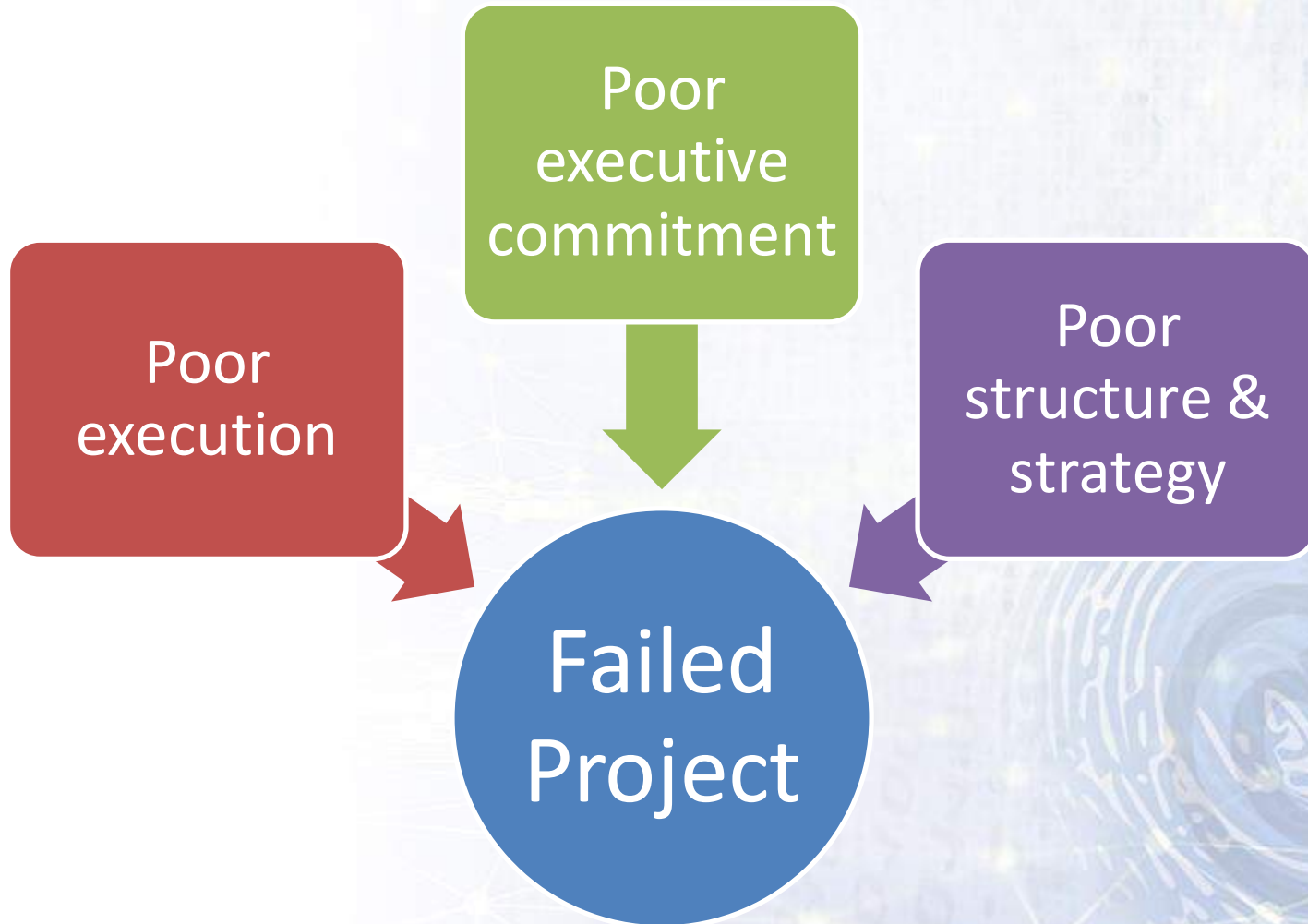
Role Of CISO In Driving Infosec Program

- Placement
 - Within IT
 - Within risk
 - Reporting to board committee

Key Inhibitors For Security Program Failure

- There may be several inhibitors to achieving a successful security transformation project

Key Inhibitors For Security Program Failure



Key Inhibitors For Security Program Failure

- Executive management
 - Allocates budget and approves resources
 - Sets organizational priority & “tone at the top”
 - Even if you start a program without executive management support, it may not last long

Key Inhibitors For Security Program Failure

- Executive management:
 - Periodic reviews by executive management drive the execution in the IT organization
 - Organizational priorities may change quickly if executive management does not sustain its commitment

Key Inhibitors For Security Program Failure

- Strategy & structure:
 - A good or poor strategy & structure will make or break any project, in any discipline, in any organization
 - Addressing the needs and inter-linkages to make the entire machinery work in a streamlined manner

Key Inhibitors For Security Program Failure

- Strategy & structure:
 - Understanding roles of various stakeholders and taking them all along
 - Having sufficient experience to work at various levels of the organization

Key Inhibitors For Security Program Failure

- Execution:
 - All information security projects boil down to strong execution & project management once leadership commitment and strategy/structure issues are addressed

Key Inhibitors For Security Program Failure

- Execution:
 - Allocating tasks to run different phases in parallel & sequentially
 - Prioritizing tasks
 - Tracking progress
 - Reporting dashboards
 - Team/Steering Committee/Board presentations

Key Inhibitors For Security Program Failure

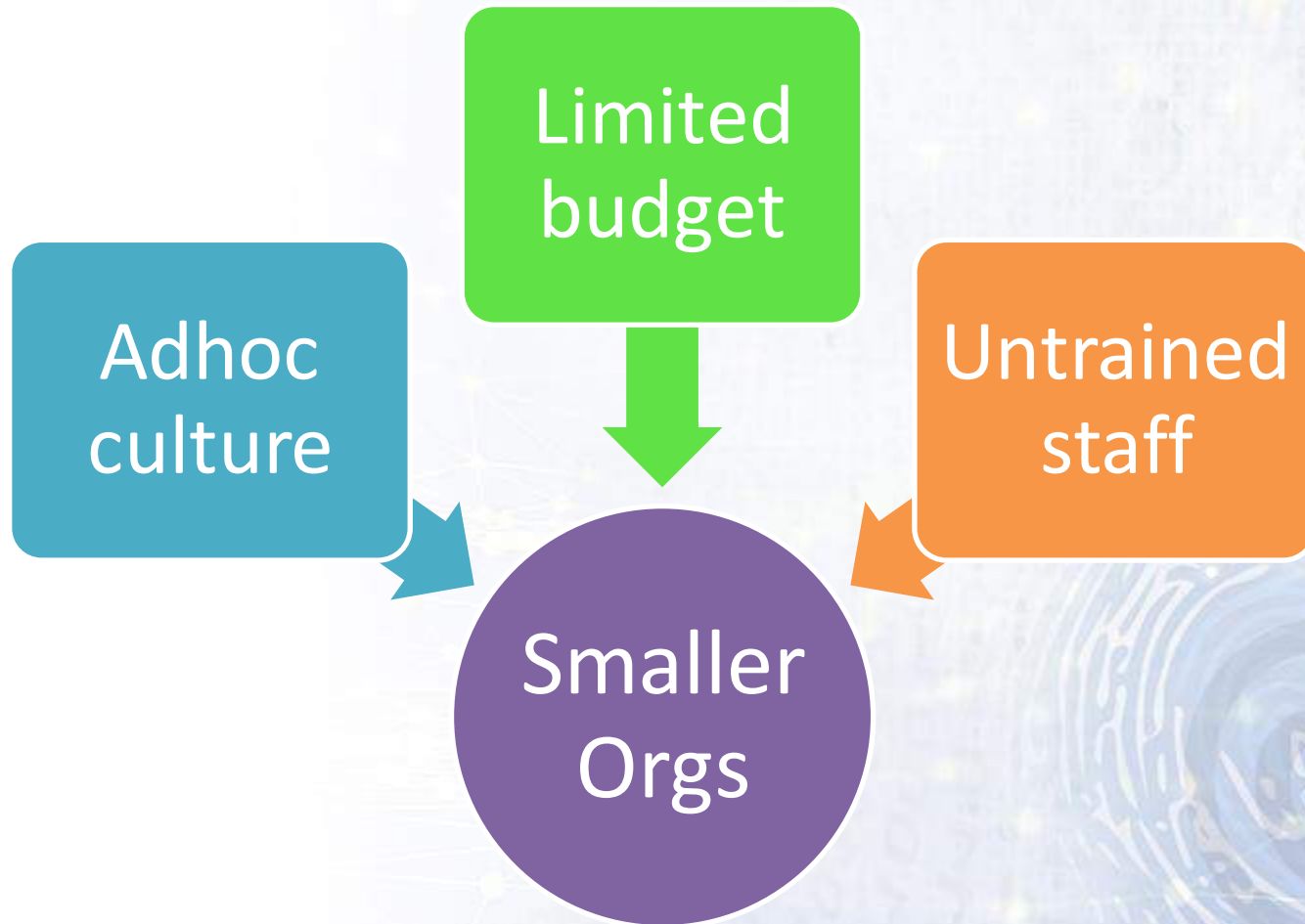
- Failure of the Information Security program will be imminent if any one of these three elements (leadership, strategy/structure, execution) is not adequately addressed

END

InfoSec Strategy For Smaller Organizations

- Smaller & newer organizations face unique challenges which may require a creative approach to implement a successful security transformation program

InfoSec Strategy For Smaller Organizations



InfoSec Strategy For Smaller Organizations

- Limited budget:
 - Limited priority with limited resources
 - **Break up project into phases matching resource allocation & organizational bandwidth available**
 - **Limit scope to 1 location, department, team, or even to 1 application**

InfoSec Strategy For Smaller Organizations

- Limited budget:
 - Consider hiring one competent security or IT member in the team
 - Provide management support and periodic review
 - 12 to 15 months for security transformation

InfoSec Strategy For Smaller Organizations

- Untrained staff:
 - Consider hiring a consultant
 - Train, incentivize, and motivate team
 - Give time to the team to adopt the security culture & processes
 - Periodic management reviews & corrective actions

InfoSec Strategy For Smaller Organizations

- Adhoc culture:
 - Smaller & newer organizations may have a chaotic and adhoc culture
 - Lack of process approach
 - Resources not disciplined for consistent delivery

InfoSec Strategy For Smaller Organizations

- Adhoc culture:
 - Rapidly changing focus and attention span
 - **May be resolved with a good project leader or competent consultant**
 - **Training & setting organizational vision**

InfoSec Strategy For Smaller Organizations

- The leaders of small organizations are usually aware of their organizational capacity and limitations with experience
- Work with the organizational leadership to deploy competent project lead and team members

END

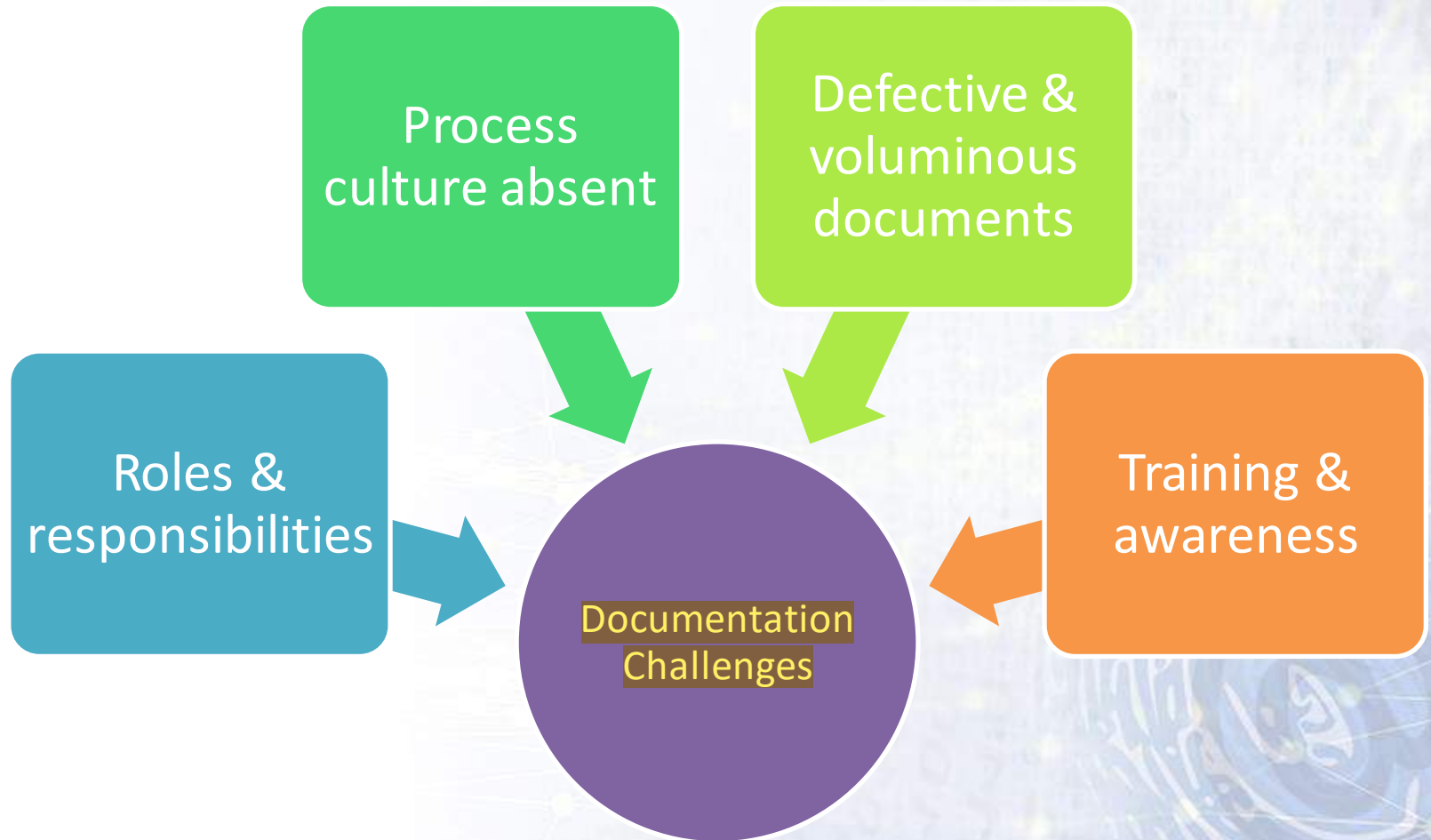
Common Challenges: Security Documentation

- Common challenges with security governance documentation

Common Challenges: Security Documentation

- As we have seen in the previous modules, policies, SOPs, checklists, guidelines, and records are all important parts of the Information Security Management System (ISMS) and are based on documentation usually with an associated process

InfoSec Strategy For Smaller Organizations



Common Challenges: Security Documentation

- Process culture absent:
 - Adhoc culture
 - Rapidly changing priorities
 - Inhibits time & concentration required for documentation
 - Requires executive support to build process oriented culture

Common Challenges: Security Documentation

- Process culture absent:
 - Requires business transformation as well as security transformation as the style in which the organization works needs to be addressed
 - New focus on quality, process, and assurance for results

Common Challenges: Security Documentation

- Defective & voluminous documentation:
 - Effective writing & documentation is a rare skill
 - No one likes to read long, winding, poorly structured documentation
 - **No one likes to read !**

Common Challenges: Security Documentation

- Defective & voluminous documentation:
 - Documentation appetite & organizational maturity
 - **Gradually build organizational appetite for documentation with extremely concise documents**

Common Challenges: Security Documentation

- Defective & voluminous documentation:
 - Documentation has a close relationship with process culture and quality – is your organizational going after the right goals with balance ?

Common Challenges: Security Documentation

- Training & awareness:
 - There may be a fear for documentation, and staff may be unaware or not possessing the skills or experience of documentation
 - Train and raise awareness in a friendly environment
 - Incentivize

Common Challenges: Security Documentation

- Training & awareness:
 - Create working templates which are easily accessible on organizational portal
 - Create how-to videos & FAQs, etc
 - Invest in raising competence & skills of staff

Common Challenges: Security Documentation

- Roles & responsibilities:
 - Is right person working at the right place ?
 - Do key people tasked with security governance & documentation have the right skills and experience to build documentation ?

Common Challenges: Security Documentation

- Roles & responsibilities:
 - Are staff aware of their responsibilities related to security governance documentation ... policies, SOPs, checklists, etc ?
 - Is documentation and process approach part of staff JDs & appraisal ?

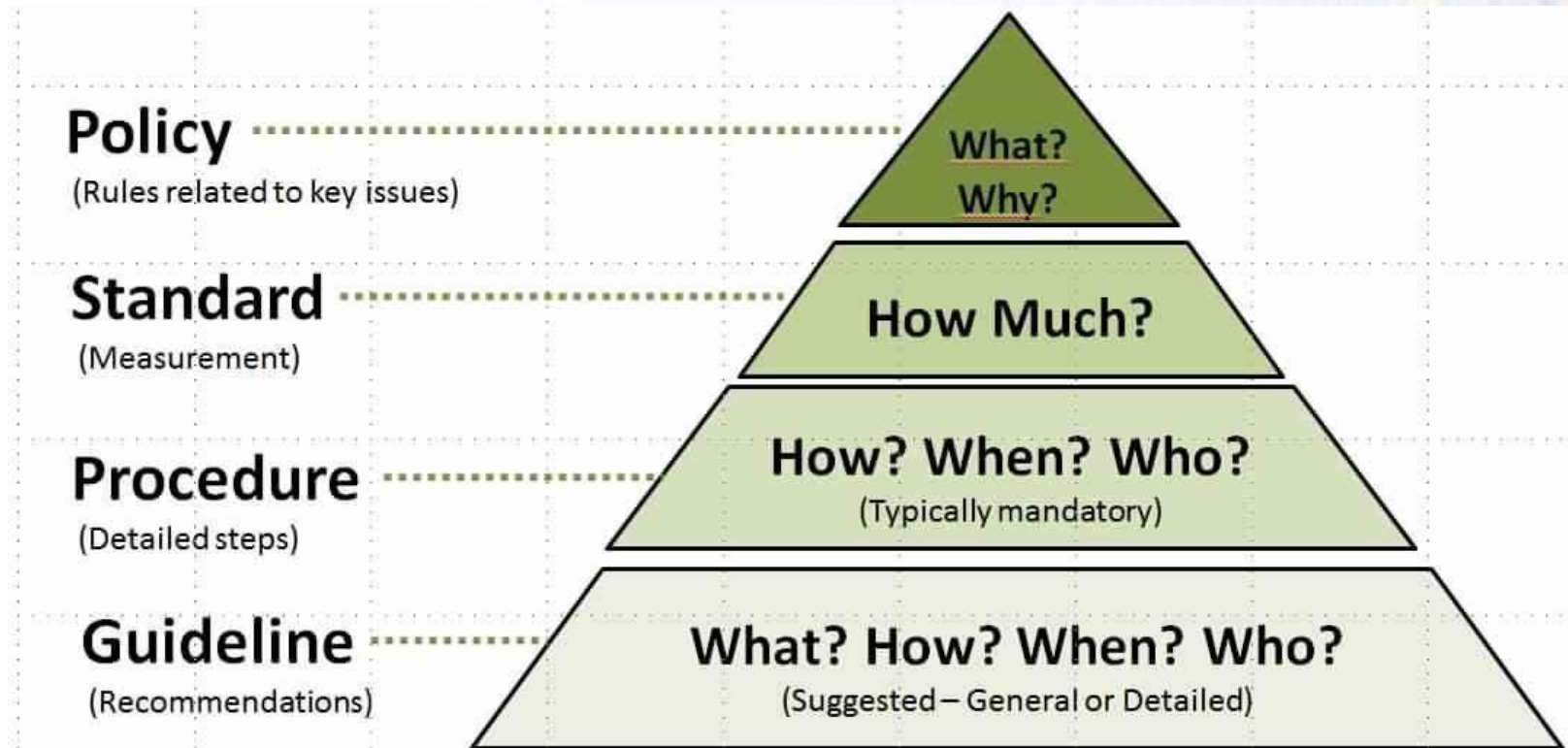
END

Security Documentation: Policies

- Policies
- Standards
- Procedures
- Guidelines

<https://frsecure.com/blog/differentiating-between-policies-standards-procedures-and-guidelines/>

Security Documentation: Policies



<https://frsecure.com/blog/differentiating-between-policies-standards-procedures-and-guidelines/>

Security Documentation: Policies

- Policies

Policies are **formal statements produced and supported by senior management**. They can be organization-wide, issue-specific or system specific. Your organization's policies should reflect your objectives for your information security program.

Security Documentation: Policies

- Policies

Your policies should be like a building foundation; **built to last and resistant to change or erosion.**

Security Documentation: Policies

- Policies
 1. **Driven by business objectives** and convey the amount of risk senior management is willing to accept.

Security Documentation: Policies

- Policies
- 2. Easily accessible and understood by the intended reader

Security Documentation: Policies

- Policies
3. Created with the intent to be **in place for several years and regularly reviewed with approved changes** made as needed.

Security Documentation: Policies

TITLE

DOC #

VERSION #
CLASSIFICATION

DATE

Information Security Policy

EO-ISMS-PL-IS-001

Version 1.1

Public

January 31, 2018

Regulatory Notice: This document contains confidential information proprietary to AEC and may not be reproduced, copied or used for purposes other than its intended use without the prior written consent of AEC. The information in this document is subject to change without notice.

Security Documentation: Policies

HEADER

REVISION HISTORY

REVIEW HISTORY

APPROVED BY

	Information Security Policy	I S M S	
		Classification: Public	Doc. Version: 1.1
		Doc. No: EO-ISMS-PL-IS-001	W&A: January 31, 2018

Revision History

Ver #	Rev Date	Author	Distr Date	Brief Description
1.0	August 18, 2017	Nahid Mahmood	November 10 th , 2017	Initial version
1.1	December 30, 2017		January 31, 2018	Section 1.3, clause number 4 has been completed. Clause xviii has been added for secure software development principles adoption.

Review History

Ver #	Review Date	Reviewed By	Identified Changes
1.0	November 7 th , 2017	CTO	No
1.0	November 9 th , 2017	CEO	No
1.1	January 5, 2018	CTO	No
1.1	January 22, 2018	CEO	No

Approved By

Name	Role	Version
	CTO	1.0 (Initial base line)
	CEO	1.0 (Initial base line)
	CTO	1.1
	CEO	1.1

Security Documentation: Policies

	Information Security Policy	I S M S			
		Classification: Public		Doc. Version: 1.1	
		Doc. No: EC-ISMS-PL-IS-001		Valid: January 31, 2018	

TABLE OF CONTENTS

1. INFORMATION SECURITY POLICY	1
1.1 INTRODUCTION	1
1.2 SCOPE	1
1.3 POLICY DESCRIPTION	1
1.4 POLICY COMMUNICATION	2
1.5 REVIEW	2
1.6 ENFORCEMENT	2

Security Documentation: Policies

INTRODUCTION

SCOPE

POLICY DESCRIPTION

	Information Security Policy	I S M S	
		Classification: Public	Doc Version: 1.1
		Doc No: ISD-0001-PL-02-001	revd. January 21, 2018

1. INFORMATION SECURITY POLICY

1.1 INTRODUCTION

This policy provides primary governance for Information security (IS) management at ABC (PVT) limited. We are committed to maintain and improve the confidentiality, integrity and availability of all information assets of the organization to ensure that regulatory, operational and contractual requirements are fulfilled. To this end, we have established an information security management system that presents a framework to identify the information we need to protect and how we must protect it with major intent of continual improvement in compliance with international best practices required for the defined scope of organization.

1.2 SCOPE

This policy covers establishment and continual improvement of a complete Information Security Management System, including related documentation, implementation and regular monitoring, both through planned audits and through reporting of any security incidents. Adherence to the policy is mandatory for all permanent and contractual employees, consultants and other workers at ABC, including all personnel affiliated with third parties and those who are granted the access to organization's information assets.

1.3 POLICY DESCRIPTION

ABC aims that:

- i. IS objectives must be defined, planned, facilitated, monitored and tracked for completion.
- ii. A comprehensive information security management system shall be developed, implemented and maintained to initiate & control the implementation of information security within the organization.
- iii. All information assets of organization shall be classified to indicate required degree of protection.
- iv. Risks to all corporate assets (tangible/intangible) are assessed and against all risks appropriate treatment is done.
- v. Physical, logical and remote accesses to the information and associated information processing facilities shall be controlled.
- vi. Business information and information processing facilities shall be protected from physical security threats and environmental hazards. Business information and information processing facilities supporting critical or sensitive business activities shall be housed in secure areas with appropriate entry controls.
- vii. Security shall be applied on operating system to restrict unauthorized access to computer resources.
- viii. All information system and the security control systems shall be monitored to detect deviation from access control policy.
- ix. All security requirements related to Human Resource shall be fulfilled.
- x. All resources in terms of technical, tactical and human capital resources in order to define, implement, monitor and improve the information security management system shall be provided adequately.
- xi. Awareness of information security requirements, policies and procedures must be given to all staff.
- xii. Mechanism shall be in place to facilitate the prompt reporting of information security incidents.

Security Documentation: Policies

POLICY COMMUNICATION

REVIEW

ENFORCEMENT

	Information Security Policy	I S M S	
		Classification: Public	Doc Version: 1.1
		Doc No: IS-003-PL-001	revd: January 21, 2010

- xxk. Controls shall be established to prevent and detect viruses and other malicious software.
- xxv. Routine procedures shall be established for taking back-up copies of information and system software, logging events and faults and, where appropriate, monitoring the equipment installed for this purpose (e.g. camera recording and its audit logs, etc.).
- xxv. Information within networks and passing over public networks shall be secured and protected adequately.
- xxvi. Changes to information assets and information processing facilities must be controlled through structured mechanism.
- xxvi. Mechanism shall be established for the handling, storage and disposal of paper and removable media.
- xxvi. Controls shall be established to protect exchanges of information and software.
- xxc. Controls shall be established to mitigate the security risks associated with mobile computing and wireless networks.
- xxc. Security requirements shall be identified and agreed prior to the processing of information system activities.
- xxd. Current capacity shall be monitored, future capacity projections shall be made and operational requirements of new systems shall be established, documented and tested prior to their acceptance and implementation.
- xxd. Redundancies to the information system and information processing facilities shall be defined, implemented and monitored for appropriateness in order to protect critical business processes from the effects of major failure or disasters.
- xxd. Information security continuity shall be planned to avoid information security breaches in case of adverse operational situations.
- xxdv. Information systems shall be audited for compliance.
- xxdv. The complete management system must be reviewed by the management or designated persons on defined frequency for effective measurement and continual improvement of the system.
- xxdv. To ensure the protection of its information assets from all threat, internal or external, deliberate or accidental and natural disasters, ABC ensures the full compliance with the local government laws and the contractual obligations.
- xxvii. Secure software development principles must be adopted.

1.4 POLICY COMMUNICATION

Internal: This policy must be available to all employees through the company's intranet.
External: To all external parties, the uncontrolled copy of will be provided in hard copy format, if and when requested.
Vendor: Contractors: prior to start the activity, the policy will be handed over to all those contractors/vendors who will be given physical / logical access to ABC's premises, information assets, information system and/or information processing facilities.

1.5 Review

This policy has been approved by the company management and shall be reviewed annually for its continuing suitability, adequacy, and effectiveness.

1.6 ENFORCEMENT

The policy is applicable to all employees and all those people who perform work at organization's premises or who is granted the access to organization's information assets. Any employee or contractor

Security Documentation: Policies

1.4 POLICY COMMUNICATION

Internal: This policy must be available to all employees through the company's intranet.

External: To all external parties, the uncontrolled copy of will be provided in hard copy format, if and when requested/required.

Vendors/ Contractors: prior to start the activity, the policy will be handed over to all those contractors/vendors who will be given physical / logical access to ABC's premises, information assets, information system and/or information processing facilities.

1.5 REVIEW

This policy has been approved by the company management and shall be reviewed annually for its continuing suitability, adequacy, and effectiveness.

1.6 ENFORCEMENT

The policy is applicable to all employees and all those people who perform work at organization's premises or who is granted the access to organization's information assets. Any employee or contractor

Security Documentation: Policies

- Policies
- Standards
- Procedures
- Guidelines

<https://frsecure.com/blog/differentiating-between-policies-standards-procedures-and-guidelines/>

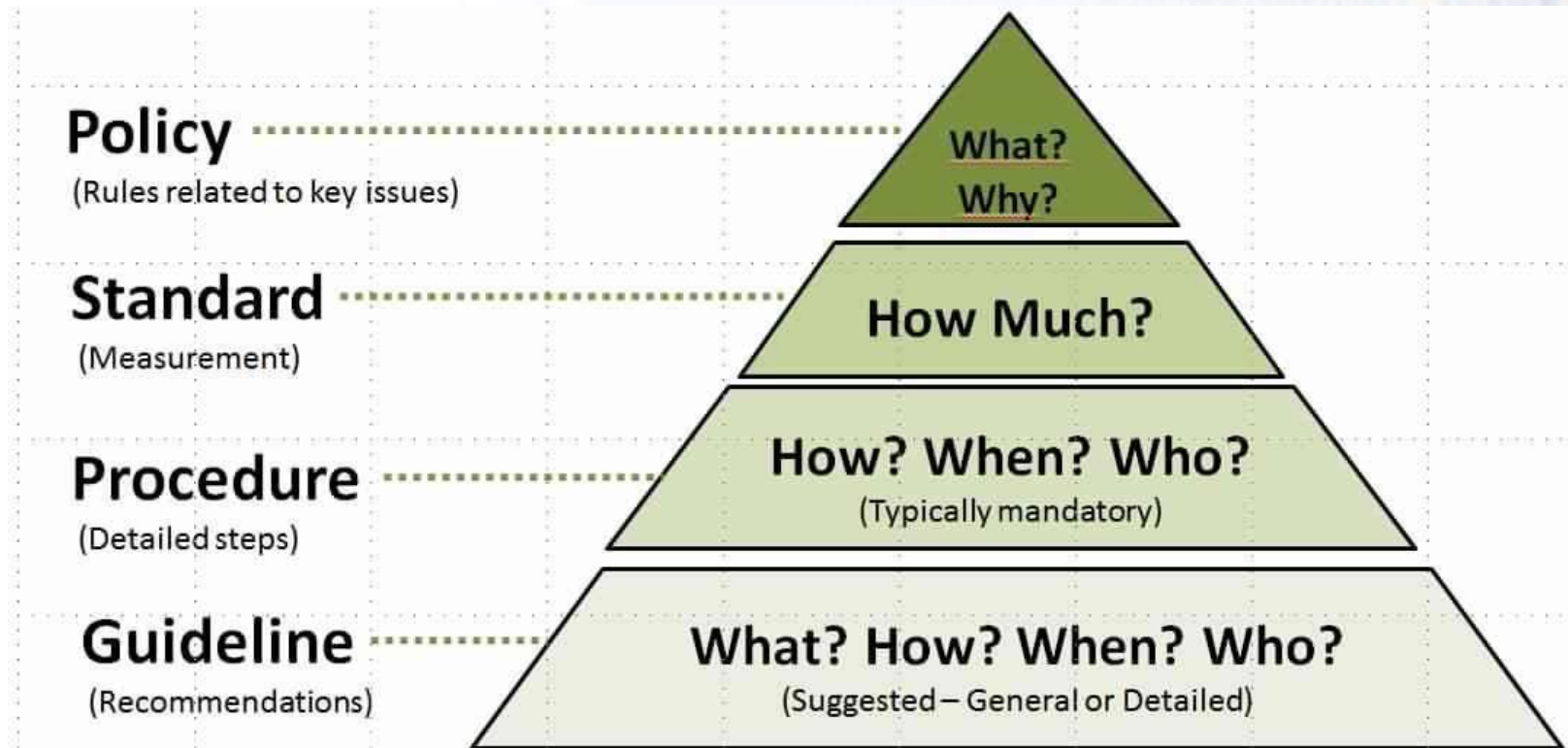
END

Security Documentation: Standards

- Policies
- **Standards**
- Procedures
- Guidelines

<https://frsecure.com/blog/differentiating-between-policies-standards-procedures-and-guidelines/>

Security Documentation: Standards



<https://frsecure.com/blog/differentiating-between-policies-standards-procedures-and-guidelines/>

Security Documentation: Standards

- Standards
Standards are **mandatory actions or rules** that give formal policies support and direction. One of the more difficult parts of writing standards for an information security program is getting a company-wide consensus on what standards need to be in place.

Security Documentation: Standards

- Standards
This can be a time-consuming process but is vital to the success of your information security program.

Security Documentation: Standards

- Standards
 1. Used to indicate expected user behavior. For example, a consistent company email signature.

Security Documentation: Standards

- Standards
 2. Might specify what hardware and software solutions are available and supported.

Security Documentation: Standards

- Standards
3. Compulsory and must be enforced to be effective. (This also applies to policies!)

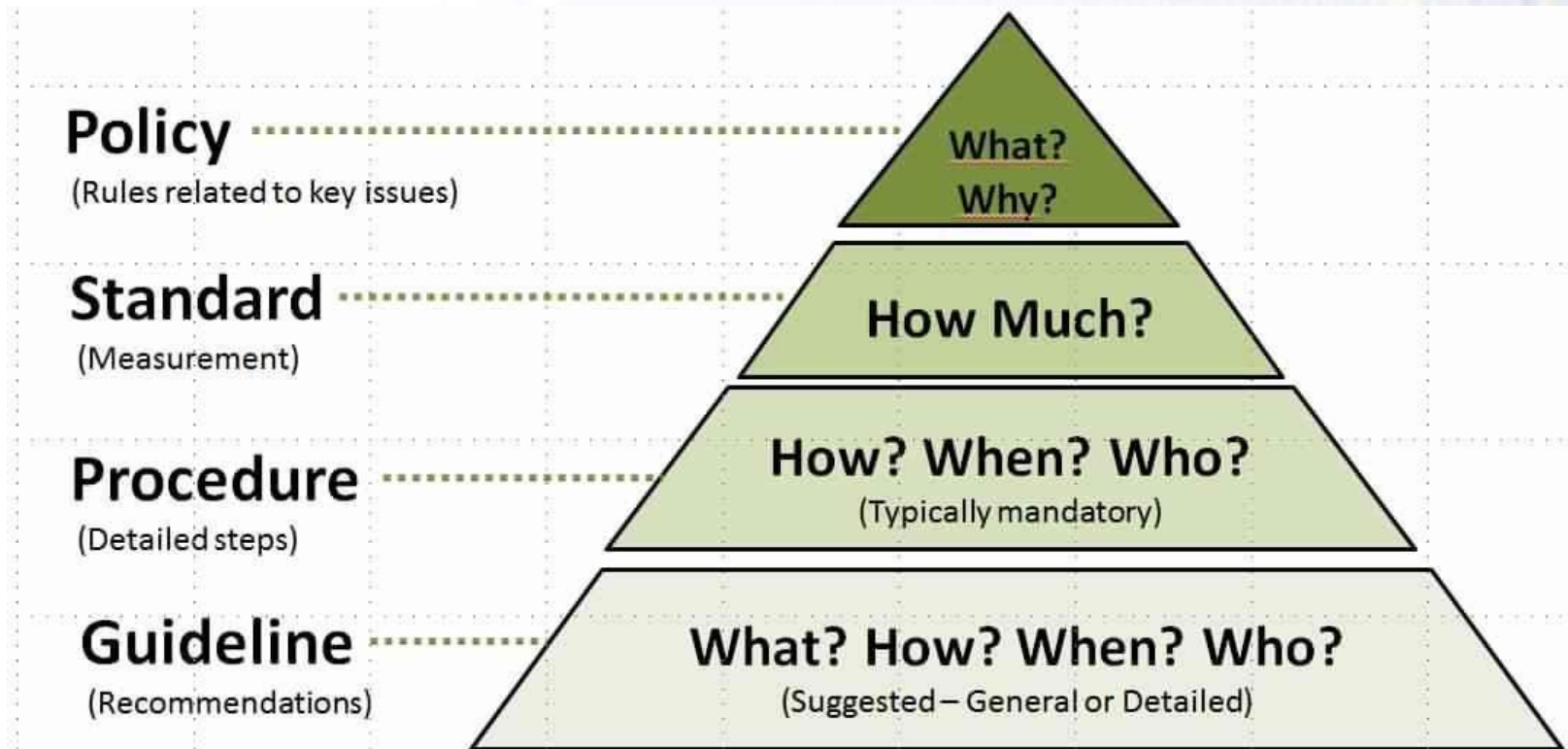
END

Security Documentation: Procedures

- Policies
- Standards
- **Procedures**
- Guidelines

<https://frsecure.com/blog/differentiating-between-policies-standards-procedures-and-guidelines/>

Security Documentation: Procedures



<https://frsecure.com/blog/differentiating-between-policies-standards-procedures-and-guidelines/>

Security Documentation: Procedures

- Procedures

Procedures are **detailed step by step instructions to achieve a given goal or mandate.** They are typically intended for internal departments and should adhere to strict change control processes.

Security Documentation: Procedures

- Procedures

Procedures can be developed as you go. If this is the route your organization chooses to take it's necessary to have comprehensive and consistent documentation of the procedures that you are developing.

Security Documentation: Procedures

- Procedures
 1. Often act as the “cookbook” for staff to consult to accomplish a repeatable process.

Security Documentation: Procedures

- Procedures
 2. **Detailed enough** and yet not too difficult that only a small group (or a single person) will understand.

Security Documentation: Procedures

- Procedures
- 3. **Installing operating systems, performing a system backup, granting access rights to a system and setting up new user accounts are all example of procedures.**

Security Documentation: Procedures

TITLE

DOC #

VERSION

CLASSIFICATION

DATE

Procedure for User Access Management

EO-ISMS-SOP-AM-009

Version 1.0

Company Public

November 13, 2017

Regulatory Notice: This document contains confidential information proprietary to AEC and may not be reproduced, copied or used for purposes other than its intended use without the prior written consent of AEC. The information in this document is subject to change without notice.

Security Documentation: Procedures

HEADER

REVISION HISTORY

REVIEW HISTORY

APPROVED BY

	Procedure for User Access Management	I S M S	
		Classification: Company Public	Doc. Version: 1.0
		Doc. No: EO-ISMS-SOP-AM-009	W.s.f.: November 13, 2017

Revision History

Ver #	Rev Date	Author	Distr Date	Brief Description
1.0	September 24, 2017	Nahil Mahmood	November 13, 2017	Initial Version

Review History

Ver #	Review Date	Reviewed By	Identified Changes
1.0	November 11 th , 2017	CTO	No

Approved By

Name	Role	Version
	CTO	1.0 (Initial base line)

Security Documentation: Procedures

HEADER

TOC

		I S M S	
Procedure for User Access Management		Classification: Company Public	Doc. Version: 1.0
		Doc. No: EO-ISMS-SOP-AM-009	w.e.f.: November 13, 2017

TABLE OF CONTENTS	
1. INTRODUCTION	1
1.1 PURPOSE	1
1.2 SCOPE	1
1.3 REFERENCE POLICY	1
2. PROCEDURE DETAIL	2
2.1 ACCESS CONTROL	2
2.1.1 User registration	2
2.1.2 Access to secure area	3
2.1.3 User deregistration	3
2.1.4 privileged utility programs	3
2.1.5 Access to source code	3
2.1.6 Log access control	4
2.1.7 Review of user access rights and logs	4
2.2 REFERENCE DOCUMENTS	4

Security Documentation: Procedures

HEADER

	Procedure for User Access Management	I S M S	
		Classification: Company Public	Doc. Version: 1.0
		Doc. No: EO-ISMS-SOP-AM-009	w.e.f.: November 13, 2017

PURPOSE

1. INTRODUCTION

1.1 PURPOSE

The purpose of this procedure is to ensure proper assignment and review of user access rights, management of privileges and passwords

SCOPE

1.2 SCOPE

The document defines the procedure to manage the physical and logical access to the information and information processing facilities. The procedure manages the access control to both ABC's employees and third parties.

REF POLIC

1.3 REFERENCE POLICY

Information security policy – clause v, vii

Security Documentation: Procedures

HEADER

PROCEDURE
DETAIL

...ACCESS
CONTROL

		I S M S	
	Procedure for User Access Management	Classification: Company Public	Doc. Version: 1.0
		Doc. No: EO-ISMS-SOP-AM-009	W.e.f.: November 13, 2017

2. PROCEDURE DETAIL

2.1 ACCESS CONTROL

- i. Network team ensures that access to all computers, laptops, networking, communication and security control devices are controlled using secure log on procedures.
- ii. Network team, applications administrators and system/data owner ensure that the access and rights are assigned on need-to-know basis and upon approval of defines authorities.
- iii. Network team ensures that unique IDs are created to access the workstations, laptops, networking equipment, communication devices, CCTV surveillance system and physical access control devices.
- iv. CTO ensures that the generic / default admin rights of network devices and systems are disabled or in case these cannot be disabled, these are assigned to single individual.
- v. The local administration rights of the workstations and laptops are restricted to the network team only
- vi. Special care is taken for the private and personally identifiable information including

Security Documentation: Procedures

- Policies
- Standards
- **Procedures**
- Guidelines

<https://frsecure.com/blog/differentiating-between-policies-standards-procedures-and-guidelines/>

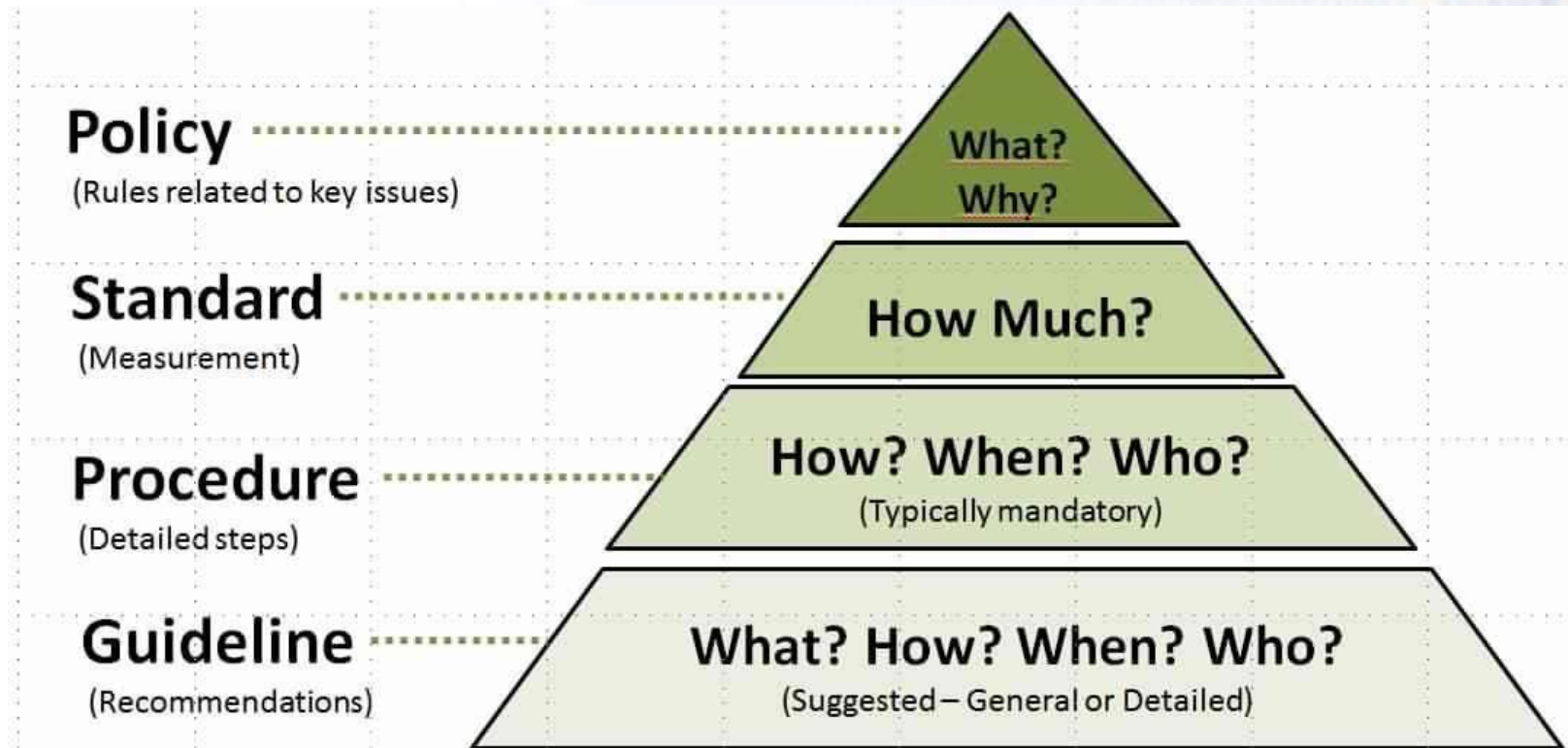
END

Security Documentation: Guidelines

- Policies
- Standards
- Procedures
- **Guidelines**

<https://frsecure.com/blog/differentiating-between-policies-standards-procedures-and-guidelines/>

Security Documentation: Guidelines



<https://frsecure.com/blog/differentiating-between-policies-standards-procedures-and-guidelines/>

Security Documentation: Guidelines

- Guidelines

Guidelines are recommendations to users when specific standards do not apply. Guidelines are designed to streamline certain processes according to what the best practices are.

Security Documentation: Guidelines

- Guidelines

Guidelines, by nature, should be open to interpretation and do not need to be followed to the letter.

Security Documentation: Guidelines

- Guidelines
 1. Are more general vs. specific rules.
 2. Provide flexibility for unforeseen circumstances.
 3. Should NOT be confused with formal policy statements.

END

How To Develop Effective Security Policies

6 Steps To Security Policy Excellence

http://www.infosectoday.com/Articles/Security_Policy_Excellence.htm

How To Develop Effective Security Policies

Purpose Of Policies & Procedures

- Policies and procedures establish **guidelines to behavior and business processes** in accordance with an organization's strategic objectives. While typically developed in response to legal and regulatory requirements, their...

How To Develop Effective Security Policies

Purpose Of Policies & Procedures

- ... primary purpose should be to convey accumulated wisdom on how best to get things done in a **risk-free, efficient and compliant way.**

How To Develop Effective Security Policies

Policy Pitfalls

1. Poorly worded policies
2. Badly structured policies
3. Out-of-date policies
4. Inadequately communicated policies
5. Unenforced policies
6. Lack of management scrutiny

How To Develop Effective Security Policies

Six Steps:

1. Create & Review

Documents must be written using language that is appropriate for the target audience and should spell out the consequences of non-compliance.

Smaller, more manageable documents are easier for an organization to review and update, while also...

How To Develop Effective Security Policies

Six Steps:

1. Create & Review

...being more palatable for the intended recipients.

How To Develop Effective Security Policies

Six Steps:

2. **Distribute**

Organizations need to effectively distribute policies, both new and updated, in a timely and efficient manner. These need to be consistently enforced across an organization.

How To Develop Effective Security Policies

Six Steps:

3. **Achieve Consent**

A process needs to be implemented that monitors users' response to policies. Policy distribution should be prioritised, ensuring that higher risk policies are signed off earlier by users than other lower risk documents.

How To Develop Effective Security Policies

Six Steps:

3. **Achieve Consent**

For example, an organization may want to ensure that a user signs up to their Information Governance policy on the first day that they start employment, whilst having up to two weeks to sign up to the Travel & Expense Policy.

How To Develop Effective Security Policies

Six Steps:

3. **Achieve Consent**

Systems need to in place to grant a user two weeks to process a particular document, after which the system should automatically force the user to process it.

How To Develop Effective Security Policies

Six Steps:

4. Understanding

To monitor and measure staff comprehension and effectiveness of policies and associated documentation, organizations should test all, or perhaps a subset of, users.

How To Develop Effective Security Policies

Six Steps:

4. **Understanding**

Any areas that show weaknesses can be identified and corrected accordingly. Additional training or guidance may be necessary or, if it's the policy that is causing confusion, it can be reworded or simplified.

How To Develop Effective Security Policies

Six Steps:

5. **Auditability**

The full revision history of all documents needs to be maintained as well as who has read what, when & if possible, how long it took; who declined a policy and why. This record should be stored for future reference & may be stored in conjunction with test results.

How To Develop Effective Security Policies

Six Steps:

6. Reporting

To affect change and improve compliance it helps if key performance indicators relating to policy uptake are clearly visible across all levels of an enterprise.

How To Develop Effective Security Policies

Six Steps:

6. **Reporting**

Dashboard visibility of policy uptake compliance by geographical or functional business units helps to consolidate information and highlights exceptions.

END

ISMS:Leading InfoSec Governance Framework

- ISO27001:2013 (ISMS)
 - Specifies the requirements for establishing, implementing, maintaining and continually improving an information security management system
 - Ten short clauses
 - Long annex

ISMS:Leading InfoSec Governance Framework



ISO27001:2013 MANDATORY CLAUSES

Reference		Description
Mandatory	Clause 4	Context of the organization
	Clause 5	Leadership
	Clause 6	Planning
	Clause 7	Support
	Clause 8	Operation
	Clause 9	Performance evaluation
	Clause 10	Improvement

<https://chapters.theiia.org/bermuda/Events/ChapterDocuments/Information%20Security%20Management%20System%20%28ISMS%29%20Overview.pdf>

ISMS:Leading InfoSec Governance Framework



ISO27001:2013 DISCRETIONARY CONTROLS

Reference	Description	Control Total
Discretionary	A5 Information security policies	2
	A6 Organization of information security	7
	A7 Human resource security	6
	A8 Asset management	10
	A9 Access control	13
	A10 Cryptography	2
	A11 Physical and environmental security	15
	A12 Operations security	14
	A13 Communications security	7
	A14 System acquisition, development and maintenance	13
	A15 Supplier relationships	5
	A16 Information security incident management	7
	A17 Information security aspects of business continuity management	4
	A18 Compliance	8

TOTAL: 113

ISMS:Leading InfoSec Governance Framework

- Merits of ISO27001:2013 (ISMS):
 - Exceptional framework with comprehensive coverage of mandatory requirements (clauses 4-10) and discretionary controls (annex)

ISMS:Leading InfoSec Governance Framework

- Merits of ISO27001:2013 (ISMS):
 - Highly beneficial as a framework for security program
 - Covers all domain areas
 - Provides a structure and organized sequence for security controls

ISMS:Leading InfoSec Governance Framework

- Merits of ISO27001:2013 (ISMS):
 - Complements security transformation model as serves as a reference and guideline for activities and controls

ISMS:Leading InfoSec Governance Framework

- **De-merits of ISO27001:2013 (ISMS):**
 - Very broad
 - Generic framework – leaves it to organization how to implement the measures and controls
 - Not suited for orgs that are new to security program

ISMS:Leading InfoSec Governance Framework

- How to best use advantages of ISO27001:2013 (ISMS):
 - Implement security transformational model
 - Cap off security transformation project with ISO27001:2013 (ISMS) certification

ISMS:Leading InfoSec Governance Framework

- How to best use advantages of ISO27001:2013 (ISMS):
 - ISMS as a complementary reference and checklist rather than main framework

Clauses 4-6 Of ISO27001:2013 (ISMS)

- Lets have a look at clauses 4-6

Clauses 4-6 Of ISO27001:2013 (ISMS)



ISO27001:2013 MANDATORY CLAUSES

Reference		Description
Mandatory	Clause 4	Context of the organization
	Clause 5	Leadership
	Clause 6	Planning
	Clause 7	Support
	Clause 8	Operation
	Clause 9	Performance evaluation
	Clause 10	Improvement

<https://chapters.theiia.org/bermuda/Events/ChapterDocuments/Information%20Security%20Management%20System%20%28ISMS%29%20Overview.pdf>

Clauses 4-6 Of ISO27001:2013 (ISMS)

- 4: Context:
 - Understanding org and its context; internal and external issues relevant to its purpose and that affect its ability to achieve intended outcomes of ISMS

Clauses 4-6 Of ISO27001:2013 (ISMS)

- 4: Context:
 - Needs and expectations of interested parties (e.g. legal and regulatory reqmts and contractual obligations)
 - Scope (boundaries); interfaces and dependencies

Clauses 4-6 Of ISO27001:2013 (ISMS)

- 5: Leadership & Commitment
 - Policy & objectives are established and are compatible with strategic direction of org
 - Integrating ISMS into org processes
 - Resources for ISMS available

Clauses 4-6 Of ISO27001:2013 (ISMS)

- 5: Leadership & Commitment
 - Communicating importance
 - Ensuring ISMS achieves intended outcomes
 - Directing & supporting persons
 - Promoting continual improvement

Clauses 4-6 Of ISO27001:2013 (ISMS)

- 5: Leadership & Commitment
 - Assign and communicate roles, responsibilities & authorities

Clauses 4-6 Of ISO27001:2013 (ISMS)

- 6: Planning
 - Address org risks & opportunities & prevent or reduce undesired effects
 - Ensure risk assessment is conducted
 - Identify, analyze, evaluate risks
 - Ensure risk treatment is effective

Clauses 4-6 Of ISO27001:2013 (ISMS)

- 6: Planning
 - Address org risks & opportunities & prevent or reduce undesired effects
 - Ensure risk assessment is conducted
 - Identify, analyze, evaluate risks
 - Ensure risk treatment is effective

Clauses 4-6 Of ISO27001:2013 (ISMS)

- 6: Planning
 - Ensure information security objectives are measurable, communicated
 - For objectives determine what will be done, what resources reqd, who will be responsible, when completed, how to evaluate results

Clauses 7-10 Of ISO27001:2013 (ISMS)

- Lets have a look at clauses 7-10

Clauses 7-10 Of ISO27001:2013 (ISMS)



27001

ISO27001:2013 MANDATORY CLAUSES

Reference		Description
Mandatory	Clause 4	Context of the organization
	Clause 5	Leadership
	Clause 6	Planning
	Clause 7	Support
	Clause 8	Operation
	Clause 9	Performance evaluation
	Clause 10	Improvement

<https://chapters.theiia.org/bermuda/Events/ChapterDocuments/Information%20Security%20Management%20System%20%28ISMS%29%20Overview.pdf>

Clauses 7-10 Of ISO27001:2013 (ISMS)

- 7: Support
 - Org shall provide the resources necessary for the establishment, implementation, maintenance and continual improvement of the ISMS
 - Ensure competence of staff for the ISMS

Clauses 7-10 Of ISO27001:2013 (ISMS)

- 7: Support
 - Awareness related to the policy and ISMS will be ensured among staff
 - Communication mechanisms related to ISMS internal and external to the org

Clauses 7-10 Of ISO27001:2013 (ISMS)

- 7: Support
 - Documentation with appropriate identification, description, format, review & approval mechanism
 - Documentation change control, protection, distribution, retention, & disposal

Clauses 7-10 Of ISO27001:2013 (ISMS)

- 8: Operations
 - Plan, implement, and control processes
 - Control planned changes
 - Outsourced processes controlled
 - Risk assessment and risk treatment & retain documented information

Clauses 7-10 Of ISO27001:2013 (ISMS)

- 9: Performance Evaluation
 - Monitoring, measurement, analysis, and evaluation
 - What needs to be monitored, methods, who will monitor, when to monitor, who shall analyze and evaluate results ?

Clauses 7-10 Of ISO27001:2013 (ISMS)

- 9: Performance Evaluation
 - Internal audit implemented at planned intervals
 - Define audit criteria and scope for each audit
 - Reporting of auditing results
 - Retain auditing docs

Clauses 7-10 Of ISO27001:2013 (ISMS)

- 9: Performance Evaluation
 - Internal audit implemented at planned intervals
 - Define audit criteria and scope for each audit
 - Reporting of auditing results
 - Retain auditing docs

Clauses 7-10 Of ISO27001:2013 (ISMS)

- 9: Management Review
 - Planned intervals
 - Status of actions
 - Changes in external and internal environment
 - Review non-conformities and corrective actions, monitoring & measurement results, audit reports, other

Clauses 7-10 Of ISO27001:2013 (ISMS)

- 10: Improvement
 - Non-conformities and corrective actions
 - Continual improvement

END

ISO27001:2013 Controls Appendix; Part 1

- Lets have a look at the ISO27001:2013 (ISMS) controls (appendix) in more detail

ISO27001:2013 Controls Appendix; Part 1

TOTAL: 114



ISO27001:2013 DISCRETIONARY CONTROLS

Reference	Description	Control Total
Discretionary	A5 Information security policies	2
	A6 Organization of information security	7
	A7 Human resource security	6
	A8 Asset management	10
	A9 Access control	13
	A10 Cryptography	2
	A11 Physical and environmental security	15
	A12 Operations security	14
	A13 Communications security	7
	A14 System acquisition, development and maintenance	13
	A15 Supplier relationships	5
	A16 Information security incident management	7
	A17 Information security aspects of business continuity management	4
	A18 Compliance	8

<https://chapters.theiia.org/bermuda/Events/ChapterDocuments/Information%20Security%20Management%20System%20%28ISMS%29%20Overview.pdf>

ISO27001:2013 Controls Appendix; Part 1

A.5 INFORMATION SECURITY POLICIES

A.5.1 MANAGEMENT DIRECTION FOR INFORMATION SECURITY

Objective: To provide management direction and support for information security in accordance with business requirements and relevant laws and regulations.

A.5.1.1	POLICIES FOR INFORMATION SECURITY	Control: A set of policies for information security shall be defined, approved by management, published and communicated to employees and relevant external parties.
A.5.1.2	REVIEW OF THE POLICIES FOR INFORMATION SECURITY	Control: The policies for information security shall be reviewed at planned intervals or if significant changes occur to ensure their continuing suitability, adequacy and effectiveness.

ISO27001:2013 Controls Appendix; Part 1

A.6 ORGANIZATION OF INFORMATION SECURITY

A.6.1 INTERNAL ORGANIZATION

Objective: To establish a management framework to initiate and control the implementation and operation of information security within the organization.

A.6.1.1	INFOSEC ROLES & RESPONSIBILITIES	Control: All information security responsibilities shall be defined and allocated.
A.6.1.2	SEGREGATION OF DUTIES	Control: Conflicting duties and areas of responsibility shall be segregated to reduce opportunities for unauthorized or unintentional modification or misuse of the organization's assets.

ISO27001:2013 Controls Appendix; Part 1

A.6 ORGANIZATION OF INFORMATION SECURITY

A.6.1 INTERNAL ORGANIZATION

A.6.1.1	INFOSEC ROLES & RESPONSIBILITIES
A.6.1.2	SEGREGATION OF DUTIES
A.6.1.3	CONTACT WITH AUTHORITIES
A.6.1.4	CONTACT WITH SPECIAL INTEREST GROUPS
A.6.1.5	INFORMATION SECURITY IN PROJECT MNGMT

ISO27001:2013 Controls Appendix; Part 1

A.6 ORGANIZATION OF INFORMATION SECURITY

A.6.1.3	CONTACT WITH AUTHORITIES	Control: Appropriate contacts with relevant authorities shall be maintained
A.6.1.4	CONTACT WITH SPECIAL INTEREST GROUPS	Control: Appropriate contacts with special interest groups or other specialist security forums and professional associations shall be maintained.

ISO27001:2013 Controls Appendix; Part 1

A.6 ORGANIZATION OF INFORMATION SECURITY

A.6.2 MOBILE DEVICES & TELEWORKING

A.6.2.1	MOBILE DEVICE POLICY
A.6.2.2	TELEWORKING

A.6.2.2	TELEWORKING	<i>Control:</i> A policy and supporting security measures shall be implemented to protect information accessed, processed or stored at teleworking sites.

ISO27001:2013 Controls Appendix; Part 1

- Gradually you will develop the skill to use the ISO27001:2013 standard quickly and with ease for your benefit...

END

ISO27001:2013 Controls Appendix; Part 2

- Lets continue to have a look at the ISO27001:2013 (ISMS) controls (appendix) in more detail...

ISO27001:2013 Controls Appendix; Part 2



ISO27001:2013 DISCRETIONARY CONTROLS

Reference	Description	Control Total
Discretionary	A5 Information security policies	2
	A6 Organization of information security	7
	A7 Human resource security	6
	A8 Asset management	10
	A9 Access control	13
	A10 Cryptography	2
	A11 Physical and environmental security	15
	A12 Operations security	14
	A13 Communications security	7
	A14 System acquisition, development and maintenance	13
	A15 Supplier relationships	5
	A16 Information security incident management	7
	A17 Information security aspects of business continuity management	4
	A18 Compliance	8

TOTAL: 114

<https://chapters.theiia.org/bermuda/Events/ChapterDocuments/Information%20Security%20Management%20System%20%28ISMS%29%20Overview.pdf>

ISO27001:2013 Controls Appendix; Part 2

A.7 HUMAN RESOURCES SECURITY

A.7.1 PRIOR TO EMPLOYMENT

Objective: To ensure that employees and contractors understand their responsibilities and are suitable for the roles for which they are considered.

ISO27001:2013 Controls Appendix; Part 2

A.7 HUMAN RESOURCES SECURITY

A.7.1 PRIOR TO EMPLOYMENT

A.7.1.1	SCREENING
A.7.1.2	TERMS & CONDITIONS OF EMPLOYMENT

A.7.2 DURING EMPLOYMENT

A.7.2.1	MANAGEMENT RESPONSIBILITIES
A.7.2.2	INFOSEC AWARENESS, EDUCATION & TRAINING
A.7.2.3	DISCIPLINARY PROCESS

ISO27001:2013 Controls Appendix; Part 2

A.7 HUMAN RESOURCES SECURITY

A.7.1.1	SCREENING	<i>Control:</i> Background verification checks on all candidates for employment shall be carried out in accordance with relevant laws, regulations & ethics and shall be proportional to the business requirements, the classification of the information to be accessed and the perceived risks.

ISO27001:2013 Controls Appendix; Part 2

A.7 HUMAN RESOURCES SECURITY

A.7.1.2	TERMS & CONDITIONS OF EMPLOYMENT	<i>Control:</i> The contractual agreements with employees and contractors shall state their and the organization's responsibilities for information security.

ISO27001:2013 Controls Appendix; Part 2

A.7 HUMAN RESOURCES SECURITY

A.7.2 DURING EMPLOYMENT	
A.7.2.1	MANAGEMENT RESPONSIBILITIES
A.7.2.2	INFOSEC AWARENESS, EDUCATION & TRAINING
A.7.2.3	DISCIPLINARY PROCESS

ISO27001:2013 Controls Appendix; Part 2

A.7 HUMAN RESOURCES SECURITY

A.7.2.1	MANAGEMENT RESPONSIBILITIES	<i>Control:</i> Management shall require all employees and contractors to apply information security in accordance with the established policies and procedures of the organization.

ISO27001:2013 Controls Appendix; Part 2

A.7 HUMAN RESOURCES SECURITY

A.7.3 TERMINATION & CHANGE OF EMPLOYMENT

A.7.3.1

TERMINATION OR CHANGE OF
EMPLOYMENT RESPONSIBILITIES

ISO27001:2013 Controls Appendix; Part 2

A.7 HUMAN RESOURCES SECURITY

A.7.3.1	TERMINATION OR CHANGE OF EMPLOYMENT RESPONSIBILITIES	<i>Control:</i> Information security responsibilities and duties that remain valid after termination or change of employment shall be defined, communicated to the employee or contractor and enforced

ISO27001:2013 Controls Appendix; Part 2

- Lets look at asset management in the next module...

END

ISO27001:2013 Controls Appendix; Part 3

- Lets continue to have a look at the ISO27001:2013 (ISMS) controls (appendix) in more detail...

ISO27001:2013 Controls Appendix; Part 3



ISO27001:2013 DISCRETIONARY CONTROLS

Reference	Description	Control Total
Discretionary	A5 Information security policies	2
	A6 Organization of information security	7
	A7 Human resource security	6
	A8 Asset management	10
	A9 Access control	13
	A10 Cryptography	2
	A11 Physical and environmental security	15
	A12 Operations security	14
	A13 Communications security	7
	A14 System acquisition, development and maintenance	13
	A15 Supplier relationships	5
	A16 Information security incident management	7
	A17 Information security aspects of business continuity management	4
	A18 Compliance	8

TOTAL: 114

<https://chapters.theiia.org/bermuda/Events/ChapterDocuments/Information%20Security%20Management%20System%20%28ISMS%29%20Overview.pdf>

ISO27001:2013 Controls Appendix; Part 3

A.8 ASSET MANAGEMENT

A.8.1 RESPONSIBILITY FOR ASSETS	
A.8.1.1	INVENTORY OF ASSETS
A.8.1.2	OWNERSHIP OF ASSETS
A.8.1.3	ACCEPTABLE USE OF ASSETS
A.8.1.4	RETURN OF ASSETS

ISO27001:2013 Controls Appendix; Part 3

A.8 ASSET MANAGEMENT

A.8.1.1	INVENTORY OF ASSETS	<i>Control:</i> Assets associated with information and information processing facilities shall be identified and an inventory of these assets shall be drawn up and maintained.

ISO27001:2013 Controls Appendix; Part 3

A.8 ASSET MANAGEMENT

A.8.1.3	ACCEPTABLE USE OF ASSETS	<i>Control:</i> Rules for the acceptable use of information and of assets associated with information and information processing facilities shall be identified, documented and implemented.

ISO27001:2013 Controls Appendix; Part 3

A.8 ASSET MANAGEMENT

A.8.2 INFORMATION CLASSIFICATION

A.8.2.1	CLASSIFICATION OF INFORMATION
A.8.2.2	LABELLING OF INFORMATION
A.8.2.3	HANDLING OF ASSETS

ISO27001:2013 Controls Appendix; Part 3

A.8 ASSET MANAGEMENT

A.8.2.1	CLASSIFICATION OF INFORMATION	<i>Control:</i> Information shall be classified in terms of legal requirements, value, criticality and sensitivity to unauthorised disclosure or modification.

ISO27001:2013 Controls Appendix; Part 3

A.8 ASSET MANAGEMENT

A.8.2.3	HANDLING OF ASSETS	<i>Control:</i> Procedures for handling assets shall be developed and implemented in accordance with the information classification scheme adopted by the organization.

ISO27001:2013 Controls Appendix; Part 3

A.8 ASSET MANAGEMENT

A.8.3 MEDIA HANDLING

A.8.3.1	MANAGEMENT OF REMOVABLE MEDIA
A.8.3.2	DISPOSAL OF MEDIA
A.8.3.3	PHYSICAL MEDIA TRANSFER

ISO27001:2013 Controls Appendix; Part 3

A.8 ASSET MANAGEMENT

A.8.3.1	MANAGEMENT OF REMOVABLE MEDIA	<i>Control:</i> Procedures shall be implemented for the management of removable media in accordance with the classification scheme adopted by the Organization.

ISO27001:2013 Controls Appendix; Part 3

A.8 ASSET MANAGEMENT

A.8.3.3	PHYSICAL MEDIA TRANSFER	<i>Control:</i> Media containing information shall be protected against unauthorized access, misuse or corruption during transportation

ISO27001:2013 Controls Appendix; Part 3

- Lets look at access control in the next module...

END

ISO27001:2013 Controls Appendix; Part 4

- In this module lets look at ISO27001:2013 (ISMS) related to access control
....

ISO27001:2013 Controls Appendix; Part 4



ISO27001:2013 DISCRETIONARY CONTROLS

Reference	Description	Control Total
Discretionary	A5 Information security policies	2
	A6 Organization of information security	7
	A7 Human resource security	6
	A8 Asset management	10
	A9 Access control	13
	A10 Cryptography	2
	A11 Physical and environmental security	15
	A12 Operations security	14
	A13 Communications security	7
	A14 System acquisition, development and maintenance	13
	A15 Supplier relationships	5
	A16 Information security incident management	7
	A17 Information security aspects of business continuity management	4
	A18 Compliance	8

TOTAL: 114

<https://chapters.theiia.org/bermuda/Events/ChapterDocuments/Information%20Security%20Management%20System%20%28ISMS%29%20Overview.pdf>

ISO27001:2013 Controls Appendix; Part 4

A.9 ACCESS CONTROL

A.9.1 BUSINESS REQUIREMENTS OF ACCESS CONTROL

A.9.1.1	ACCESS CONTROL POLICY
A.9.1.2	ACCESS TO NETWORKS AND NETWORK SERVICES

ISO27001:2013 Controls Appendix; Part 4

A.9 ACCESS CONTROL

A.9.1.2	ACCESS TO NETWORKS & NETWORK SERVICES	<i>Control:</i> Users shall only be provided with access to the network and network services that they have been specifically authorized to use.

ISO27001:2013 Controls Appendix; Part 4

A.9 ACCESS CONTROL

A.9.2 USER ACCESS MANAGEMENT

A.9.2.1	USER REGISTRATION & DE-REGISTRATION
A.9.2.2	USER ACCESS PROVISIONING
A.9.2.3	MNGMT OF PRIVILEGED ACCESS RIGHTS
A.9.2.4	MANAGEMENT OF SECRET AUTHENTICATION INFO OF USERS
A.9.2.5	REVIEW OF USERS ACCESS RIGHTS
A.9.2.6	REMOVAL OR ADJUSTMENT OF ACCESS RIGHTS

ISO27001:2013 Controls Appendix; Part 4

A.9 ACCESS CONTROL

A.9.2.3	MANAGEMENT OF PRIVILEGED ACCESS RIGHTS	<i>Control:</i> The allocation and use of privileged access rights shall be restricted and controlled.

ISO27001:2013 Controls Appendix; Part 4

A.9 ACCESS CONTROL

A.9.2.5	REVIEW OF USER ACCESS RIGHTS	<i>Control:</i> Asset owners shall review users' access rights at regular intervals.

ISO27001:2013 Controls Appendix; Part 4

A.9 ACCESS CONTROL

A.9.2.6	REMOVAL OR ADJUSTMENT OF ACCESS RIGHTS	<i>Control:</i> Access rights of all employees and external party users to info & info processing facilities shall be removed upon termination of their employment, contract or agreement, or adjusted upon change.

ISO27001:2013 Controls Appendix; Part 4

A.9 ACCESS CONTROL

A.9.3 USER RESPONSIBILITIES

A.9.3.1

USE OF SECRET AUTHENTICATION
INFORMATION

ISO27001:2013 Controls Appendix; Part 4

A.9 ACCESS CONTROL

A.9.3.1	USE OF SECRET AUTHENTICATION INFORMATION	<i>Control:</i> Users shall be required to follow the organization's practices in the use of secret authentication information.

ISO27001:2013 Controls Appendix; Part 4

A.9 ACCESS CONTROL

A.9.4 SYSTEM & APPLICATION ACCESS CONTROL

A.9.4.1	INFORMATION ACCESS RESTRICTION
A.9.4.2	SECURE LOG-ON PROCEDURES
A.9.4.3	PASSWORD MANAGEMENT SYSTEM
A.9.4.4	USE OF PRIVILEGED UTILITY PROGRAMS
A.9.4.5	ACCESS CONTROL TO PROGRAM SOURCE CODE

ISO27001:2013 Controls Appendix; Part 4

A.9 ACCESS CONTROL

A.9.4.3	PASSWORD MANAGEMENT SYSTEM	Control: Password management systems shall be interactive and shall ensure quality passwords.
A.9.4.5	ACCESS CONTROL TO PROGRAM SOURCE CODE	Control: Access to program source code shall be restricted.

ISO27001:2013 Controls Appendix; Part 4

- Lets look at cryptography, and physical & environmental security in the next module...

END

ISO27001:2013 Controls Appendix; Part 5

- In this module lets look at ISO27001:2013 (ISMS) related to cryptography, and physical & environmental security...

ISO27001:2013 Controls Appendix; Part 5



ISO27001:2013 DISCRETIONARY CONTROLS

Reference	Description	Control Total
Discretionary	A5 Information security policies	2
	A6 Organization of information security	7
	A7 Human resource security	6
	A8 Asset management	10
	A9 Access control	13
	A10 Cryptography	2
	A11 Physical and environmental security	15
	A12 Operations security	14
	A13 Communications security	7
	A14 System acquisition, development and maintenance	13
	A15 Supplier relationships	5
	A16 Information security incident management	7
	A17 Information security aspects of business continuity management	4
	A18 Compliance	8

TOTAL: 114

<https://chapters.theiia.org/bermuda/Events/ChapterDocuments/Information%20Security%20Management%20System%20%28ISMS%29%20Overview.pdf>

ISO27001:2013 Controls Appendix; Part 5

A.10 CRYPTOGRAPHY

A.10.1 CRYPTOGRAPHIC CONTROLS

A.10.1.1	POLICY ON THE USE OF CRYPTOGRAPHIC CONTROLS
A.10.1.2	KEY MANAGEMENT

ISO27001:2013 Controls Appendix; Part 5

A.10 CRYPTOGRAPHY

A.10.1.2	KEY MANAGEMENT	<i>Control:</i> A policy on the use, protection and lifetime of cryptographic keys shall be developed and implemented through their whole lifecycle.

ISO27001:2013 Controls Appendix; Part 5

A.11 PHYSICAL & ENVIRONMENTAL SECURITY

A.11.1 SECURE AREAS

A.11.1.1	PHYSICAL SECURITY PERIMETER
A.11.1.2	PHYSICAL ENTRY CONTROLS
A.11.1.3	SUCURING OFFICES, ROOMS, AND FACILITIES
A.11.1.4	PROTECTING AGAINST EXTERNAL & ENVIRONMENTAL THREATS
A.11.1.5	WORKING IN SECURE AREAS
A.11.1.6	DELIVERY & LOADING AREAS

ISO27001:2013 Controls Appendix; Part 5

A.11 PHYSICAL & ENVIRONMENTAL SECURITY

A.11.1.1	PHYSICAL SECURITY PERIMETER	<i>Control:</i> Security perimeters shall be defined and used to protect areas that contain either sensitive or critical info & information processing facilities.

ISO27001:2013 Controls Appendix; Part 5

A.11 PHYSICAL & ENVIRONMENTAL SECURITY

A.11.1.2	PHYSICAL ENTRY CONTROLS	Control: Secure areas shall be protected by appropriate entry controls to ensure that only authorized personnel are allowed access.
A.11.1.5	WORKING IN SECURE AREAS	Control: Procedures for working in secure areas shall be designed and applied.

ISO27001:2013 Controls Appendix; Part 5

A.11 PHYSICAL & ENVIRONMENTAL SECURITY

A.11.2 EQUIPMENT

A.11.2.1	EQUIPMENT SITING & PROTECTION
A.11.2.2	SUPPORTING UTILITIES
A.11.2.3	CABLING SECURITY
A.11.2.4	EQUIPMENT MAINTENANCE
A.11.2.5	REMOVAL OF ASSETS
A.11.2.6	SECURITY OF EQUIPMENT & ASSETS OFF-PREMISES

ISO27001:2013 Controls Appendix; Part 5

A.11 PHYSICAL & ENVIRONMENTAL SECURITY

A.11.2.2	SUPPORTING UTILITIES	Control: Equipment shall be protected from power failures and other disruptions caused by failures in supporting utilities.
A.11.2.4	EQUIPMENT MAINTENANCE	Control: Equipment shall be correctly maintained to ensure its continued availability and integrity.

ISO27001:2013 Controls Appendix; Part 5

A.11 PHYSICAL & ENVIRONMENTAL SECURITY

A.11.2 EQUIPMENT...

A.11.2.7	SECURE DISPOSAL OR RE-USE OF EQUIPMENT
A.11.2.8	UNATTENDED USER EQUIPMENT
A.11.2.9	CLEAR DESK & CLEAR SCREEN POLICY

ISO27001:2013 Controls Appendix; Part 5

A.11 PHYSICAL & ENVIRONMENTAL SECURITY

A.11.2.9	CLEAR DESK & CLEAR SCREEN POLICY	<i>Control:</i> A clear desk policy for papers and removable storage media and a clear screen policy for information processing facilities shall be adopted.

ISO27001:2013 Controls Appendix; Part 5

- Lets look at operations security in the next module...

END

ISO27001:2013 Controls Appendix; Part 6

- In this module lets look at ISO27001:2013 (ISMS) related to operations security...

ISO27001:2013 Controls Appendix; Part 6



ISO27001:2013 DISCRETIONARY CONTROLS

Reference	Description	Control Total
Discretionary	A5 Information security policies	2
	A6 Organization of information security	7
	A7 Human resource security	6
	A8 Asset management	10
	A9 Access control	13
	A10 Cryptography	2
	A11 Physical and environmental security	15
	A12 Operations security	14
	A13 Communications security	7
	A14 System acquisition, development and maintenance	13
	A15 Supplier relationships	5
	A16 Information security incident management	7
	A17 Information security aspects of business continuity management	4
	A18 Compliance	8

TOTAL: 114

<https://chapters.theiia.org/bermuda/Events/ChapterDocuments/Information%20Security%20Management%20System%20%28ISMS%29%20Overview.pdf>

ISO27001:2013 Controls Appendix; Part 6

A.12 OPERATIONS SECURITY

A.12.1 OPERATIONAL PROCEDURES & RESPONSIBILITIES

A.12.1.1	DOCUMENTED OPERATING PROCEDURES
A.12.1.2	CHANGE MANAGEMENT
A.12.1.3	CAPACITY MANAGEMENT
A.12.1.4	SEPARATION OF DEVELOPMENT, TESTING, AND OPERATIONAL ENVIRONMENTS

ISO27001:2013 Controls Appendix; Part 6

A.12 OPERATIONS SECURITY

A.12.1.1	DOCUMENTED OPERATING PROCEDURES	<i>Control:</i> Operating procedures shall be documented and made available to all users who need them.

ISO27001:2013 Controls Appendix; Part 6

A.12 OPERATIONS SECURITY

A.12.1.2	CHANGE MANAGEMENT	<i>Control:</i> Changes to the organization, business processes, information processing facilities and systems that affect information security shall be controlled.

ISO27001:2013 Controls Appendix; Part 6

A.12 OPERATIONS SECURITY

A.12.1.3	CAPACITY MANAGEMENT	<i>Control:</i> The use of resources shall be monitored, tuned and projections made of future capacity requirements to ensure the required system performance.

ISO27001:2013 Controls Appendix; Part 6

A.12 OPERATIONS SECURITY

A.12.1.4	SEPARATION OF DEVELOPMENT, TESTING, AND OPERATIONAL ENVIRONMENTS	Control: Development, testing, and operational environments shall be separated to reduce the risks of unauthorized access or changes to the operational environment.

ISO27001:2013 Controls Appendix; Part 6

- Lets continue to look at operations security in the next module...

END

ISO27001:2013 Controls Appendix; Part 7

- In this module lets look at ISO27001:2013 (ISMS) related to operations security...

ISO27001:2013 Controls Appendix; Part 7



ISO27001:2013 DISCRETIONARY CONTROLS

Reference	Description	Control Total
Discretionary	A5 Information security policies	2
	A6 Organization of information security	7
	A7 Human resource security	6
	A8 Asset management	10
	A9 Access control	13
	A10 Cryptography	2
	A11 Physical and environmental security	15
	A12 Operations security	14
	A13 Communications security	7
	A14 System acquisition, development and maintenance	13
	A15 Supplier relationships	5
	A16 Information security incident management	7
	A17 Information security aspects of business continuity management	4
	A18 Compliance	8

TOTAL: 114

<https://chapters.theiia.org/bermuda/Events/ChapterDocuments/Information%20Security%20Management%20System%20%28ISMS%29%20Overview.pdf>

ISO27001:2013 Controls Appendix; Part 7

A.12 OPERATIONS SECURITY

A.12.2 PROTECTION FROM MALWARE

A.12.2.1	CONTROLS AGAINST MALWARE

A.12.2.1	CONTROLS AGAINST MALWARE	<i>Control:</i> Detection, prevention and recovery controls to protect against malware shall be implemented, combined with appropriate user awareness.

ISO27001:2013 Controls Appendix; Part 7

A.12 OPERATIONS SECURITY

A.12.3 BACKUP

A.12.3.1	INFORMATION BACKUP

A.12.3.1	INFORMATION BACKUP	Control: Backup copies of information, software and system images shall be taken and tested regularly in accordance with an agreed backup policy.

ISO27001:2013 Controls Appendix; Part 7

A.12 OPERATIONS SECURITY

A.12.4 LOGGING & MONITORING

A.12.4.1	EVENT LOGGING
A.12.4.2	PROTECTION OF LOG INFORMATION
A.12.4.3	ADMINISTRATOR & OPERATOR LOGS
A.12.4.4	CLOCK SYNCHRONISATION

ISO27001:2013 Controls Appendix; Part 7

A.12 OPERATIONS SECURITY

A.12.4.1	EVENT LOGGING	Control: Event logs recording user activities, exceptions, faults and information security events shall be produced, kept and regularly reviewed.

ISO27001:2013 Controls Appendix; Part 7

A.12 OPERATIONS SECURITY

A.12.4.3	ADMINISTRATOR & OPERATOR LOGS	<i>Control:</i> System administrator and system operator activities shall be logged and the logs protected and regularly reviewed.

ISO27001:2013 Controls Appendix; Part 7

A.12 OPERATIONS SECURITY

A.12.5 CONTROL OF OPERATIONAL SOFTWARE

A.12.5.1

INSTALLATION OF SOFTWARE ON
OPERATIONAL SYSTEMS

A.12.5.1

INSTALLATION
OF SOFTWARE
ON
OPERATIONAL
SYSTEMS

Control:

Procedures shall be implemented to control the installation of software on operational systems.

ISO27001:2013 Controls Appendix; Part 7

A.12 OPERATIONS SECURITY

A.12.6 TECHNICAL VULNERABILITY MANAGEMENT

A.12.6.1	MANAGEMENT OF TECHNICAL VULNERABILITIES
A.12.6.2	RESTRICTIONS ON SOFTWARE INSTALLATION

ISO27001:2013 Controls Appendix; Part 7

A.12 OPERATIONS SECURITY

A.12.6.1	MANAGEMENT OF TECHNICAL VULNERABILITIES	<i>Control:</i> Information about technical vulnerabilities of information systems being used shall be obtained in a timely fashion, the organization's exposure to such vulnerabilities evaluated and appropriate measures taken to address the associated risk.

ISO27001:2013 Controls Appendix; Part 7

A.12 OPERATIONS SECURITY

A.12.6.2	RESTRICTIONS ON SOFTWARE INSTALLATION	<i>Control:</i> Rules governing the installation of software by users shall be established and implemented.

ISO27001:2013 Controls Appendix; Part 7

A.12 OPERATIONS SECURITY

A.12.7 INFORMATION SYSTEMS AUDIT CONSIDERATIONS

A.12.7.1

INFORMATION SYSTEMS AUDIT
CONTROLS

ISO27001:2013 Controls Appendix; Part 7

A.12 OPERATIONS SECURITY

A.12.7.1	INFORMATION SYSTEMS AUDIT CONTROLS	<i>Control:</i> Audit requirements and activities involving verification of operational systems shall be carefully planned and agreed to minimise disruptions to business processes.

ISO27001:2013 Controls Appendix; Part 7

- Lets look at communications security in the next module...

END

ISO27001:2013 Controls Appendix; Part 8

- In this module lets look at ISO27001:2013 (ISMS) related to operations security...

ISO27001:2013 Controls Appendix; Part 8



ISO27001:2013 DISCRETIONARY CONTROLS

Reference	Description	Control Total
Discretionary	A5 Information security policies	2
	A6 Organization of information security	7
	A7 Human resource security	6
	A8 Asset management	10
	A9 Access control	13
	A10 Cryptography	2
	A11 Physical and environmental security	15
	A12 Operations security	14
	A13 Communications security	7
	A14 System acquisition, development and maintenance	13
	A15 Supplier relationships	5
	A16 Information security incident management	7
	A17 Information security aspects of business continuity management	4
	A18 Compliance	8

TOTAL: 114

<https://chapters.theiia.org/bermuda/Events/ChapterDocuments/Information%20Security%20Management%20System%20%28ISMS%29%20Overview.pdf>

ISO27001:2013 Controls Appendix; Part 8

A.13 COMMUNICATIONS SECURITY

A.13.1 COMMUNICATIONS SECURITY

A.13.1.1	NETWORK CONTROLS
A.13.1.2	SECURITY OF NETWORK SERVICES
A.13.1.3	SEGREGATION IN NETWORKS

ISO27001:2013 Controls Appendix; Part 8

A.13 COMMUNICATIONS SECURITY

A.13.1.1	NETWORK CONTROLS	<i>Control:</i> Networks shall be managed and controlled to protect information in systems and applications.

ISO27001:2013 Controls Appendix; Part 8

A.13 COMMUNICATIONS SECURITY

A.13.1.2	SECURITY OF NETWORK SERVICES	Control: Security mechanisms, service levels and management requirements of all network services shall be identified and included in network services agreements, whether these services are provided in-house or outsourced.

ISO27001:2013 Controls Appendix; Part 8

A.13 COMMUNICATIONS SECURITY

A.13.1.3	SEGREGATION IN NETWORKS	<i>Control:</i> Groups of information services, users and information systems shall be segregated on networks.

ISO27001:2013 Controls Appendix; Part 8

A.13 COMMUNICATIONS SECURITY

A.13.2 INFORMATION TRANSFER

A.13.2.1	INFORMATION TRANSFER POLICIES & PROCEDURES
A.13.2.2	AGREEMENTS ON INFORMATION TRANSFER
A.13.2.3	ELECTRONIC MESSAGING
A.13.2.4	CONFIDENTIALITY OR NON-DISCLOSURE AGREEMENTS

ISO27001:2013 Controls Appendix; Part 8

A.13 COMMUNICATIONS SECURITY

A.13.2.1	INFORMATION TRANSFER POLICIES & PROCEDURES	<i>Control:</i> Formal transfer policies, procedures and controls shall be in place to protect the transfer of information through the use of all types of communication facilities.

ISO27001:2013 Controls Appendix; Part 8

A.13 COMMUNICATIONS SECURITY

A.13.2.2	AGREEMENTS ON INFORMATION TRANSFER	<i>Control:</i> Agreements shall address the secure transfer of business information between the organization and external parties.

ISO27001:2013 Controls Appendix; Part 8

- Lets look at system acquisition, development & maintenance in the next module...

END

ISO27001:2013 Controls Appendix; Part 9

- In this module lets look at ISO27001:2013 (ISMS) related to system acquisition, development, and maintenance....

ISO27001:2013 Controls Appendix; Part 9



ISO27001:2013 DISCRETIONARY CONTROLS

Reference	Description	Control Total
Discretionary	A5 Information security policies	2
	A6 Organization of information security	7
	A7 Human resource security	6
	A8 Asset management	10
	A9 Access control	13
	A10 Cryptography	2
	A11 Physical and environmental security	15
	A12 Operations security	14
	A13 Communications security	7
	A14 System acquisition, development and maintenance	13
	A15 Supplier relationships	5
	A16 Information security incident management	7
	A17 Information security aspects of business continuity management	4
	A18 Compliance	8

TOTAL: 114

<https://chapters.theiia.org/bermuda/Events/ChapterDocuments/Information%20Security%20Management%20System%20%28ISMS%29%20Overview.pdf>

ISO27001:2013 Controls Appendix; Part 9

A.14 SYSTEM ACQUISITION, DEVELOPMENT, & MAINTENANCE

A.14.1 SECURITY REQMTS OF INFORMATION SYSTEMS

A.14.1.1	INFORMATION SECURITY REQMTS ANALYSIS & SPECIFICATION
A.14.1.2	SECURING APPLICATION SERVICES ON PUBLIC NETWORKS
A.14.1.3	PROTECTING APPLICATION SERVICES TRANSACTIONS

ISO27001:2013 Controls Appendix; Part 9

A.14 SYSTEM ACQUISITION, DEVELOPMENT, & MAINTENANCE

A.14.1.1	INFORMATION SECURITY REQMTS ANALYSIS & SPECIFICATION	<i>Control:</i> The information security related requirements shall be included in the requirements for new information systems or enhancements to existing information systems.

ISO27001:2013 Controls Appendix; Part 9

A.14 SYSTEM ACQUISITION, DEVELOPMENT, & MAINTENANCE

A.14.1.2	SECURING APPLICATION SERVICES ON PUBLIC NETWORKS	Control: Information involved in application services passing over public networks shall be protected from fraudulent activity, contract dispute and unauthorized disclosure and modification.

ISO27001:2013 Controls Appendix; Part 9

A.14 SYSTEM ACQUISITION, DEVELOPMENT, & MAINTENANCE

A.14.2 SECURITY IN DEV. & SUPPORT PROCESSES

A.14.2.1	SECURE DEVELOPMENT POLICY
A.14.2.2	SYSTEM CHANGE CONTROL PROCEDURES
A.14.2.3	TECHNICAL REVIEW OF APPLICATIONS AFTER OPERATING PLATFORM CHANGES
A.14.2.4	RESTRICTIONS ON CHANGES TO SOFTWARE PACKAGES
A.14.2.5	SECURE SYSTEM ENGINEERING PRINCIPLES

ISO27001:2013 Controls Appendix; Part 9

A.14 SYSTEM ACQUISITION, DEVELOPMENT, & MAINTENANCE

A.14.2 SECURITY IN DEV. & SUPPORT PROCESSES

A.14.2.6	SECURE DEVELOPMENT ENVIRONMENT
A.14.2.7	OUTSOURCED DEVELOPMENT
A.14.2.8	SYSTEM SECURITY TESTING
A.14.2.9	SYSTEM ACCEPTANCE TESTING

ISO27001:2013 Controls Appendix; Part 9

A.14 SYSTEM ACQUISITION, DEVELOPMENT, & MAINTENANCE

A.14.2.3	TECHNICAL REVIEW OF APPLICATIONS AFTER OPERATING PLATFORM CHANGES	<i>Control:</i> When operating platforms are changed, business critical applications shall be reviewed and tested to ensure there is no adverse impact on organizational operations or security.

ISO27001:2013 Controls Appendix; Part 9

A.14 SYSTEM ACQUISITION, DEVELOPMENT, & MAINTENANCE

A.14.2.4	RESTRICTIONS ON CHANGES TO SOFTWARE PACKAGES	<i>Control:</i> Modifications to software packages shall be discouraged, limited to necessary changes and all changes shall be strictly controlled.

ISO27001:2013 Controls Appendix; Part 9

A.14 SYSTEM ACQUISITION, DEVELOPMENT, & MAINTENANCE

A.14.2.5	SECURE SYSTEM ENGINEERING PRINCIPLES	<i>Control:</i> Principles for engineering secure systems shall be established, documented, maintained and applied to any information system implementation efforts.

ISO27001:2013 Controls Appendix; Part 9

A.14 SYSTEM ACQUISITION, DEVELOPMENT, & MAINTENANCE

A.14.2.8	SYSTEM SECURITY TESTING	<i>Control:</i> Testing of security functionality shall be carried out during development.

ISO27001:2013 Controls Appendix; Part 9

A.14 SYSTEM ACQUISITION, DEVELOPMENT, & MAINTENANCE

A.14.3 TEST DATA

A.14.3.1	PROTECTION OF TEST DATA

A.14.3.1	PROTECTION OF TEST DATA	<i>Control:</i> Test data shall be selected carefully, protected and controlled.

ISO27001:2013 Controls Appendix; Part 9

- Lets look at supplier relationships in the next module...

END

ISO27001:2013 Controls Appendix; Part 10

- In this module lets look at ISO27001:2013 (ISMS) related to supplier relationships...

ISO27001:2013 Controls Appendix; Part 10



ISO27001:2013 DISCRETIONARY CONTROLS

Reference	Description	Control Total
Discretionary	A5 Information security policies	2
	A6 Organization of information security	7
	A7 Human resource security	6
	A8 Asset management	10
	A9 Access control	13
	A10 Cryptography	2
	A11 Physical and environmental security	15
	A12 Operations security	14
	A13 Communications security	7
	A14 System acquisition, development and maintenance	13
	A15 Supplier relationships	5
	A16 Information security incident management	7
	A17 Information security aspects of business continuity management	4
	A18 Compliance	8

TOTAL: 114

<https://chapters.theiia.org/bermuda/Events/ChapterDocuments/Information%20Security%20Management%20System%20%28ISMS%29%20Overview.pdf>

ISO27001:2013 Controls Appendix; Part 10

A.15 SUPPLIER RELATIONSHIPS

A.15.1 INFORMATION SECURITY IN SUPPLIER RELATIONSHIPS

A.15.1.1	INFORMATION SECURITY POLICY FOR SUPPLIER RELATIONSHIPS
A.15.1.2	ADDRESSING SECURITY WITHIN SUPPLIER AGREEMENTS
A.15.1.3	INFORMATION & COMMUNICATION TECHNOLOGY SUPPLY CHAIN

ISO27001:2013 Controls Appendix; Part 10

A.15 SUPPLIER RELATIONSHIPS

A.15.1.1	INFORMATION SECURITY POLICY FOR SUPPLIER RELATIONSHIPS	<i>Control:</i> Information security requirements for mitigating the risks associated with supplier's access to the organization's assets shall be agreed with the supplier and documented.

ISO27001:2013 Controls Appendix; Part 10

A.15 SUPPLIER RELATIONSHIPS

A.15.1.2	ADDRESSING SECURITY WITHIN SUPPLIER AGREEMENTS	<i>Control:</i> All relevant information security requirements shall be established and agreed with each supplier that may access, process, store, communicate, or provide IT infrastructure components for, the organization's information.

ISO27001:2013 Controls Appendix; Part 10

A.15 SUPPLIER RELATIONSHIPS

A.15.2 SUPPLIER SERVICE DELIVERY MANAGEMENT

A.15.2.1	MONITORING & REVIEW OF SUPPLIER SERVICES
A.15.2.2	MANAGING CHANGES TO SUPPLIER SERVICES

ISO27001:2013 Controls Appendix; Part 10

A.15 SUPPLIER RELATIONSHIPS

A.15.2.1	MONITORING & REVIEW OF SUPPLIER SERVICES	<i>Control:</i> Organizations shall regularly monitor, review and audit supplier service delivery.

ISO27001:2013 Controls Appendix; Part 10

A.15 SUPPLIER RELATIONSHIPS

A.15.2.2	MANAGING CHANGES TO SUPPLIER SERVICES	<i>Control:</i> Changes to the provision of services by suppliers, including maintaining & improving existing information security policies, procedures & controls, shall be managed, taking account of the criticality of business information, systems and processes involved and re-assessment of risks.

ISO27001:2013 Controls Appendix; Part 10

- Lets look at incident management in the next module...

END

ISO27001:2013 Controls Appendix; Part 11

- In this module lets look at ISO27001:2013 (ISMS) related to information security incidents...

ISO27001:2013 Controls Appendix; Part 11



ISO27001:2013 DISCRETIONARY CONTROLS

Reference	Description	Control Total
Discretionary	A5 Information security policies	2
	A6 Organization of information security	7
	A7 Human resource security	6
	A8 Asset management	10
	A9 Access control	13
	A10 Cryptography	2
	A11 Physical and environmental security	15
	A12 Operations security	14
	A13 Communications security	7
	A14 System acquisition, development and maintenance	13
	A15 Supplier relationships	5
	A16 Information security incident management	7
	A17 Information security aspects of business continuity management	4
	A18 Compliance	8

TOTAL: 114

<https://chapters.theiia.org/bermuda/Events/ChapterDocuments/Information%20Security%20Management%20System%20%28ISMS%29%20Overview.pdf>

ISO27001:2013 Controls Appendix; Part 11

A.16 INFORMATION SECURITY INCIDENT MANAGEMENT

A.16.1 MNGMT OF INFOSEC INCIDENTS & IMPROVEMENTS

A.16.1.1	RESPONSIBILITIES & PROCEDURES
A.16.1.2	REPORTING INFOSEC SECURITY EVENTS
A.16.1.3	REPORTING INFOSEC WEAKNESSES
A.16.1.4	ASSESSMENT OF & DECISION ON INFOSEC EVENTS

ISO27001:2013 Controls Appendix; Part 11

A.16 INFORMATION SECURITY INCIDENT MANAGEMENT

A.16.1 MNGMT OF INFOSEC INCIDENTS & IMPROVEMENTS

A.16.1.5	RESPONSE TO INFOSEC INCIDENTS
A.16.1.6	LEARNING FROM INFOSEC INCIDENTS
A.16.1.7	COLLECTION OF EVIDENCE

ISO27001:2013 Controls Appendix; Part 11

A.16 INFORMATION SECURITY INCIDENT MANAGEMENT

A.16.1.2	REPORTING INFORMATION SECURITY EVENTS	<i>Control:</i> Information security events shall be reported through appropriate management channels as quickly as possible.

ISO27001:2013 Controls Appendix; Part 11

A.16 INFORMATION SECURITY INCIDENT MANAGEMENT

A.16.1.3	REPORTING INFORMATION SECURITY WEAKNESSES	<i>Control:</i> Employees and contractors using the organization's information systems and services shall be required to note and report any observed or suspected information security weaknesses in systems or services.

ISO27001:2013 Controls Appendix; Part 11

A.16 INFORMATION SECURITY INCIDENT MANAGEMENT

A.16.1.5	RESPONSE TO INFORMATION SECURITY INCIDENTS	<i>Control:</i> Information security incidents shall be responded to in accordance with the documented procedures.

ISO27001:2013 Controls Appendix; Part 11

A.16 INFORMATION SECURITY INCIDENT MANAGEMENT

A.16.1.6	LEARNING FROM INFORMATION SECURITY INCIDENTS	<i>Control:</i> Knowledge gained from analysing and resolving information security incidents shall be used to reduce the likelihood or impact of future incidents.

ISO27001:2013 Controls Appendix; Part 11

- Lets look at business continuity in the next module...

END

ISO27001:2013 Controls Appendix; Part 12

- In this module lets look at ISO27001:2013 (ISMS) related to business continuity...

ISO27001:2013 Controls Appendix; Part 12



ISO27001:2013 DISCRETIONARY CONTROLS

Reference	Description	Control Total
Discretionary	A5 Information security policies	2
	A6 Organization of information security	7
	A7 Human resource security	6
	A8 Asset management	10
	A9 Access control	13
	A10 Cryptography	2
	A11 Physical and environmental security	15
	A12 Operations security	14
	A13 Communications security	7
	A14 System acquisition, development and maintenance	13
	A15 Supplier relationships	5
	A16 Information security incident management	7
	A17 Information security aspects of business continuity management	4
	A18 Compliance	8

TOTAL: 114

<https://chapters.theiia.org/bermuda/Events/ChapterDocuments/Information%20Security%20Management%20System%20%28ISMS%29%20Overview.pdf>

ISO27001:2013 Controls Appendix; Part 12

A.17 INFOSEC ASPECTS OF BUSINESS CONTINUITY MNGMT

A.17.1 INFORMATION SECURITY CONTINUITY

A.17.1.1	PLANNING INFOSEC CONTINUITY
A.17.1.2	IMPLEMENTING INFOSEC CONTINUITY
A.17.1.3	VERIFY, REVIEW, & EVALUATE INFOSEC CONTINUITY

ISO27001:2013 Controls Appendix; Part 12

A.17 INFOSEC ASPECTS OF BUSINESS CONTINUITY MNGMT

A.17.1.1	PLANNING INFOSEC CONTINUITY	<i>Control:</i> The organization shall determine its requirements for information security and the continuity of information security management in adverse situations, e.g. during a crisis or disaster.

ISO27001:2013 Controls Appendix; Part 12

A.17 INFOSEC ASPECTS OF BUSINESS CONTINUITY MNGMT

A.17.1.2	IMPLEMENTING INFOSEC CONTINUITY	<i>Control:</i> The organization shall establish, document, implement and maintain processes, procedures and controls to ensure the required level of continuity for information security during an adverse situation.

ISO27001:2013 Controls Appendix; Part 12

A.17 INFOSEC ASPECTS OF BUSINESS CONTINUITY MNGMT

A.17.1.3	VERIFY, REVIEW, & EVALUATE INFOSEC CONTINUITY	<i>Control:</i> The organization shall verify the established and implemented info security continuity controls at regular intervals in order to ensure that they are valid and effective during adverse situations.

ISO27001:2013 Controls Appendix; Part 12

A.17 INFOSEC ASPECTS OF BUSINESS CONTINUITY MNGMT

A.17.2 REDUNDANCIES

A.17.2.1	AVAILABILITY OF INFORMATION PROCESSING FACILITIES

A.17.2.1	AVAILABILITY OF INFORMATION PROCESSING FACILITIES	Control: Information processing facilities shall be implemented with redundancy sufficient to meet availability requirements.

ISO27001:2013 Controls Appendix; Part 12

- Lets look at compliance in the next module...

END

ISO27001:2013 Controls Appendix; Part 13

- In this module lets look at ISO27001:2013 (ISMS) related to compliance...

ISO27001:2013 Controls Appendix; Part 13



ISO27001:2013 DISCRETIONARY CONTROLS

Reference		Description	Control Total
Discretionary	A5	Information security policies	2
	A6	Organization of information security	7
	A7	Human resource security	6
	A8	Asset management	10
	A9	Access control	13
	A10	Cryptography	2
	A11	Physical and environmental security	15
	A12	Operations security	14
	A13	Communications security	7
	A14	System acquisition, development and maintenance	13
	A15	Supplier relationships	5
	A16	Information security incident management	7
	A17	Information security aspects of business continuity management	4
	A18	Compliance	8

TOTAL: 114

<https://chapters.theiia.org/bermuda/Events/ChapterDocuments/Information%20Security%20Management%20System%20%28ISMS%29%20Overview.pdf>

ISO27001:2013 Controls Appendix; Part 13

A.18 COMPLIANCE

A.18.1 COMPLIANCE WITH LEGAL & CONTRACTUAL REQUIREMENTS

A.18.1.1	IDENTIFICATION OF APPLICABLE LEGISLATION & CONTRACTUAL REQMTS
A.18.1.2	INTELLECTUAL PROPERTY RIGHTS
A.18.1.3	PROTECTION OF RECORDS
A.18.1.4	PRIVACY & PROTECTION OF PERSONALLY IDENTIFIABLE INFORMATION
A.18.1.4	REGULATION OF CRYPTOGRAPHIC CONTROLS

ISO27001:2013 Controls Appendix; Part 13

A.18 COMPLIANCE

A.18.1.1	IDENTIFICATION OF APPLICABLE LEGISLATION & CONTRACTUAL REQMTS	<i>Control:</i> All relevant legislative statutory, regulatory, contractual requirements and the organization's approach to meet these requirements shall be explicitly identified, documented and kept up to date for each information system and the organiz.

ISO27001:2013 Controls Appendix; Part 13

A.18 COMPLIANCE

A.18.1.2	INTELLECTUAL PROPERTY RIGHTS	<i>Control:</i> Appropriate procedures shall be implemented to ensure compliance with legislative, regulatory and contractual requirements related to intellectual property rights and use of proprietary software products.

ISO27001:2013 Controls Appendix; Part 13

A.18 COMPLIANCE

A.18.2 INFORMATION SECURITY REVIEWS

A.18.2.1	INDEPENDENT REVIEW OF INFORMATION SECURITY
A.18.2.2	COMPLIANCE WITH SECURITY POLICY & STANDARDS
A.18.2.3	TECHNICAL COMPLIANCE REVIEW

ISO27001:2013 Controls Appendix; Part 13

A.18 COMPLIANCE

A.18.2.1	INDEPENDENT REVIEW OF INFORMATION SECURITY	<i>Control:</i> The organization's approach to managing information security & its implementation (i.e. control objectives, controls, policies, processes & procedures for info security) shall be reviewed independently at planned intervals or when significant changes occur.

ISO27001:2013 Controls Appendix; Part 13

A.18 COMPLIANCE

A.18.2.2	COMPLIANCE WITH SECURITY POLICY & STANDARDS	<i>Control:</i> Managers shall regularly review the compliance of information processing and procedures within their area of responsibility with the appropriate security policies, standards and any other security requirements.

ISO27001:2013 Controls Appendix; Part 13

A.18 COMPLIANCE

A.18.2.3	TECHNICAL COMPLIANCE REVIEW	<i>Control:</i> Information systems shall be regularly reviewed for compliance with the organization's information security policies and standards.

ISO27001:2013 Controls Appendix; Part 13

- That completes an in-depth overview of the controls and structure of ISO27001:2013 (ISMS)

END

How to Use ISO27002:2013

- What is ISO27002:2013 ?
 - Information technology -- Security techniques -- Code of practice for information security controls
 - Renamed from ISO 17799

How to Use ISO27002:2013

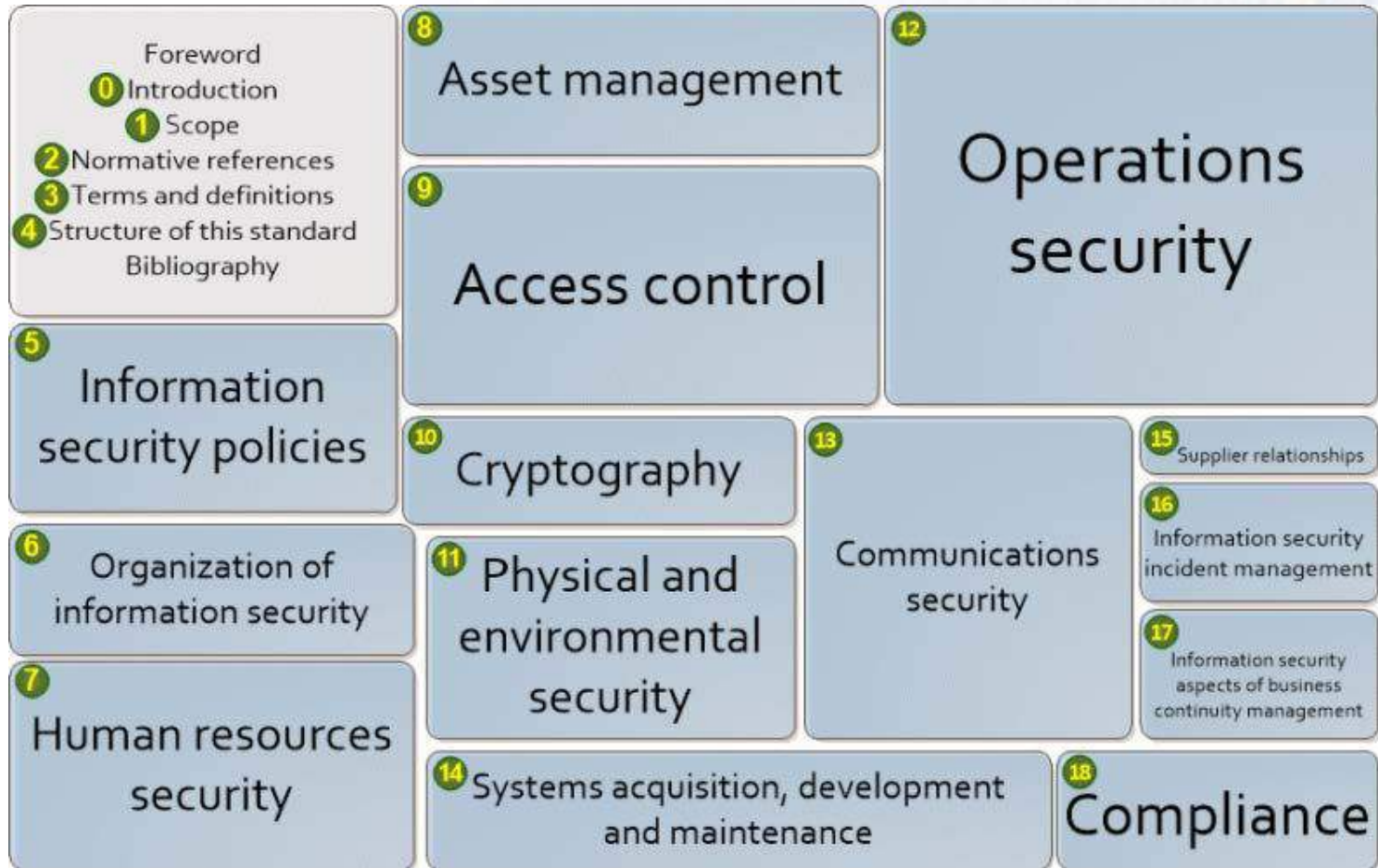
- 0.1 Background & Context
 - This Int'l Standard is designed for orgs to use as a **reference** for selecting controls within the process of implementing an Information Security Management System (ISMS) based on ISO/IEC 27001;

How to Use ISO27002:2013

- 0.1 Background & Context
 - or as a **guidance document** for organizations implementing commonly accepted information security controls.

How to Use ISO27002:2013

STRUCTURE OF ISO27002:2013



<http://www.iso27001security.com/html/27002.html>

How to Use ISO27002:2013

- Lets have a look at control A.5.1.2 (**Review Of The Policies Of Information Security**)

How to Use ISO27002:2013

ISO27001:2013

A.5.1.2	REVIEW OF THE POLICIES FOR INFORMATION SECURITY	<i>Control:</i> The policies for information security shall be reviewed at planned intervals or if significant changes occur to ensure their continuing suitability, adequacy and effectiveness.

How to Use ISO27002:2013

ISO27002:2013

TITLE

5.1.2 Review of the policies for information security

Control

The policies for information security should be reviewed at planned intervals or if significant changes occur to ensure their continuing suitability, adequacy and effectiveness.

Implementation guidance

Each policy should have an owner who has approved management responsibility for the development, review and evaluation of the policies. The review should include assessing opportunities for improvement of the organization's policies and approach to managing information security in response to changes to the organizational environment, business circumstances, legal conditions or technical environment.

How to Use ISO27002:2013

ISO27002:2013

CONTROL

5.1.2 Review of the policies for information security

Control

The policies for information security should be reviewed at planned intervals or if significant changes occur to ensure their continuing suitability, adequacy and effectiveness.

Implementation guidance

Each policy should have an owner who has approved management responsibility for the development, review and evaluation of the policies. The review should include assessing opportunities for improvement of the organization's policies and approach to managing information security in response to changes to the organizational environment, business circumstances, legal conditions or technical environment.

How to Use ISO27002:2013

ISO27002:2013

5.1.2 Review of the policies for information security

Control

The policies for information security should be reviewed at planned intervals or if significant changes occur to ensure their continuing suitability, adequacy and effectiveness.

Implementation guidance

Each policy should have an owner who has approved management responsibility for the development, review and evaluation of the policies. The review should include assessing opportunities for improvement of the organization's policies and approach to managing information security in response to changes to the organizational environment, business circumstances, legal conditions or technical environment.

27002 IMPLEMENTATION GUIDANCE

How to Use ISO27002:2013

ISO27002:2013

A.5.1.2	REVIEW OF THE POLICIES FOR INFOSEC	<i>27002: Implementation Guidance:</i> Each policy should have an owner who has approved mngmt responsibility for the development, review and evaluation of the policies. The review should include assessing opportunities for improvement of the org's policies and approach to managing Infosec in response to changes to the org environment, business circumstances, legal conditions or tech environment.

How to Use ISO27002:2013

- Practically:
 - ISO27001:2013 controls are brief and generic
 - **27002 clarifies further what is being referred to, gives further context & very useful implementation guidance**

END

PCI DSS V3

- PCI Data Security Standard (DSS): 
 - Designed to ensure that ALL companies that accept, process, store or transmit credit card info maintain a secure environment
 - Managed by Security Standards Council

<https://www.pcicomplianceguide.org/pci-faqs-2/>

PCI DSS V3

- PCI DSS: 
 - SSC is an independent body that was created by the major payment card brands (Visa, MasterCard, American Express, Discover and JCB)
 - 6 Broad goals and 12 requirements

REF: PCI Best Practices For Implementing Security Awareness;
<https://www.pcisecuritystandards.org/documents/>

PCI DSS V3

PAYMENT CARD INDUSTRY SECURITY STANDARDS

Protection of Cardholder Payment Data



<https://www.pcisecuritystandards.org/documents/PCI%20SSC%20Quick%20Reference%20Guide.pdf>

PCI DSS V3

Goals	PCI DSS Requirements
Build and Maintain a Secure Network and Systems	1. Install and maintain a firewall configuration to protect cardholder data 2. Do not use vendor-supplied defaults for system passwords and other security parameters
Protect Cardholder Data	3. Protect stored cardholder data 4. Encrypt transmission of cardholder data across public networks 
Maintain a Vulnerability Management Program	5. Protect all systems against malware and regularly update anti-virus software or programs 6. Develop and maintain secure systems and applications
Implement Strong Access Control Measures	7. Restrict access to cardholder data by business need to know 8. Identify and authenticate access to system components 9. Restrict physical access to cardholder data
Regularly Monitor and Test Networks	10. Track and monitor all access to network resources and cardholder data 11. Regularly test security systems and processes
Maintain an Information Security Policy	12. Maintain a policy that addresses information security for all personnel

<https://www.pcisecuritystandards.org/documents/PCI%20SSC%20Quick%20Reference%20Guide.pdf>

PCI DSS V3

PCI DSS Requirements	Testing Procedures	Guidance
	1.1.1.c Identify a sample of actual changes made to firewall and router configurations, compare to the change records, and interview responsible personnel to verify the changes were approved and tested.	
1.1.2 Current network diagram that identifies all connections between the cardholder data environment and other networks, including any wireless networks	1.1.2.a Examine diagram(s) and observe network configurations to verify that a current network diagram exists and that it documents all connections to cardholder data, including any wireless networks.	Network diagrams describe how networks are configured, and identify the location of all network devices. Without current network diagrams, devices could be overlooked and be unknowingly left out of the security controls implemented for PCI DSS and thus be vulnerable to compromise.
	1.1.2.b Interview responsible personnel to verify that the diagram is kept current.	

REQUIREMENT

PCI DSS V3

PCI DSS Requirements	Testing Procedures	Guidance
	1.1.1.c Identify a sample of actual changes made to firewall and router configurations, compare to the change records, and interview responsible personnel to verify the changes were approved and tested.	 Network diagrams describe how networks are configured, and identify the location of all network devices. Without current network diagrams, devices could be overlooked and be unknowingly left out of the security controls implemented for PCI DSS and thus be vulnerable to compromise.
1.1.2 Current network diagram that identifies all connections between the cardholder data environment and other networks, including any wireless networks	1.1.2.a Examine diagram(s) and observe network configurations to verify that a current network diagram exists and that it documents all connections to cardholder data, including any wireless networks.	
	1.1.2.b Interview responsible personnel to verify that the diagram is kept current.	

TESTING PROCEDURES

PCI DSS V3

PCI DSS Requirements	Testing Procedures	Guidance
	1.1.1.c Identify a sample of actual changes made to firewall and router configurations, compare to the change records, and interview responsible personnel to verify the changes were approved and tested.	
1.1.2 Current network diagram that identifies all connections between the cardholder data environment and other networks, including any wireless networks	1.1.2.a Examine diagram(s) and observe network configurations to verify that a current network diagram exists and that it documents all connections to cardholder data, including any wireless networks.	Network diagrams describe how networks are configured, and identify the location of all network devices. Without current network diagrams, devices could be overlooked and be unknowingly left out of the security controls implemented for PCI DSS and thus be vulnerable to compromise.
	1.1.2.b Interview responsible personnel to verify that the diagram is kept current.	

GUIDANCE

PCI DSS V3

REQMT	TEST PROCEDURES	GUIDANCE
7.1.4 Require documented approval by authorized parties specifying required privileges.	7.1.4 Select a sample of user IDs & compare with documented approvals to verify that: -Documented approval exists for the assigned privileges -The approval was by authorized parties -That specified privileges match the roles assigned to the individual.	Documented approval (for example, in writing or electronically) assures that those with access and privileges are known and authorized by management, and that their access is necessary for their job function.

PCI DSS V3

REQMT	TEST PROCEDURES	GUIDANCE
8.1.4 Remove/disable inactive user accounts within 90 days.	8.1.4 Observe user accounts to verify that any inactive accounts over 90 days old are either removed or disabled.	Accounts that are not used regularly are often targets of attack since it is less likely that any changes (such as a changed password) will be noticed. As such, these accounts may be more easily exploited and used to access cardholder data.

PCI DSS V3

- PCI is specific to the card environment to protect cardholder data
- PCI controls are very specific and in-depth compared to generic and high-level controls of ISO27001

END

SANS/CIS CRITICAL SECURITY CONTROLS

- A very useful collection of controls for improving security posture

SANS/CIS CRITICAL SECURITY CONTROLS

SN	CONTROL
1	Inventory of Authorized and Unauthorized Devices
2	Inventory of Authorized and Unauthorized Software
3	Secure Configurations for Hardware and Software
4	Continuous Vulnerability Assessment and Remediation
5	Controlled Use of Administrative Privileges

SANS/CIS CRITICAL SECURITY CONTROLS

SN	CONTROL
6	Maintenance, Monitoring, and Analysis of Audit Logs
7	Email and Web Browser Protections
8	Malware Defenses
9	Limitation and Control of Network Ports
10	Data Recovery Capability

SANS/CIS CRITICAL SECURITY CONTROLS

SN	CONTROL
11	Secure Configurations for Network Devices
12	Boundary Defense
13	Data Protection
14	Controlled Access Based on the Need to Know
15	Wireless Access Control

SANS/CIS CRITICAL SECURITY CONTROLS

SN	CONTROL
16	Account Monitoring and Control
17	Security Skills Assessment and Appropriate Training to Fill Gaps
18	Application Software Security
19	Incident Response and Management
20	Penetration Tests and Red Team Exercises

SANS/CIS CRITICAL SECURITY CONTROLS

CONTROL 1.1: INVENTORY OF AUTH & UNAUTH DEVICES

Deploy an **automated asset inventory discovery tool** and use it to build a preliminary inventory of systems connected to an organization's public and private network(s). Both active tools that scan through IPv4 or IPv6 network address ranges and passive tools that identify hosts based on analyzing their traffic should be employed.

SANS/CIS CRITICAL SECURITY CONTROLS

CONTROL 2.1: INVENTORY OF AUTH & UNAUTH SW

Devise a **list of authorized software and version** that is required in the enterprise **for each type of system**, including servers, workstations, and laptops of various kinds and uses. This list should be **monitored by file integrity checking tools** to validate that the authorized software has not been modified.

SANS/CIS CRITICAL SECURITY CONTROLS

CONTROL 3.1: SECURE CONFIGS FOR HW & SW

Establish **standard secure configurations of your operating systems and software applications**. Standardized **images** should **represent hardened versions** of the underlying **operating system and the applications** installed on the system. These images should be **validated and refreshed on a regular basis** to update their security configuration in light of recent vulnerabilities and attack vectors.

SANS/CIS CRITICAL SECURITY CONTROLS

CONTROL 4.1: CONTINUOUS VULNERABILITY ASSESSMENT & REMEDIATION

Run **automated vulnerability scanning tools** against all systems on the network on a **weekly or more frequent basis** and deliver prioritized lists of the most critical vulnerabilities to each responsible system administrator **along with risk scores that compare the effectiveness of system administrators and departments in reducing risk.**

SANS/CIS CRITICAL SECURITY CONTROLS

CONTROL 4.1: CONTINUOUS VULNERABILITY ASSESSMENT & REMEDIATION

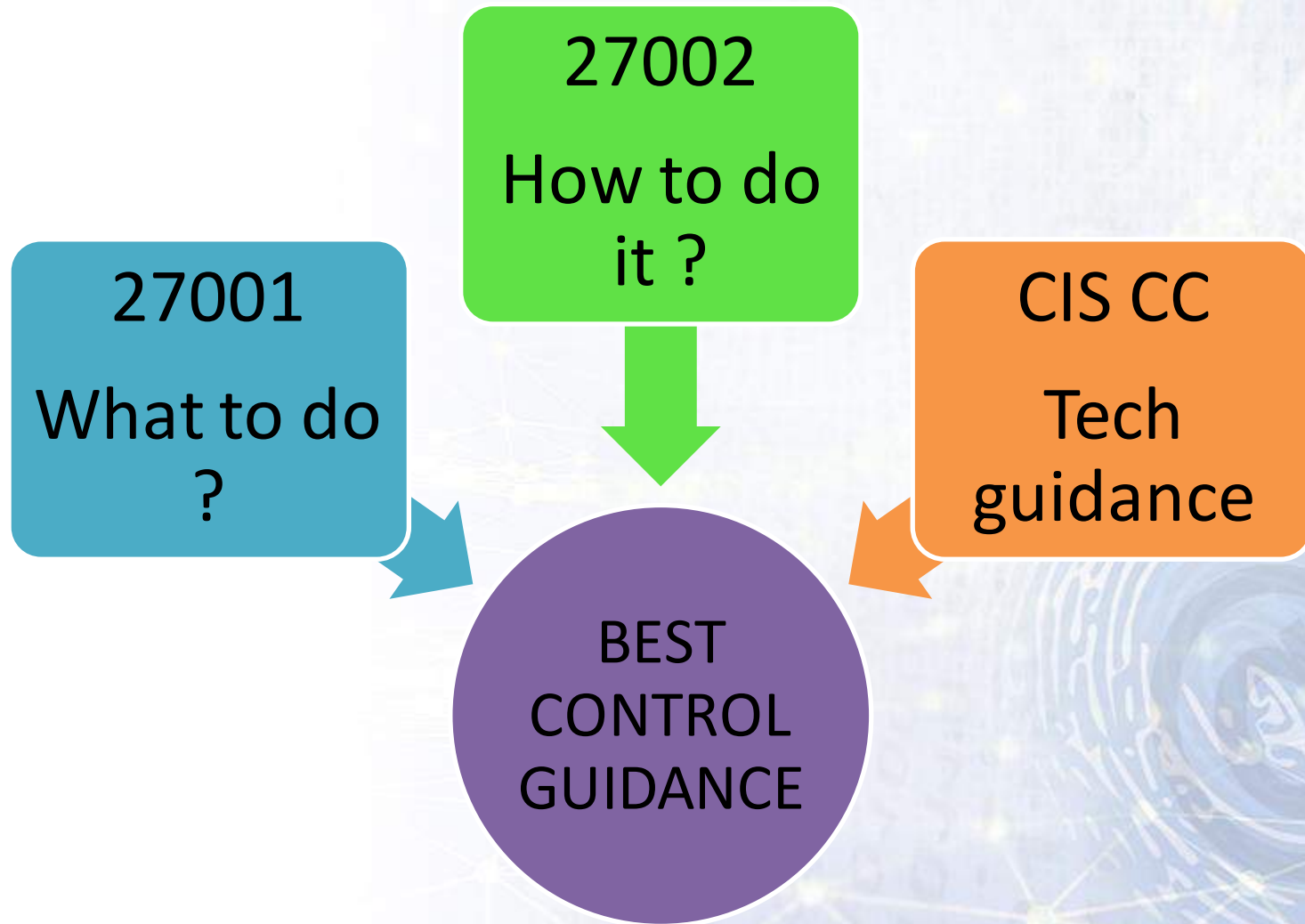
....Use a SCAP-validated vulnerability scanner that looks for both code-based vulnerabilities (such as those described by Common Vulnerabilities and Exposures entries) and configuration-based vulnerabilities (as enumerated by the Common Configuration Enumeration Project).

SANS/CIS CRITICAL SECURITY CONTROLS

CONTROL 5.1 CONTROLLED USE OF ADMIN PRIVILEGES

Minimize administrative privileges and only use administrative accounts when they are required. Implement focused auditing on the use of administrative privileged functions and monitor for anomalous behavior.

SANS/CIS CRITICAL SECURITY CONTROLS



SANS/CIS CRITICAL SECURITY CONTROLS

- An ideal framework for more detailed and specific guidance on deeper and more stringent security controls

END

NIST FRAMEWORK

- The Computer Security Resource Center (CSRC) website guides users to NIST resources on **computer, cyber, and information security and privacy.**

NIST FRAMEWORK

- Its content includes **publications, projects, research, news and events** from the NIST Information Technology Laboratory's (ITL) two security divisions

NIST FRAMEWORK

[CONTACT](#) [SITE MAP](#)

Computer Security Division

Computer Security Resource Center

[CSRC Home](#) [About](#) [Projects / Research](#) [Publications](#) [News & Events](#)

Search

Fulltext search of NIST's computer security publications:

 [Advanced Search](#)

Browse Publications

NEW PUBLICATIONS

- SP 800-67 Rev. 2 (Draft)
- SP 800-190 (2nd Draft)
- NISTIR 8179 (Draft)
- SP 800-192
- SP 800-12 Rev. 1

CSRC HOME > PUBLICATIONS > NIST SPECIAL PUBLICATIONS

NIST SPECIAL PUBLICATIONS (SP)

NIST uses three NIST Special Publication subseries to publish computer/cyber/information security and guidelines, recommendations and reference materials:

- ***SP 800, Computer Security*** (December 1990-present):
NIST's primary mode of publishing computer/cyber/information security ***guidelines, recommendations and reference materials*** (SP 800s are also searchable in the [NIST Library Catalog](#));
- ***SP 1800, NIST Cybersecurity Practice Guides*** (2015-present):
A new subseries created to complement the SP 800s; targets specific cybersecurity challenges in the public and private sectors; ***practical, user-friendly guides*** to facilitate adoption of standards-based approaches to cybersecurity;

NIST FRAMEWORK

- **[SP 800](#), Computer Security** (December 1990-present):
NIST's primary mode of publishing computer/cyber/information security ***guidelines, recommendations and reference materials*** (SP 800s are also searchable in the **[NIST Library Catalog](#)**);

NIST FRAMEWORK

PUBLICATIONS BY TOPIC/PROJECT

Browse FIPS, Special Publications, NISTIRs and ITL Bulletins *by topic or project*:

Security Concepts

- [General IT Security](#)
- [Audit & Accountability](#)
- [Authentication](#)
- [Awareness & Training](#)
- [Certification & Accreditation](#)
- [Contingency Planning](#)
- [Cryptography](#)
- [Digital Signatures](#)
- [Incident Response](#)
- [Maintenance](#)
- [Personal Identity Verification \(PIV\)](#)
- [Planning](#)
- [Privacy](#)
- [Public Key Infrastructure \(PKI\)](#)
- [Research](#)
- [Risk Assessment](#)
- [Security Automation](#)
- [Services & Acquisition](#)
- [Threats & Vulnerability Management](#)
- [Usability](#)

Technologies

- [Biometrics](#)
- [Cloud Computing & Virtualization](#)
- [Communications & Wireless](#)
- [Mobile](#)
- [Smart Cards](#)

Applications

- [Cyber-Physical Systems / Smart Grid](#)
- [Forensics](#)
- [Healthcare](#)
- [Internet of Things \(IoT\)](#)
- [Public Safety](#)
- [Supply Chain](#)
- [Voting](#)

Activities

- [Annual Reports](#)
- [Conferences & Workshops](#)

NIST FRAMEWORK

SP 800s - Computer Security

Number	Date	Title
SP 800-193 (Draft)	May 2017	DRAFT Platform Firmware Resiliency Guidelines ➤ Announcement and Draft Publication
SP 800-192	June 2017	Verification and Test Methods for Access Control Policies/Models 📄 SP 800-192 FAQ doi:10.6028/NIST.SP.800-192 [Direct Link]
SP 800-190 (Draft)	July 2017	DRAFT Application Container Security Guide (2nd Draft) ➤ Announcement and Draft Publication
SP 800-188 (Draft)	December 2016	DRAFT De-Identifying Government Datasets (2nd Draft) ➤ Announcement and Draft Publication
SP 800-187 (Draft)	November 2016	DRAFT Guide to LTE Security ➤ Announcement and Draft Publication
SP 800-185	December 2016	SHA-3 Derived Functions: cSHAKE, KMAC, TupleHash, and ParallelHash 📄 SP 800-185 FAQ doi:10.6028/NIST.SP.800-185 [Direct Link] 📄 Comments Received on Draft SP 800-185
SP 800-184	December	Guide for Cybersecurity Event Recovery

NIST FRAMEWORK

This publication is available free of charge from <http://dx.doi.org/10.6028/NIST.SP.800-147B>

NIST Special Publication 800-147B

BIOS Protection Guidelines for Servers

Andrew Regenscheid

AUGUST 2014
32 PAGES DOC

<http://dx.doi.org/10.6028/NIST.SP.800-147B>

NIST FRAMEWORK

- NIST has a tremendous library of free documentation on a diverse range of topics
- **Relevance is often average, however, depth and detail of material is extraordinary**

END

COBIT

- COBIT:



- ISACA framework for IT Governance
- COBIT 5 helps enterprises to create optimal value from IT by maintaining a balance between realising benefits and optimising risk levels and resource use (ISACA)

COBIT

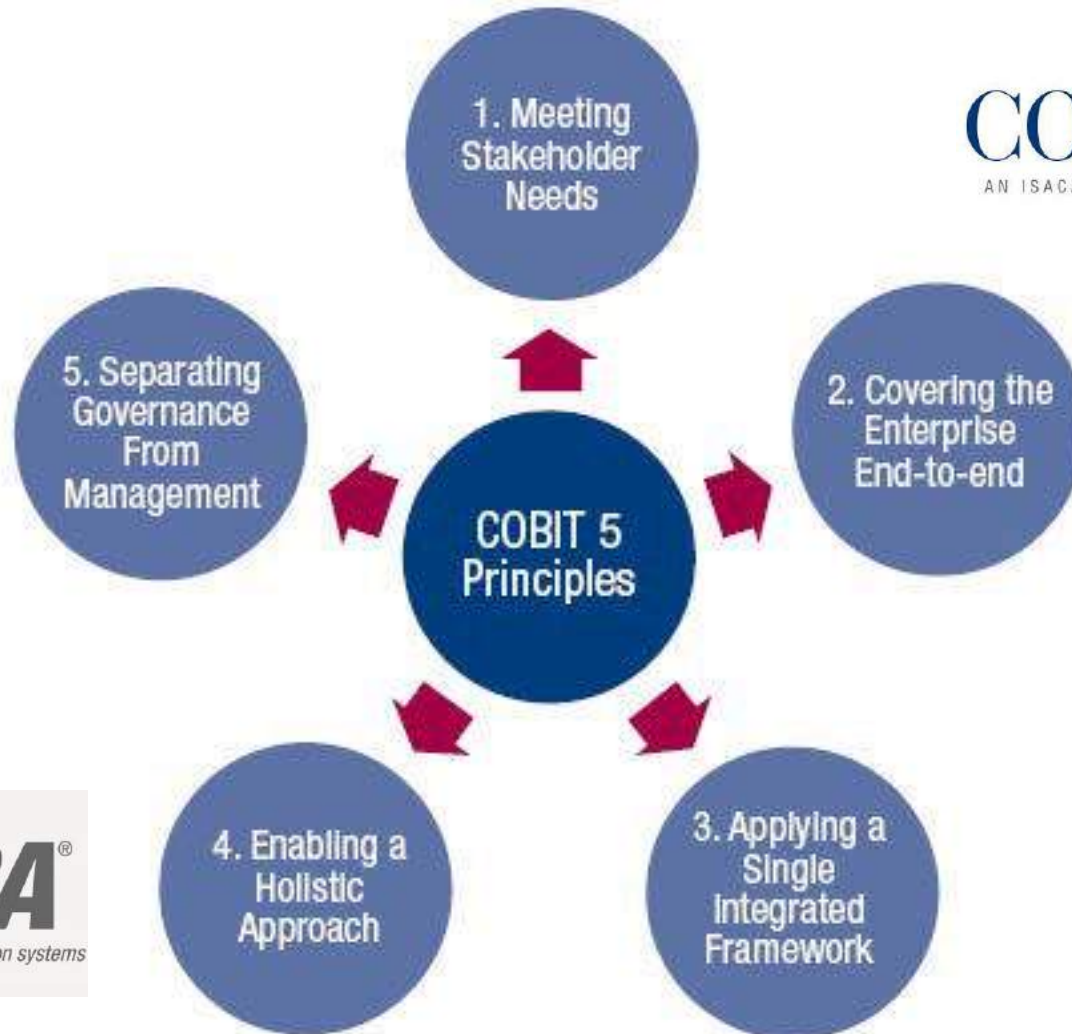


COBIT

- COBIT 5 brings together **five principles** that allow the enterprise to build an effective governance and management framework (ISACA)
- Based on a holistic set of **seven enablers** that optimises IT investment and use for the benefit of stakeholders (ISACA)

COBIT

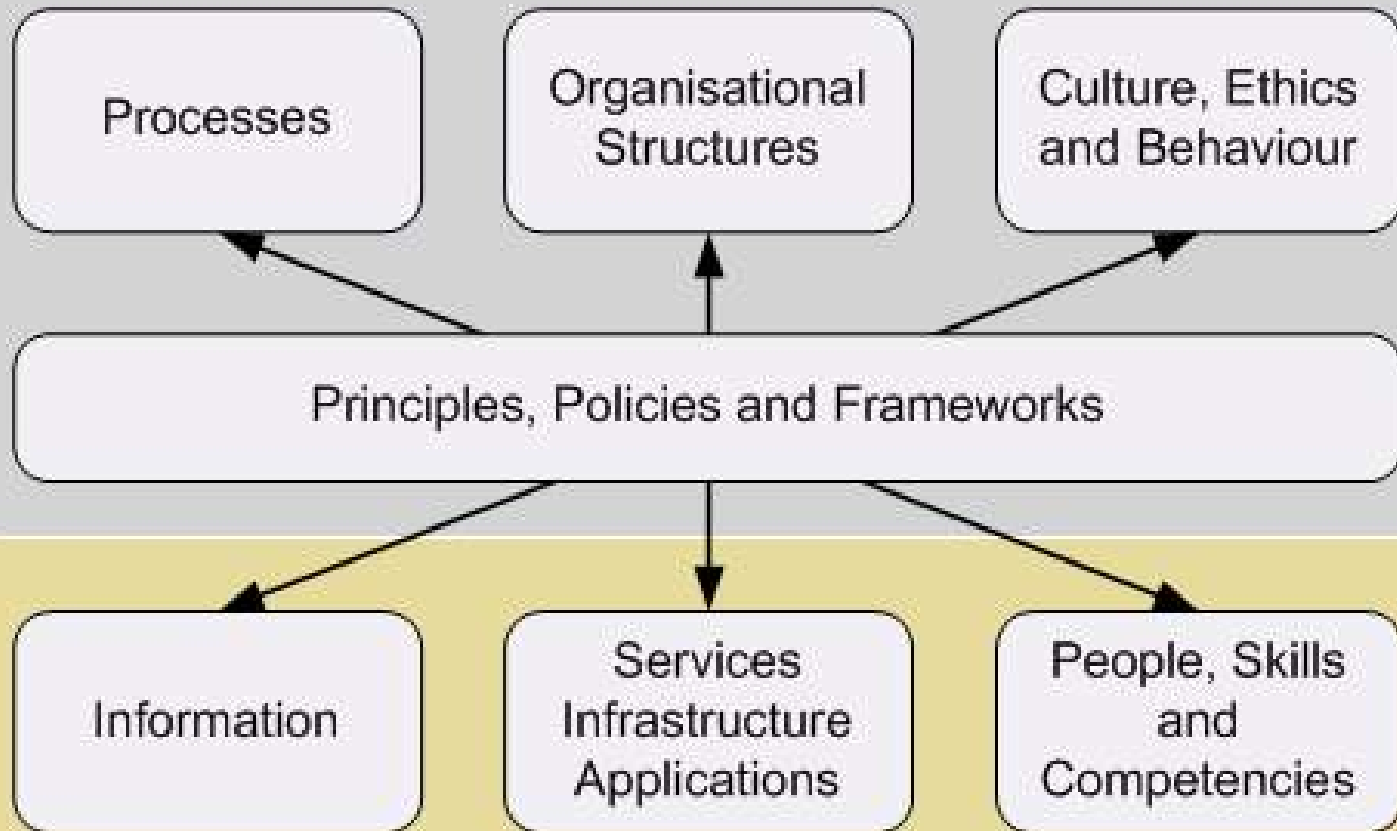
COBIT®
AN ISACA® FRAMEWORK



COBIT



COBIT 5 ENTERPRISE ENABLERS



COBIT

- **Governance** ensures that enterprise objectives are achieved by **evaluating** stakeholder needs, conditions & options; setting **direction** through prioritisation & decision making;

COBIT

- ... & **monitoring** performance, compliance and progress against agreed direction and objectives (**EDM**)



COBIT

- **Management plans, builds, runs and monitors** activities in alignment with the direction set by the governance body to achieve the enterprise objectives (**PBRM**)



COBIT

Processes for Governance of Enterprise IT

Evaluate, Direct and Monitor

EDM01 Ensure Governance Framework Setting and Maintenance

EDM02 Ensure Benefits Delivery

EDM03 Ensure Risk Optimisation

EDM04 Ensure Resource Optimisation

EDM05 Ensure Stakeholder Transparency

Align, Plan and Organise

AP001 Manage the IT Management Framework

AP002 Manage Strategy

AP003 Manage Enterprise Architecture

AP004 Manage Innovation

AP005 Manage Portfolio

AP006 Manage Budget and Costs

AP007 Manage Human Resources

AP008 Manage Relationships

AP009 Manage Service Agreements

AP010 Manage Suppliers

AP011 Manage Quality

AP012 Manage Risk

AP013 Manage Security

Build, Acquire and Implement

BAI01 Manage Programmes and Projects

BAI02 Manage Requirements Definition

BAI03 Manage Solutions Identification and Build

BAI04 Manage Availability and Capacity

BAI05 Manage Organisational Change Enablement

BAI06 Manage Changes

BAI07 Manage Changes Acceptance and Transitioning

BAI08 Manage Knowledge

BAI09 Manage Assets

BAI010 Manage Configuration

Deliver, Service and Support

DSS01 Manage Operations

DSS02 Manage Service Requests and Incidents

DSS03 Manage Problems

DSS04 Manage Continuity

DSS05 Manage Security Services

DSS06 Manage Business Process Controls

Monitor, Evaluate and Assess

MEA01 Monitor, Evaluate and Assess Performance and Conformance

MEA02 Monitor, Evaluate and Assess the System of Internal Control

MEA03 Monitor, Evaluate and Assess Compliance With External Requirements

Processes for Management of Enterprise IT

COBIT®
AN ISACA® FRAMEWORK

COBIT

- COBIT 5 is a detailed framework for IT governance developed by ISACA which has principles, enablers, and processes
- These tools assist implementers and customer organizations to successfully deploy the framework
- Certifiable framework

END

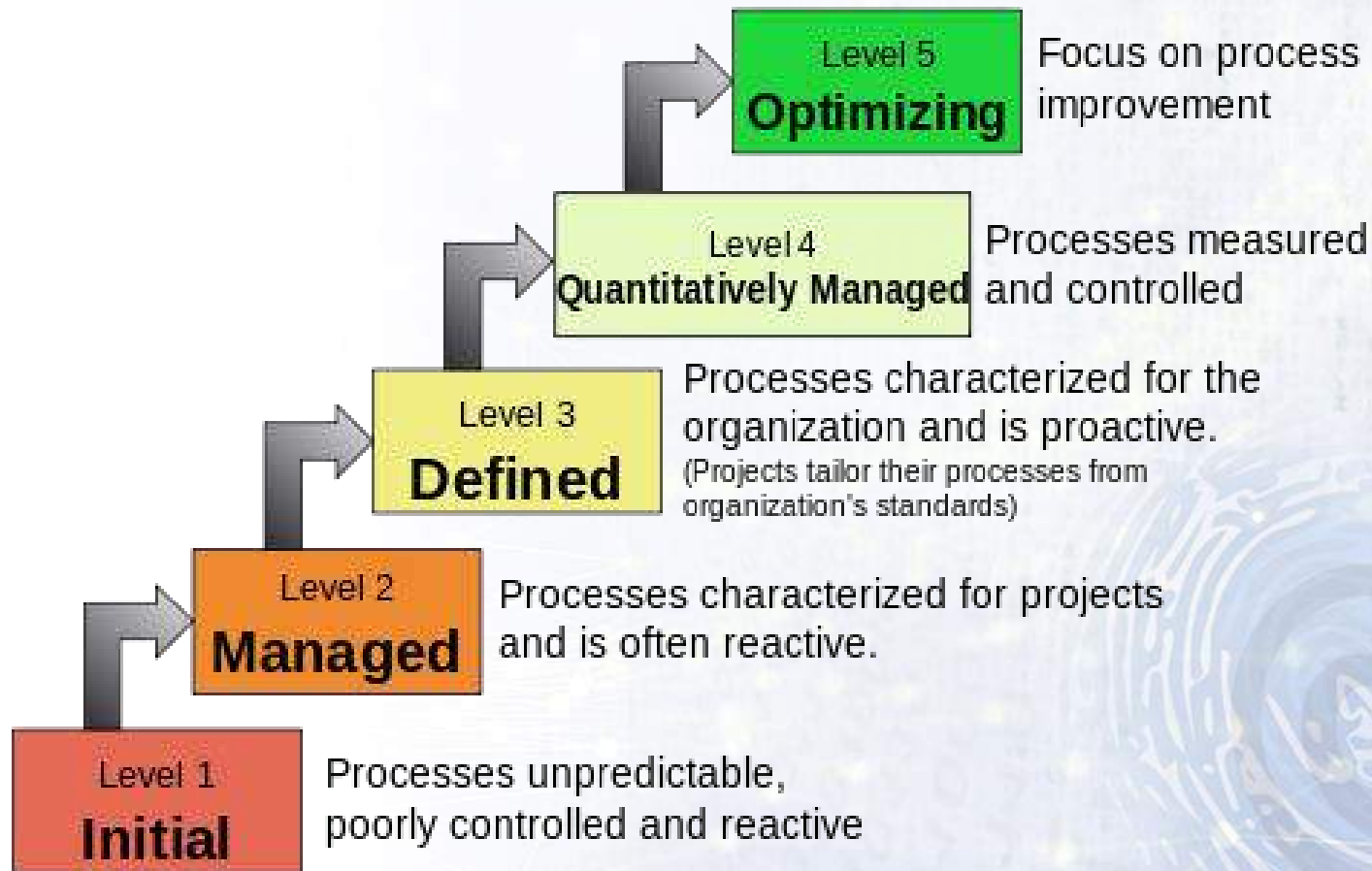
CMMI

- **The Capability Maturity Model (CMM)** is a methodology used to **develop & refine an org's software dev process**. The model describes a **five-level evolutionary path** of increasingly organized & systematically more mature processes.

<http://searchsoftwarequality.techtarget.com/definition/Capability-Maturity-Model>

CMMI

Characteristics of the Maturity levels



https://en.wikipedia.org/wiki/Capability_Maturity_Model_Integration

CMMI

- CMM was developed and is promoted by the [Software Engineering Institute \(SEI\)](#), a research and development center sponsored by the U.S. Department of Defense (DoD)
- **Now CMMI Institute (ISACA)**
<http://searchsoftwarequality.techtarget.com/definition/Capability-Maturity-Model>

CMMI

- **The Capability Maturity Model Integration (CMMI®)** is a performance improvement model for competitive organizations that want to achieve **high-performance operations.**

<http://cmmiinstitute.com/about-cmmi-institute>

CMMI

- Building upon an org's business performance objectives, **CMMI provides a set of practices for improving processes**, resulting in a performance improvement system that paves the way for **better operations and performance.**

<http://cmmiinstitute.com/about-cmmi-institute>

CMMI

- More than any other approach, CMMI **doesn't just help to improve org processes**. CMMI also has **built-in practices** that help to improve the way you use any performance improvement approach, setting you up to achieve a **positive return on your investment**

<http://cmmiinstitute.com/about-cmmi-institute>

CMMI

- CMMI does not provide a single process. Rather, the CMMI provides **guidance on what to do to improve your processes, not define your processes.** CMMI is designed to **compare an organization's existing processes to proven best practices...**

<http://cmmiinstitute.com/about-cmmi-institute>

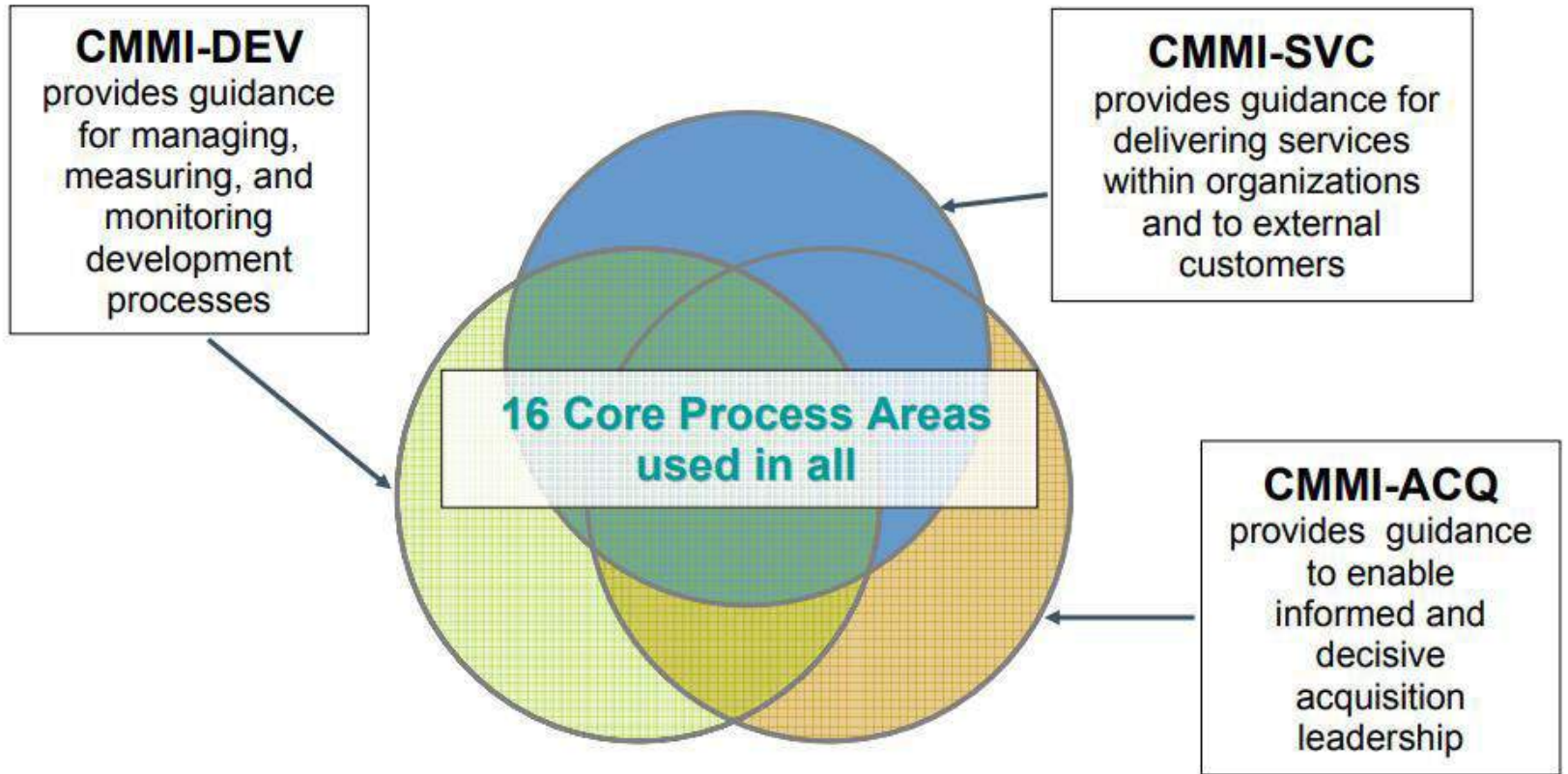
CMMI

- ... developed by members of industry, govt, & academia; **reveal possible areas for improvement; & provide ways to measure progress.**
- CMMI helps **you to build & manage performance improvement systems** that fit your unique environment.

• <http://cmmiinstitute.com/about-cmmi-institute>

CMMI

THREE COMPLEMENTARY CONSTELLATIONS



<http://www.sei.cmu.edu/library/assets/cmmi-overview071.pdf>

CMMI

- CMMI is a very well regarded framework especially in the software industry
- Very useful for demonstrating process & quality capabilities to **customers, partners, and investors**

END

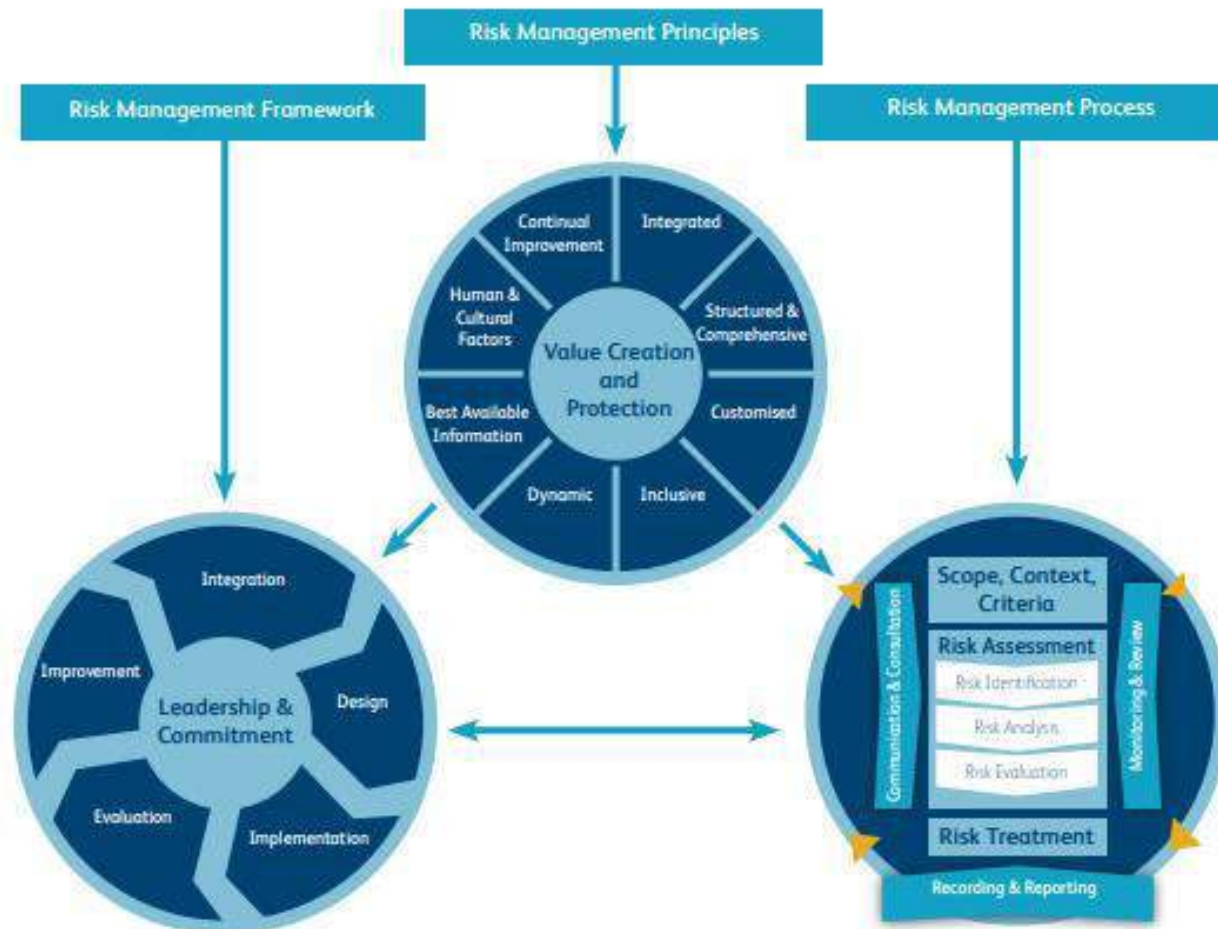
ISO31000:2018 – RISK MANAGEMENT – AN INTRO

A Risk Practitioners Guide
To ISO31000:2018

<https://www.theirm.org/media/3513119/IRM-Report-ISO-31000-2018-v3.pdf>

ISO31000:2018 – RISK MANAGEMENT – AN INTRO

Figure 3: Principles, framework and risk management process from ISO 31000



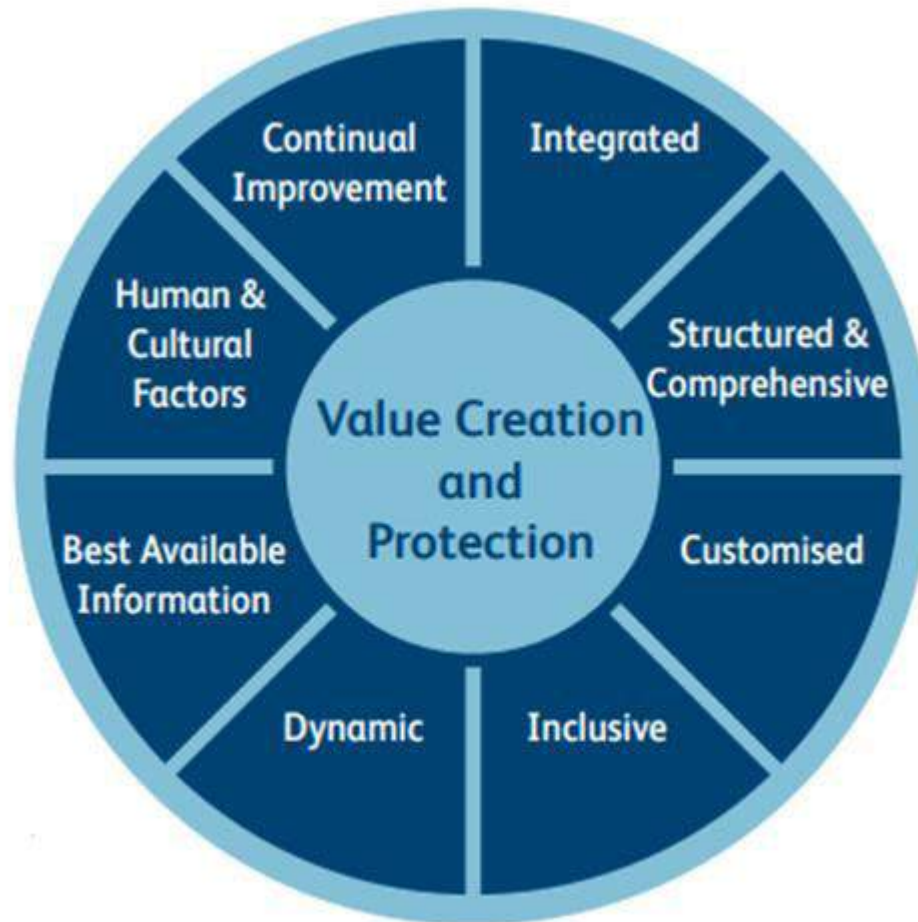
ISO31000:2018 – RISK MANAGEMENT – AN INTRO

Framework
5 components



ISO31000:2018 – RISK MANAGEMENT – AN INTRO

8 PRINCIPLES



ISO31000:2018 – RISK MANAGEMENT – AN INTRO

RISK MANAGEMENT PROCESS



ISO31000:2018 – RISK MANAGEMENT – AN INTRO

ISO31000 objectives:

- ISO 31000 states that the guidelines should be used by people who create and protect value in organisations by managing risks, making decisions, setting and achieving objectives and improving performance.

<https://www.iso.org/obp/ui/#iso:std:iso:31000:ed-2:v1:en>

ISO31000:2018 – RISK MANAGEMENT – AN INTRO

ISO31000 purpose:

- ISO 31000 states that the purpose of risk management is the creation and protection of value.

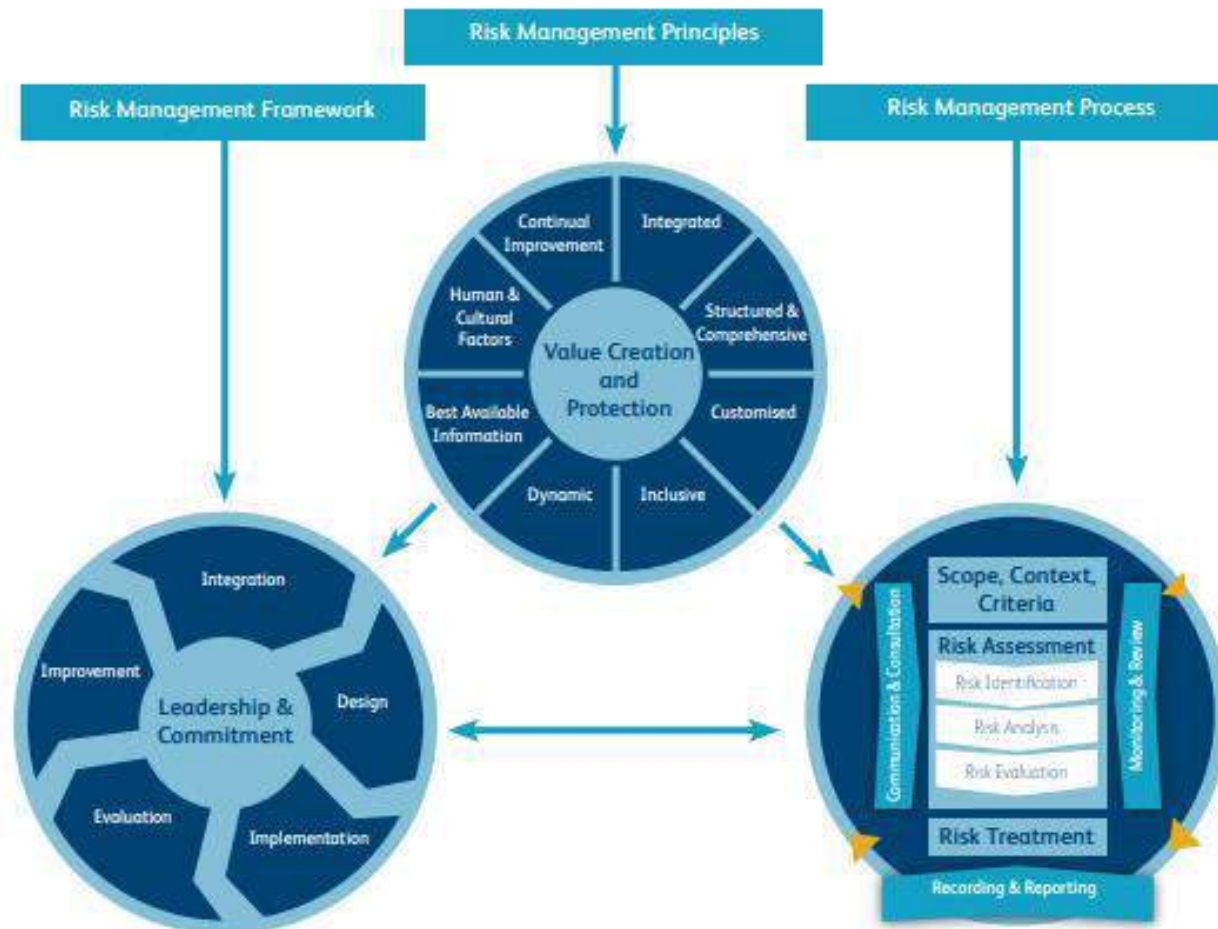
ISO31000:2018 – RISK MANAGEMENT – 8 PRINCIPLES

A Risk Practitioners Guide
To ISO31000:2018

<https://www.theirm.org/media/3513119/IRM-Report-ISO-31000-2018-v3.pdf>

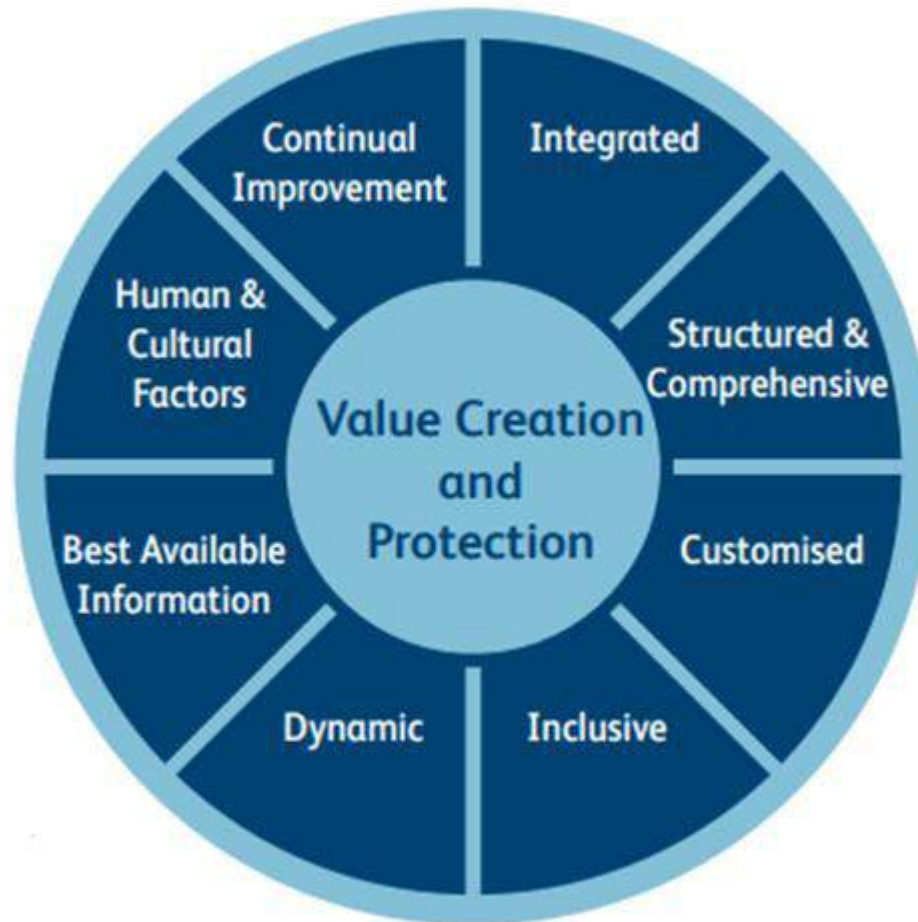
ISO31000:2018 – RISK MANAGEMENT – AN INTRO

Figure 3: Principles, framework and risk management process from ISO 31000



ISO31000:2018 – RISK MANAGEMENT – AN INTRO

8 PRINCIPLES



ISO31000:2018 – RISK MANAGEMENT – 8 PRINCIPLES

PRINCIPLES:

1. Framework and processes should be customized and proportionate.
2. Appropriate and timely involvement of stakeholders is necessary.
3. Structured and comprehensive approach is required.

ISO31000:2018 – RISK MANAGEMENT – 8 PRINCIPLES

PRINCIPLES:

- 4. Risk management is an integral part of all organizational activities.
- 5. Risk management anticipates, detects, acknowledges and responds to changes.
- 6. Risk management explicitly considers any limitations of available information.

ISO31000:2018 – RISK MANAGEMENT – 8 PRINCIPLES

PRINCIPLES:

7. Human and cultural factors influence all aspects of risk management.

8. Risk management is continually improved through learning and experience.

ISO31000:2018 – RISK MANAGEMENT – 8 PRINCIPLES

- The first five principles provide guidance on how a risk management initiative should be designed, and principles six, seven and eight relate to the operation of the risk management initiative.

ISO31000:2018 – RISK MANAGEMENT – 8 PRINCIPLES

- The latter principles confirm that the best information available should be used; human and cultural factors should be considered; and the risk management arrangements should ensure continual improvement.

ISO31000:2018 – RISK MANAGEMENT – 8 PRINCIPLES

- The first five principles are concerned with the design and planning of the risk management initiative and these principles are often summarized as proportionate, aligned, comprehensive, embedded and dynamic (PACED), as shown in Table 1.

ISO31000:2018 – RISK MANAGEMENT – AN INTRO

Table 1: Principles of risk management

Principle	Description
Proportionate	Risk management activities must be proportionate to the level of risk faced by the organisation.
Aligned	Risk management activities need to be aligned with the other activities in the organisation.
Comprehensive	In order to be fully effective, the risk management approach must be comprehensive.
Embedded	Risk management activities need to be embedded within the organisation.
Dynamic	Risk management activities must be dynamic and responsive to emerging and changing risks.

ISO31000:2018 – RISK MANAGEMENT – 8 PRINCIPLES

A Risk Practitioners Guide
To ISO31000:2018

<https://www.theirm.org/media/3513119/IRM-Report-ISO-31000-2018-v3.pdf>

END

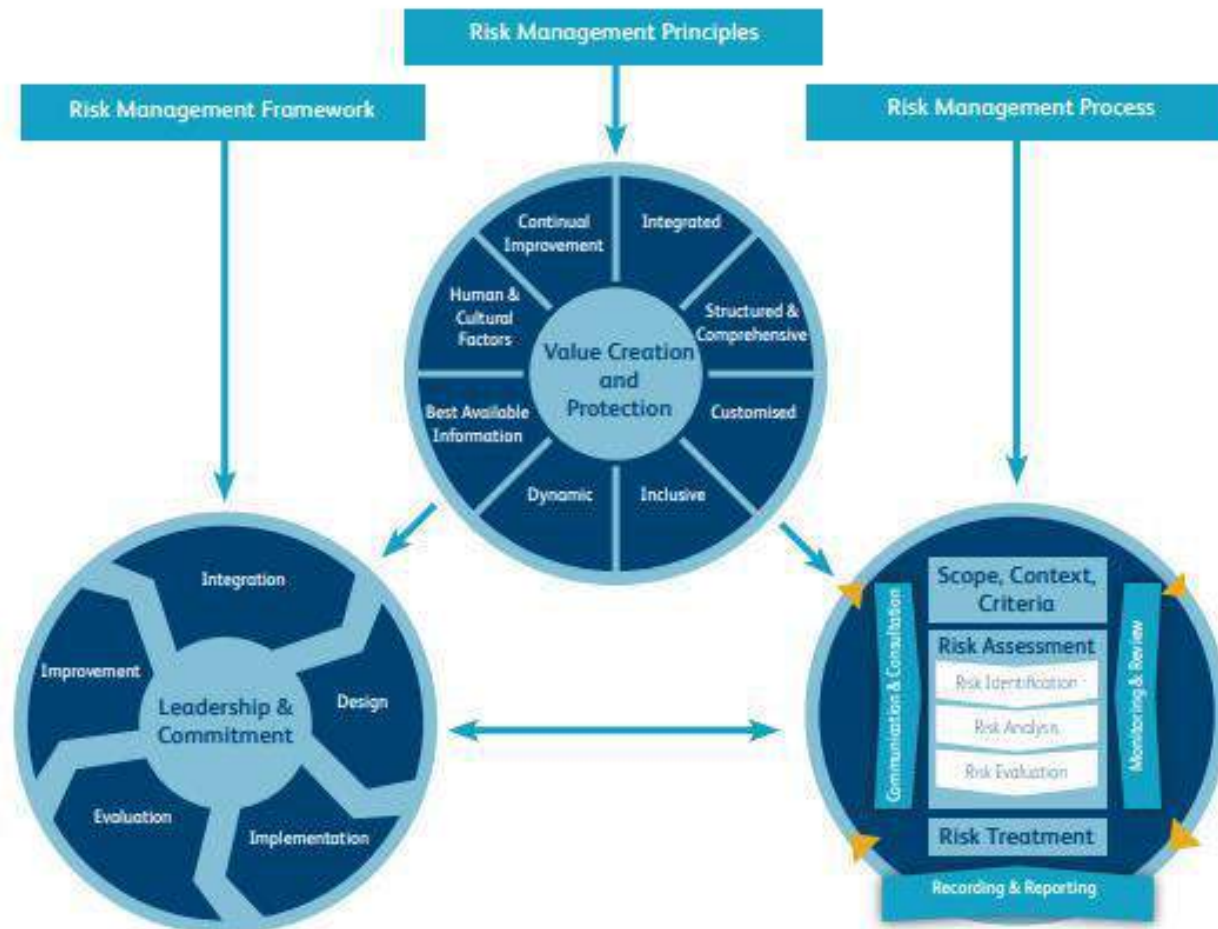
ISO31000:2018 – RISK MANAGEMENT – FRAMEWORK

A Risk Practitioners Guide
To ISO31000:2018

<https://www.theirm.org/media/3513119/IRM-Report-ISO-31000-2018-v3.pdf>

ISO31000:2018 – RISK MANAGEMENT – FRAMEWORK

Figure 3: Principles, framework and risk management process from ISO 31000



ISO31000:2018 – RISK MANAGEMENT – FRAMEWORK

Framework
5 components



ISO31000:2018 – RISK MANAGEMENT – FRAMEWORK

- The principles of risk management and the **framework** are closely related.
- For example, one of the principles is that risk management should be integrated and one of the components of the framework is **integration**.

ISO31000:2018 – RISK MANAGEMENT – FRAMEWORK

- The principle outlines what must be achieved, and the framework provides information on how to achieve the required **integration**.

ISO31000:2018 – RISK MANAGEMENT – FRAMEWORK

- The ISO 31000 guidelines are centered on leadership and commitment.
- The effectiveness of risk management will depend on its **integration** into all aspects of the organization, including decision-making.

ISO31000:2018 – RISK MANAGEMENT – FRAMEWORK

- The remaining components of the framework are **design, implementation, evaluation and improvement**. This approach is often represented in management literature as plan-do-check-act.

ISO31000:2018 – RISK MANAGEMENT – FRAMEWORK

- ISO 31000 provides narrative description of how the framework should support risk management activities in an organization.
- This is often referred to as the **risk architecture, strategy and protocols** of the organization, as set out in Table 2.

ISO31000:2018 – RISK MANAGEMENT – FRAMEWORK

RISK MANAGEMENT FRAMEWORK

- ARCHITECTURE
- STRATEGY
- PROTOCOLS

Table 2: Risk management framework

Risk management architecture

- Committee structure and terms of reference
- Roles and responsibilities
- Internal reporting requirements
- External reporting controls
- Risk management assurance arrangements

Risk management strategy

- Risk management philosophy
- Arrangements for embedding risk management
- Risk appetite and attitude to risk
- Benchmark tests for significance
- Specific risk statements/policies
- Risk assessment techniques
- Risk priorities for the present year

Risk management protocols

- Tools and techniques
- Risk classification system
- Risk assessment procedures
- Risk control rules and procedures
- Responding to incidents, issues and events
- Documentation and record keeping
- Training and communications
- Audit procedures and protocols
- Reporting/disclosures/certification

ISO31000:2018 – RISK MANAGEMENT – FRAMEWORK

A Risk Practitioners Guide
To ISO31000:2018

<https://www.theirm.org/media/3513119/IRM-Report-ISO-31000-2018-v3.pdf>

END

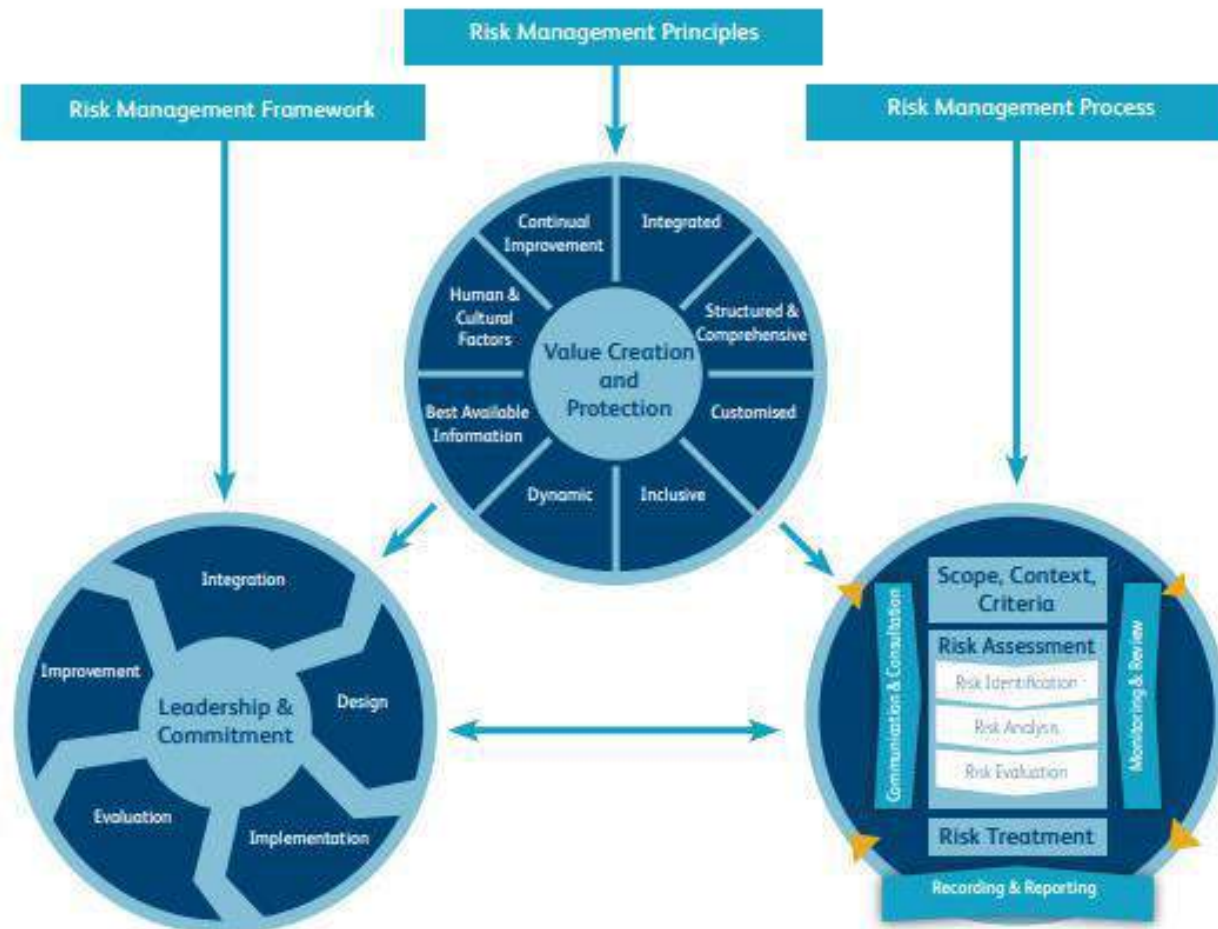
ISO31000:2018 – RISK MANAGEMENT – PROCESS

A Risk Practitioners Guide
To ISO31000:2018

<https://www.theirm.org/media/3513119/IRM-Report-ISO-31000-2018-v3.pdf>

ISO31000:2018 – RISK MANAGEMENT – PROCESS

Figure 3: Principles, framework and risk management process from ISO 31000



ISO31000:2018 – RISK MANAGEMENT – PROCESS

RISK MANAGEMENT PROCESS



ISO31000:2018 – RISK MANAGEMENT – PROCESS

At the center of the risk management process are the activities of **risk assessment and risk treatment**.

Risk assessment is described as having the three stages of **risk identification, risk analysis and risk evaluation**.

ISO31000:2018 – RISK MANAGEMENT – PROCESS

- Each of the three stages is described in detail in ISO 31000 and it provides valuable insight into how risks can be **identified**, how they can be **analyzed** in terms of likelihood and consequences and finally, how they can be **evaluated** in relation to

ISO31000:2018 – RISK MANAGEMENT – PROCESS

- ..the **established risk criteria (risk appetite)** to determine whether additional action is required.

ISO31000:2018 – RISK MANAGEMENT – PROCESS

- Risk **treatment** is also a vitally important part of the risk management process and ISO 31000 provides information on the selection of **risk treatment options**, the preparation and implementation of **risk treatment plans**.

ISO31000:2018 – RISK MANAGEMENT – PROCESS

- ISO 31000 states that the selection of **risk treatment options** involves balancing the potential benefits of introducing further risk treatment (controls) against the associated cost, effort or disadvantages.

ISO31000:2018 – RISK MANAGEMENT – PROCESS

- The **risk treatment plan** should clearly identify the timescale and responsibilities for implementing the selected **risk treatments**.

END

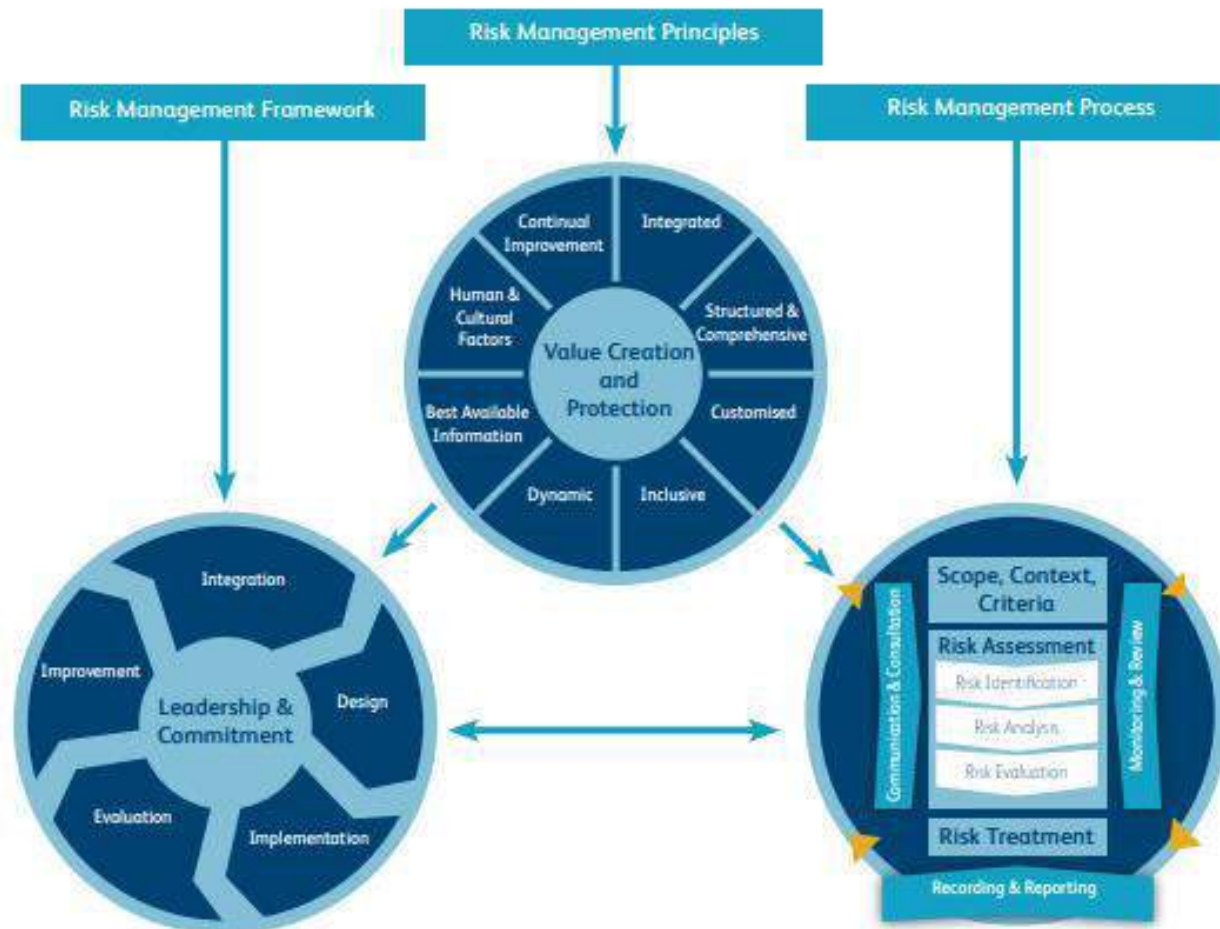
ISO31000:2018 – RISK MANAGEMENT – HOW TO IMPLEMENT

A Risk Practitioners Guide
To ISO31000:2018

<https://www.theirm.org/media/3513119/IRM-Report-ISO-31000-2018-v3.pdf>

ISO31000:2018 – RISK MANAGEMENT – HOW TO IMPLEMENT

Figure 3: Principles, framework and risk management process from ISO 31000



Successful implementation of a risk management initiative is an ongoing process that involves working through 10 activities below on a continuous basis. These activities relate to:

- (1) Plan;
- (2) Implement;
- (3) Measure; and
- (4) Learn.

Plan:

1. Identify intended benefits of the RM initiative and gain board support
2. Plan the scope of the RM initiative and develop common language of risk
3. Establish the RM strategy, framework and the roles and responsibilities

Implement:

4. Adopt suitable risk assessment tools and an agreed risk classification system
5. Establish risk benchmarks (risk criteria) & undertake risk assessments
6. Determine risk appetite and risk tolerance levels and evaluate the existing controls

Measure:

- 7. Evaluate effectiveness of existing controls and introduce improvements
- 8. Embed risk-aware culture and align RM with other activities in the organization

Learn

- 9. Monitor and review risk performance indicators to measure RM contribution
- 10. Report risk performance in line with obligations and monitor improvement

Although ISO 31000 covers the full scope of requirements for a management system, it is for the organization to convert those requirements into a checklist and action plan.

END

INCIDENT MANAGEMENT-I

Information Security Incident Management

- Have a look at ISO27002: 2013 (Page 67+) for best practices guidance

INCIDENT MANAGEMENT-I

Objective:

- “To ensure a consistent and effective approach to the management of information security incidents, including communication on security events and weaknesses.”

ISO27001:2013 (16.1)

INCIDENT MANAGEMENT-I

Top 10 Considerations For Incident Response

<https://www.owasp.org/images/9/92/Top10ConsiderationsForIncidentResponse.pdf>

INCIDENT MANAGEMENT-I

WHY IS INCIDENT RESPONSE IMPORTANT?



<https://www.owasp.org/images/9/92/Top10ConsiderationsForIncidentResponse.pdf>

INCIDENT MANAGEMENT-I

1. Audit & Due Diligence

Performing an audit will let you know how well prepared the organization is for Incident Response in terms of:

- People
- Process
- Equipment

INCIDENT MANAGEMENT-I

2. Create Response Team

An Incident Response team should consist of people with sufficient technical skills. It is important that the team members consist of SME's (Subject Matter Experts) or Knowledge Engineers from different domains across the organization.

INCIDENT MANAGEMENT-I

2. Create Response Team

- Team lead
- Triage officer
- Incident handler

INCIDENT MANAGEMENT-I

3. Create Documented IR Plan

An organization should have a well-documented IR plan that would guide the IR Team during an incident.

A comprehensive plan at minimum, should cover Roles & Responsibilities, Investigation, Triage and Mitigation, Recovery, and Documentation process.

4. Identify Indicators & Triggers

- What would be categorized as an incident at your organization?
- How important or weighty are the factors that would trigger an incident?
- Clearly define what can trigger an incident

INCIDENT MANAGEMENT-I

5. Investigate the Problem

- Establishing, clearly what has occurred
- Identify what systems, people or processes have been compromised or affected based on incident
- Determine what happened & what was compromised

INCIDENT MANAGEMENT-I

5. Investigate the Problem

- Determine the point of origin of the incident where possible. This infers that you establish the source of the threat or attack vector
- Specify your investigation objectives, triage and resolution methodology

END

INCIDENT MANAGEMENT-II

Top 10 Considerations For Incident Response

<https://www.owasp.org/images/9/92/Top10ConsiderationsForIncidentResponse.pdf>

6. Triage & Mitigation

Investigation leads to the triage and resolution process. As the team identifies potential exposure, they should plan and execute effective mitigation accordingly:

- Classification of Incident
- Incident Prioritization
- Assigning specific tasks to specific people

INCIDENT MANAGEMENT-II

7. Recovery

Once a thorough investigation has been carried out, recovery is a significant step for restoring services or materials that might have been affected during an incident. This could be the task of the technical team (transition from active incident to standard monitoring)

8. Documentation & Reporting

A comprehensive incident report is required in keeping with best practices and with the Incident Response plan. The type of reports that might be required might vary but should help in managing and reviewing incidents satisfactorily.

9. Process Review

Make intelligent decisions about important factors:

- Should I increase or decrease the number of Incident Handlers?
- What risks did we identify during the incident that needs to be followed up for action and monitored closely?

INCIDENT MANAGEMENT-II

10. Practice, Practice, Practice !

Do not wait until an incident occurs before you put your team to work. Once the organization has a workable plan in place, it is advisable to run through part or all of it as a tabletop exercise, and run through various scenarios and drills.

END

CHANGE MANAGEMENT-I

ITIL CHANGE MANAGEMENT BEST PRACTICES

<http://www.bmc.com/guides/itil-change-management.html>

CHANGE MANAGEMENT-I



CHANGE MANAGEMENT-I

ITIL change management is a process designed to understand and minimize risks while making IT changes. Businesses have two main expectations of the services provided by IT:

CHANGE MANAGEMENT-I

1. The services should be stable, reliable, and predictable.
2. The services should be able to change rapidly to meet evolving business requirements.

CHANGE MANAGEMENT-I

- These expectations are in conflict. The objective of change management is to enable IT service management to meet both expectations—to enable rapid change while minimizing the possibility of disruption to services.

CHANGE MANAGEMENT-I

Types Of Changes

Standard changes are changes to a service or to the IT infrastructure where the implementation process and the risks are known upfront.

- These changes are managed according to policies that are the IT organization already has in place.

CHANGE MANAGEMENT-I

- Since these changes are subject to established policies and procedures, they are the easiest to prioritize and implement, and often don't require approval from a risk management perspective.

CHANGE MANAGEMENT-I

Normal Changes

- Those that must go through the change process before being approved and implemented. If they are determined to be high-risk, a change advisory board must decide whether they will be implemented.

CHANGE MANAGEMENT-I

Emergency Changes

- Arise when an unexpected error or threat occurs, such as when a flaw in the infrastructure related to services needs to be addressed immediately. A security threat is another example of an emergency situation that requires changes to be made immediately.

END

CHANGE MANAGEMENT-II

ITIL CHANGE MANAGEMENT BEST PRACTICES

<http://www.bmc.com/guides/itil-change-management.html>

CHANGE MANAGEMENT-II



CHANGE MANAGEMENT-II

Mission

The mission of the IT change management process is to implement changes in the most efficient manner, while minimizing the negative impact on customers when changes are implemented. KPIs for tracking success of the IT change management process are:

CHANGE MANAGEMENT-II

i. Successful changes: The number of changes that have been completed successfully compared to the total number of completed changes. The higher the percentage of successful changes, the better.

CHANGE MANAGEMENT-II

ii. Backlog of changes: The number of changes that are not yet completed. While this absolute number depends on the size of the organization, it should not grow over time.

CHANGE MANAGEMENT-II

iii. Emergency changes:

The number of completed “emergency” changes.

This absolute number depends on the size of the organization and should not increase over time.

CHANGE MANAGEMENT-II

Scope

The scope of the IT change management process is limited to change implementations that will cause:

- i. A service to become unavailable or degraded during service hours

CHANGE MANAGEMENT-II

Scope

- ii. The functionality of a service to become different
- iii. The CMDB to require an update

Other IT changes don't usually require formal change management. Instead, they can be tracked as standard IT activities.

CHANGE MANAGEMENT-II

IT Change Management Procedures

a. Request for change review: Change coordinators use this procedure when they are dealing with requests for change.

CHANGE MANAGEMENT-II

b. Change planning:

Change coordinators and specialists employ this process to prepare the implementation plans for changes.

c. Change approval: The change manager and approvers (e.g., customer representatives and service owners) follow this procedure to approve planned changes.

CHANGE MANAGEMENT-II

d. Change implementation:

Specialists use this process to implement infrastructure changes.

e. change closure:

Specialists follow this procedure when they perform production tests after changes have been implemented, and change coordinators employ it to close out changes.

END

CHANGE MANAGEMENT-III

ITIL CHANGE MANAGEMENT BEST PRACTICES

<http://www.bmc.com/guides/itil-change-management.html>

CHANGE MANAGEMENT-III



CHANGE MANAGEMENT-III

CHANGE MANAGEMENT ROLES

The **change initiator** recognizes and identifies the need for change.

- The initiator should be someone who works directly with support services tools.

CHANGE MANAGEMENT-III

CHANGE MANAGEMENT ROLES

- Members of your team who provide support services to customers may be best suited for this position due to their frequent interaction with the system.

CHANGE MANAGEMENT-III

CHANGE MANAGEMENT ROLES

The **change coordinator** assesses requests for change that originate from incident management, problem management, release management, or continuity management.

CHANGE MANAGEMENT-III

CHANGE MANAGEMENT ROLES

- The change coordinator registers changes as needed to handle requests for change or receives change requests from other change initiators; determines the risk and impact for requested changes;

CHANGE MANAGEMENT-III

CHANGE MANAGEMENT ROLES

- prepares implementation plans by creating tasks; and monitors the progress of changes.

CHANGE MANAGEMENT-III

CHANGE MANAGEMENT ROLES

The **change manager** is generally needed in mid-sized and larger organizations. If your IT department is part of a larger company, you will need to pick one or multiple persons to perform the role of change manager.

CHANGE MANAGEMENT-III

CHANGE MANAGEMENT ROLES

- These individuals are responsible for managing change procedures, receiving and prioritizing change requests, evaluating the risk level associated with requests, and keeping thorough records of the outcome of each change.

CHANGE MANAGEMENT-III

CHANGE MANAGEMENT ROLES

The **change advisory board** is responsible for authorizing changes and further evaluating requests when the change manager determines that there is a high risk associated with these requests.

CHANGE MANAGEMENT-III

CHANGE MANAGEMENT ROLES

- The board takes into account the impact that a requested change may have on all affected parties.
- When these high-risk changes are brought to the attention of the change advisory board, the board will ...

CHANGE MANAGEMENT-III

CHANGE MANAGEMENT ROLES

- ...schedule a meeting with a detailed agenda to determine how to proceed.

CHANGE MANAGEMENT-III

CHANGE MANAGEMENT ROLES

The **approver** decides whether to approve or reject changes.

CHANGE MANAGEMENT-III

CHANGE MANAGEMENT ROLES

The **change implementation team** consists of the specialists on your team who are responsible for actually making changes.

CHANGE MANAGEMENT-III

CHANGE MANAGEMENT ROLES

- You will likely be part of this team and employees directly under you may also be assigned to implement changes.
- As an IT manager, you will often be responsible for overseeing changes.

END

PROJECT MANAGEMENT FOR INFOSEC: PART 1

- **PART 1:**
 - IMPORTANCE OF PROJECT MANAGEMENT FOR INFORMATION SECURITY

- **CYBER SECURITY CHALLENGES:**
 1. Reactive
 2. Superficial
 3. Contention
 4. Box-Approach
 5. Governance-Overkill

Denial During The Last 10 Years

PROJECT MANAGEMENT FOR INFOSEC: PART 1

- **Effective project management makes or breaks any project**
- Project management is the sum-total of managing, organizing, and prioritizing all resources, and tasks in order to achieve a successful outcome within the stipulated timeframe

PROJECT MANAGEMENT FOR INFOSEC: PART 1

- Successful Security Transformation Implementation is heavily dependent upon the project being in the hands of an experienced project manager:
 - Has **authority**
 - Has **domain knowledge**
 - Has ability to suggest **solutions**

PROJECT MANAGEMENT FOR INFOSEC: PART 1

- In a nut-shell, effective project management for Security Transformation is about understanding the landscape, understanding what is required to solve the problem, **and being fully committed to ensure that the successful outcome is achieved within time**

PROJECT MANAGEMENT FOR INFOSEC: PART 1

- Common Challenges During Projects:
 - **Discipline during the one year duration**
 - **Prior shortage of resources**
 - **New initiatives (diversions)**
 - **Constant slippage of tasks**
 - **Lack of commitment by team members**

PROJECT MANAGEMENT FOR INFOSEC: PART 1

END

- Without bold, well-organized, disciplined, and committed project management, the Security Transformation cannot be achieved within an organization
- Effective project management is the cornerstone of achieving success for Security Transformation projects

PROJECT MANAGEMENT FOR INFOSEC: PART 2

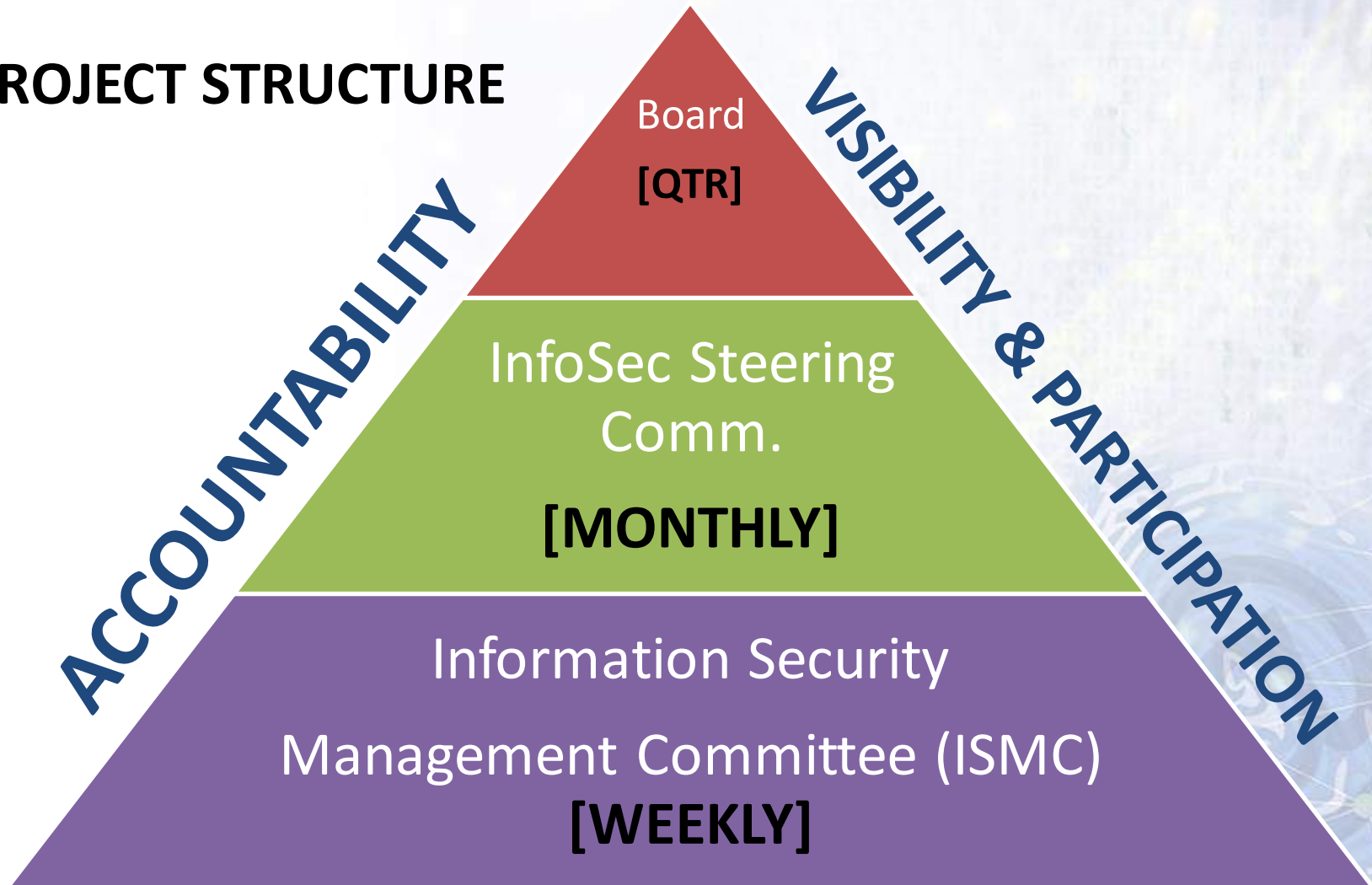
- **PART 2:**
 - STRUCTURE

PROJECT MANAGEMENT FOR INFOSEC: PART 2

- **Structure** refers to the hierarchy and organization of teams, their interaction along with frequency, reporting, and problem-resolution mechanisms

PROJECT MANAGEMENT FOR INFOSEC: PART 2

PROJECT STRUCTURE



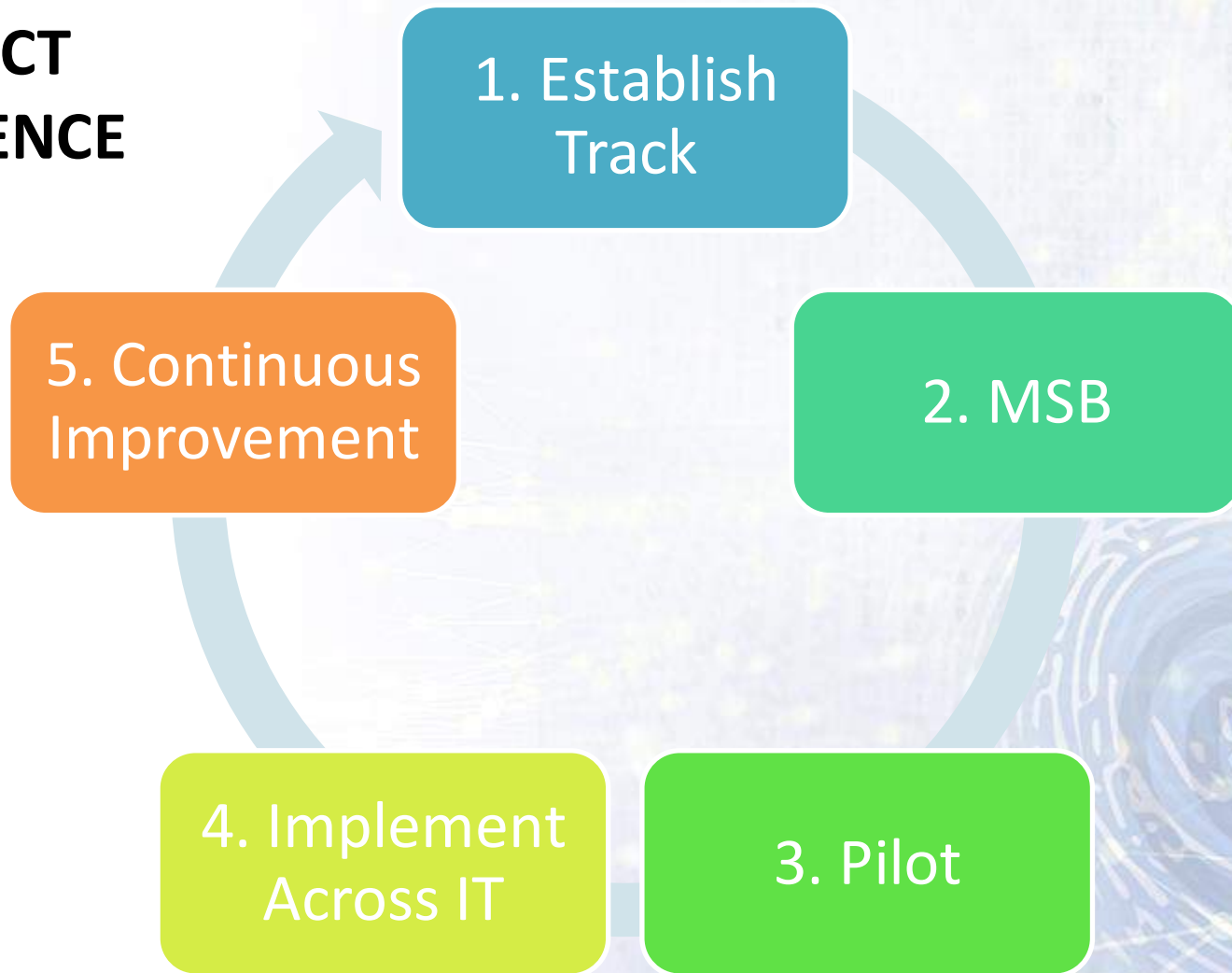
PROJECT MANAGEMENT FOR INFOSEC: PART 2

TEAM STRUCTURE

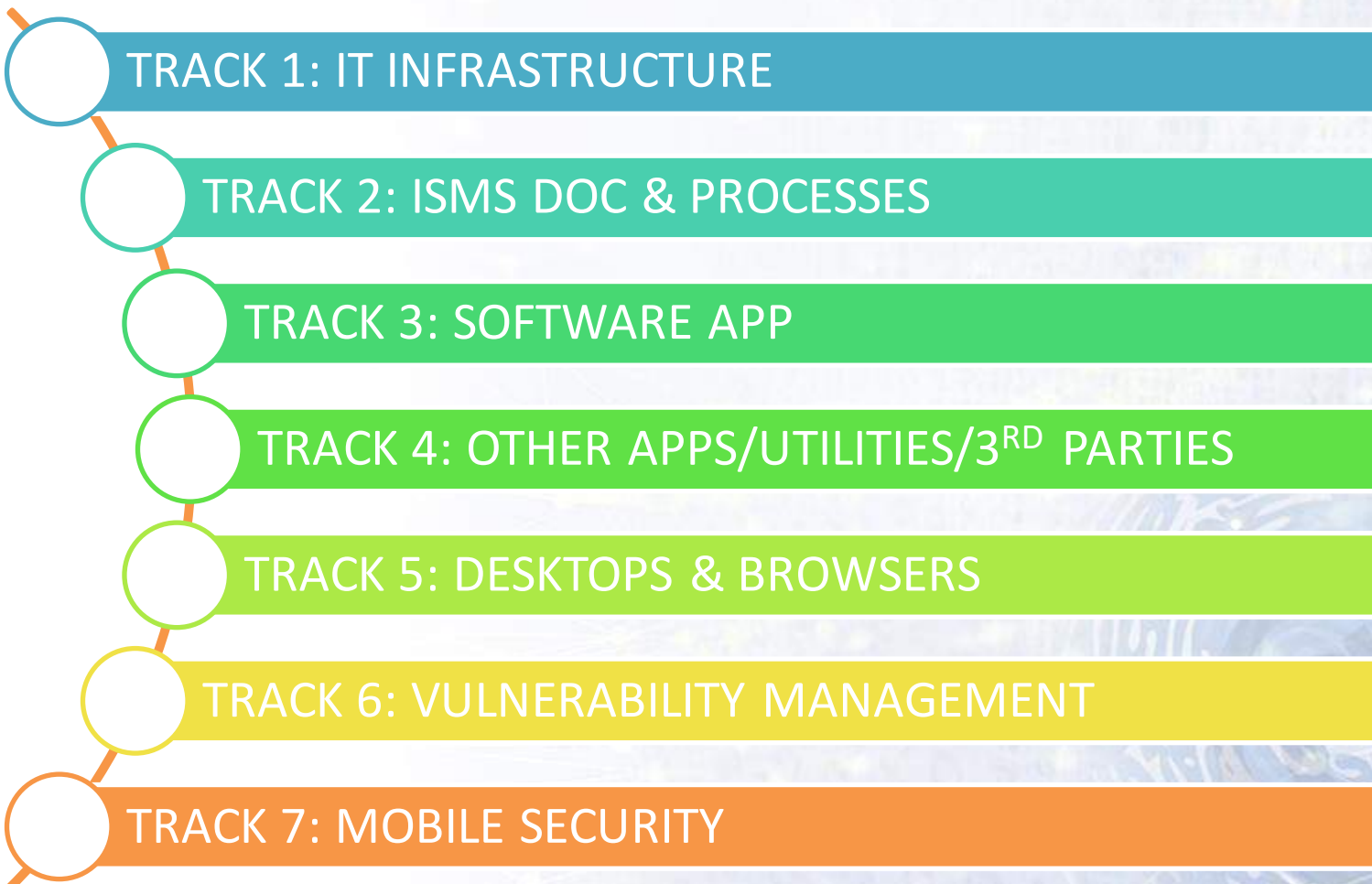


PROJECT MANAGEMENT FOR INFOSEC: PART 2

PROJECT SEQUENCE



PROJECT MANAGEMENT FOR INFOSEC: PART 2



TRACK 1: IT INFRASTRUCTURE

TRACK 2: ISMS DOC & PROCESSES

TRACK 3: SOFTWARE APP

TRACK 4: OTHER APPS/UTILITIES/3RD PARTIES

TRACK 5: DESKTOPS & BROWSERS

TRACK 6: VULNERABILITY MANAGEMENT

TRACK 7: MOBILE SECURITY

PROJECT MANAGEMENT FOR INFOSEC: PART 2

- **An effective project manager has a thorough understanding of what needs to be achieved, and is able to orchestrate resources, teams, hierarchy, and reporting in order to achieve a successful project outcome**

END

PROJECT MANAGEMENT FOR INFOSEC: PART 3

- **PART 3:**
 - REPORTING

PROJECT MANAGEMENT FOR INFOSEC: PART 3

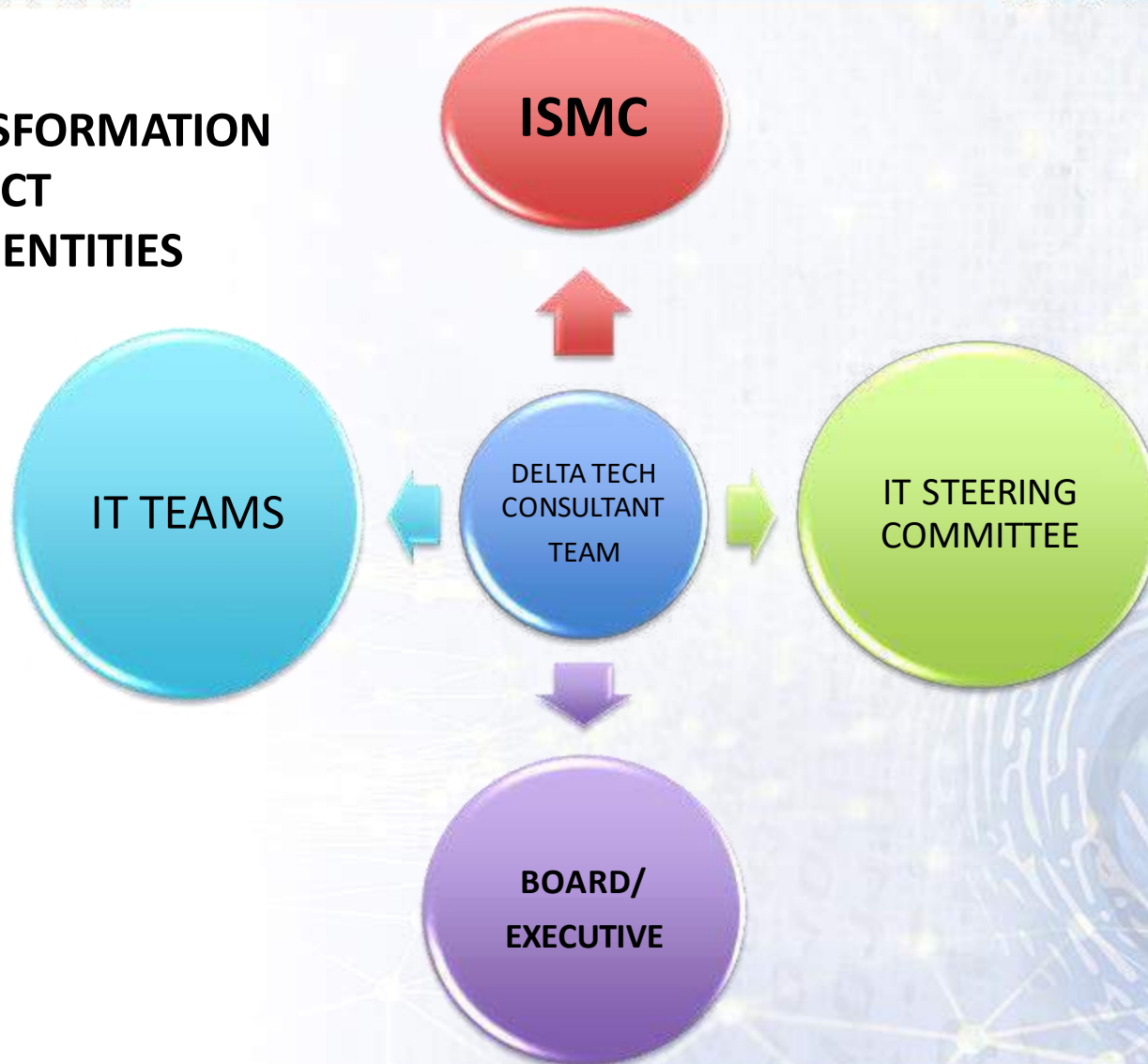
- **Reporting** is a critical component of effective project management and has the following objectives:

PROJECT MANAGEMENT FOR INFOSEC: PART 3

- **Reporting Objectives:**
 1. Creating visibility
 2. Keeping resources engaged for their inputs and involvement
 3. Keeping management informed of successes & challenges
 4. Creating credibility
 5. Ensuring team members are on their toes

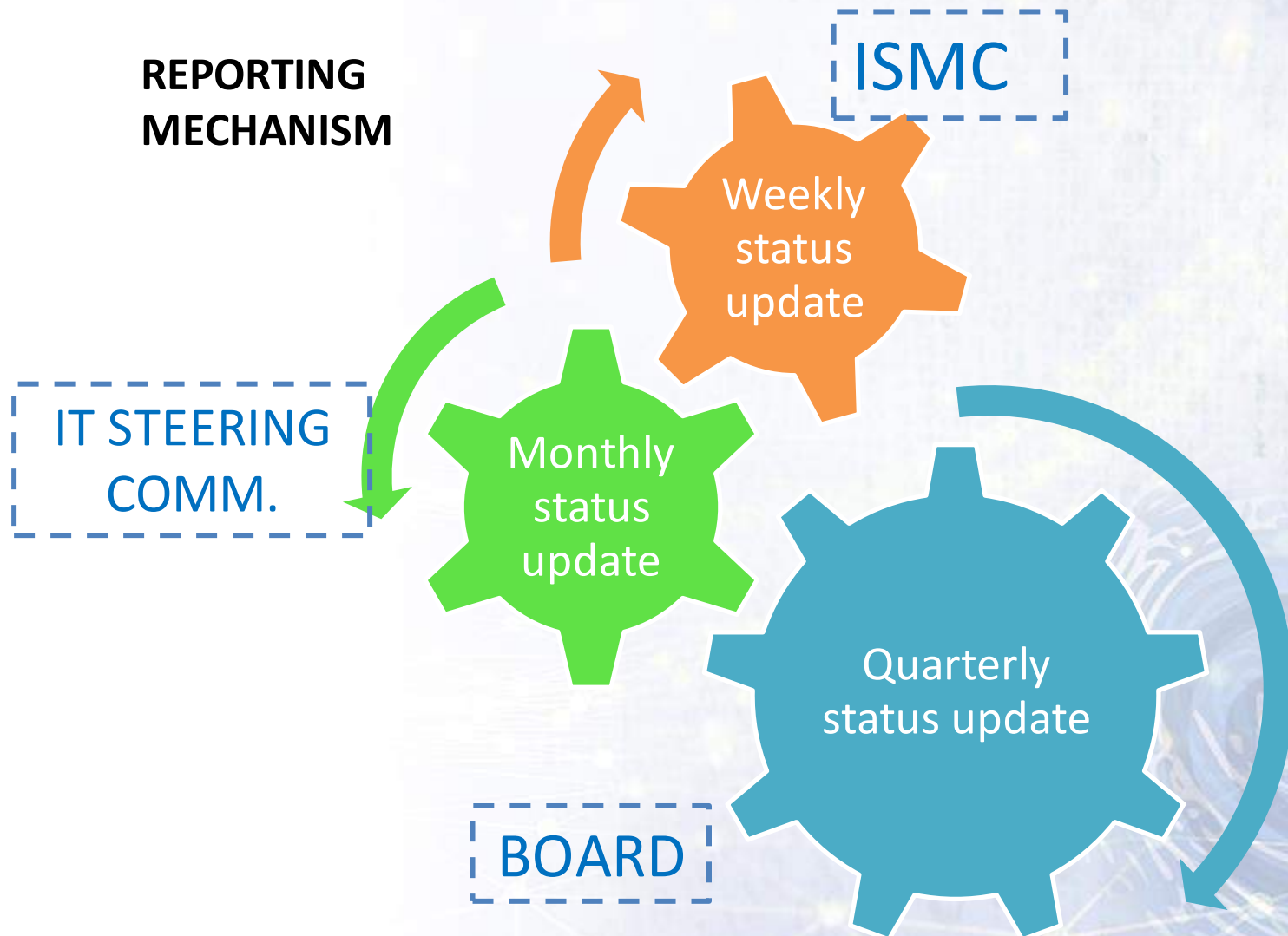
PROJECT MANAGEMENT FOR INFOSEC: PART 3

**TRANSFORMATION
PROJECT
MAIN ENTITIES**



PROJECT MANAGEMENT FOR INFOSEC: PART 3

REPORTING MECHANISM



PROJECT MANAGEMENT FOR INFOSEC: PART 3

PROJECT DASHBOARD			
Tracks		Status	Comments
Track 1 Infrastructure		 On Schedule	
Track 2 Documentation		 Requires Attention	
Track 3 Software Security			
Track 4 CORE APP Security		 In Progress	
Track 5 Desktop Security		 In Progress	
Track 6 Vulnerability Management		 In Progress	
Track 7 Awareness & Training		 Delayed	

PROJECT MANAGEMENT FOR INFOSEC: PART 3

- **Dashboard Objectives:**
 1. Provide simple & single view of all project tracks, and where the project stands
 2. Highlight problem areas for management intervention and support
 3. Monthly Steering Committee & Quarterly Board reports

PROJECT MANAGEMENT FOR INFOSEC: PART 3

Forum	Frequency	Report Format	Objectives
ISMC	WEEKLY	PDF MINS OF MEETING	IDENTIFY TASKS, RESPONSIBILITY, TIMELINE
STEERING COMMITTEE	MONTHLY	PPT PRESENTATION	INFORM RELEVANT HEADS OF PROGRESS, IDENTIFY CHALLENGES
BOARD MEETING	QUARTERLY	PPT PRESENTATION	CRITICAL LOOK AT PROGRESS ACHIEVED, IDENTIFY CHALLENGES & SOLUTIONS, SEEK ASSISTANCE

PROJECT MANAGEMENT FOR INFOSEC: PART 3

- By creating an accurate, honest, and disciplined reporting mechanism, the project manager ensures that all project stakeholders are informed, involved and helping where necessary for project success

END

PROJECT MANAGEMENT FOR INFOSEC: PART 4

- **PART 4:**
 - LEADERSHIP

PROJECT MANAGEMENT FOR INFOSEC: PART 4

- The Security Transformation requires **significant effort** over a one year period
- All resources have to be **tightly focused** on the successful outcome
- Without leadership, the transformation cannot take place

PROJECT MANAGEMENT FOR INFOSEC: PART 4

- **Leadership:**
 1. Authenticity
 2. Openness and transparency
 3. Respect for all individuals and teams
 4. Creating motivation
 5. Integrity
 6. Boldness to take a stand

PROJECT MANAGEMENT FOR INFOSEC: PART 4

- Technical resources will always respect a leader who has knowledge of his/her domain, and is able to provide a clear and effective strategy

PROJECT MANAGEMENT FOR INFOSEC: PART 4

- **Security Transformation Leadership** is about creating trust, and a team environment to facilitate efforts resulting in positive outcome
- Security Transformation Leadership is about working with people, at all levels to create a credible and successful project

END

Capacity Management – Part 1

- ISO27001:2013
 - 12.1.3: The use of resources should be **monitored, tuned and projections made of future capacity** requirements to ensure the **required system performance**

Capacity Management – Part 1

- What is capacity management?
 - Aims to ensure that the **capacity of IT services and the IT infrastructure is able to deliver the agreed service level targets** in a cost effective and timely manner.

https://wiki.en.it-processmaps.com/index.php/Capacity_Management

Capacity Management – Part 1

- What is capacity management?
 - The Capacity Management process **considers all resources required to deliver the IT service, and plans for short, medium and long term business requirements.**

https://wiki.en.it-processmaps.com/index.php/Capacity_Management

Capacity Management – Part 1

- ITIL suggests three sub-processes:
 - **Business** capacity management
 - **Service** capacity management
 - **Component** capacity management

<https://advisera.com/20000academy/knowledgebase/three-faces-capacity-management/>

Capacity Management – Part 1

- **Business** capacity management:
 - Translates business plans and needs into requirements for IT services and architecture

<https://advisera.com/20000academy/knowledgebase/three-faces-capacity-management/>

Capacity Management – Part 1

- **Business** capacity management:
 - As customers' business changes, so are service requirements changing. Change in service requirements usually has an impact on demand for capacity.

<https://advisera.com/20000academy/knowledgebase/three-faces-capacity-management/>

Capacity Management – Part 1

- **Service** capacity management:
 - Service capacity mngmt focuses on management, control and prediction of end-to-end performance of live IT services usage and workloads.

<https://advisera.com/20000academy/knowledgebase/three-faces-capacity-management/>

Capacity Management – Part 1

- **Service** capacity management:
 - It's about measuring performance and comparing it to reqmts that are set in Service Level Agreements (SLAs) or Service Level Requirements (SLRs).

<https://advisera.com/20000academy/knowledgebase/three-faces-capacity-management/>

Capacity Management – Part 1

- **Component** capacity management:
 - Focuses on mngmt, control, performance prediction, utilization & capacity of technology components (e.g. a hard disc, processor, etc.).

<https://advisera.com/20000academy/knowledgebase/three-faces-capacity-management/>

Capacity Management – Part 1

- In the next module lets look at ISO27002:2013 guidance for capacity management...

END

Capacity Management – Part 2

- In this module, let's look at capacity management guidance from **ISO27002:2013**

Capacity Management – Part 2

- ISO27002 guidance:
 - Capacity requirements should be identified, taking into account the **business criticality** of the concerned system

Capacity Management – Part 2

- ISO27002 guidance:
 - **System tuning and monitoring** should be applied to ensure and, where necessary, improve the **availability and efficiency of systems.**

Capacity Management – Part 2

- ISO27002 guidance:
 - **Detective controls** should be put in place to indicate problems in due time.

Capacity Management – Part 2

- ISO27002 guidance:
 - **Projections of future capacity reqmts** should take account of **new business** and system reqmts and **current & projected trends** in the organization's info processing capabilities

Capacity Management – Part 2

- ISO27002 guidance:
 - Particular attention needs to be paid to any resources with **long procurement lead times or high costs**; therefore managers should monitor the utilization of key system resources.

Capacity Management – Part 2

- ISO27002 guidance:
 - Providing sufficient capacity can be achieved by **increasing capacity or by reducing demand.**

Capacity Management – Part 2

- ISO27002 guidance:
 - Examples of managing capacity demand include:
 - a) **deletion of obsolete data** (disk space);
 - b) **decommissioning** of applications, systems, databases or environments;
 - c) **optimising** batch processes & schedules;

Capacity Management – Part 2

- ISO27002 guidance:
 - A documented capacity management plan should be considered for mission critical systems
 - Also consider human resources & offices/facilities

Capacity Management – Part 2

- **ITIL** looks at capacity management more in-depth under **service design phase**
- **ISO27002** provides some useful guidance
- In the industry we find that capacity management is not formalized as a process and lacks documentation

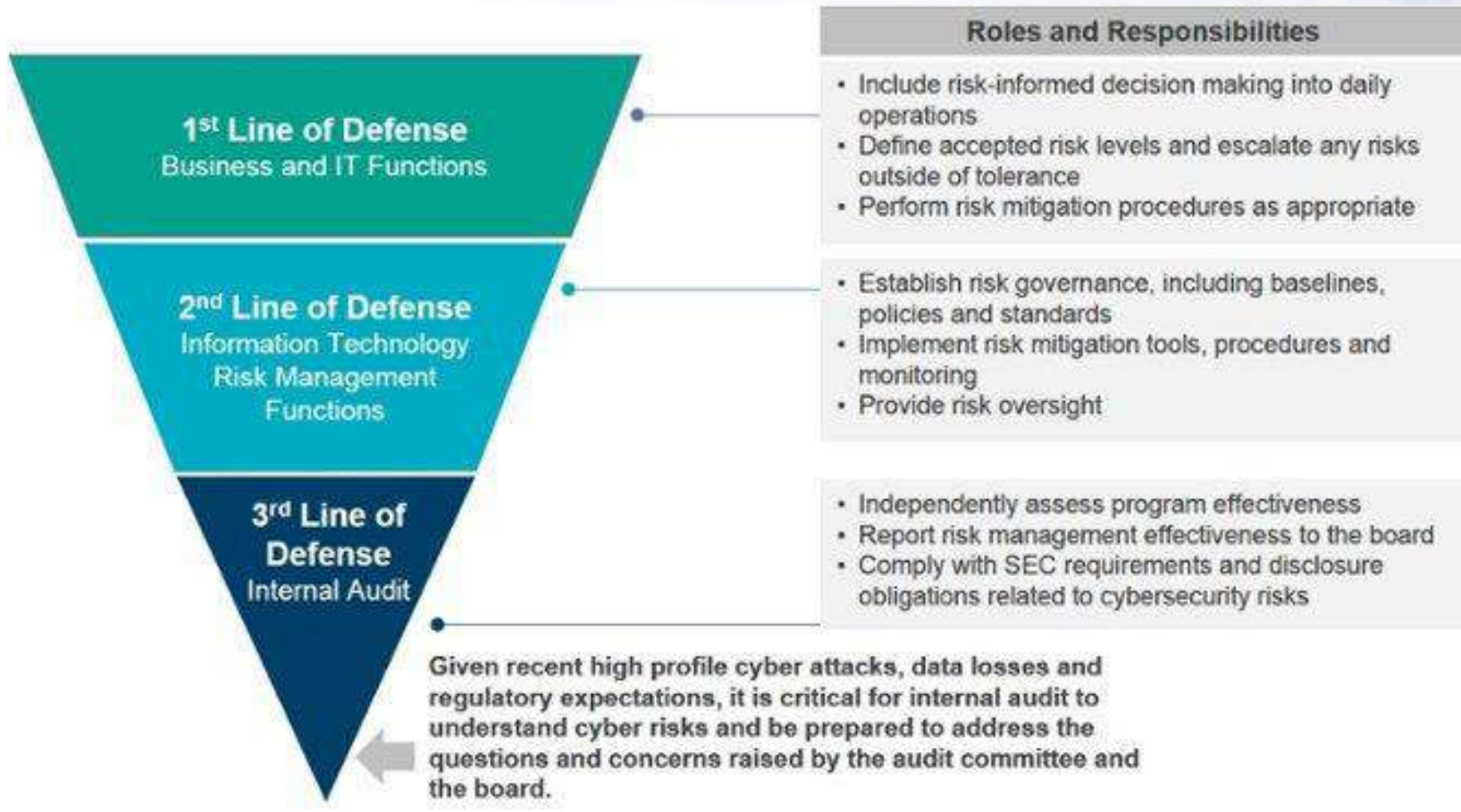
END

RISK MANAGEMENT & INTERNAL AUDIT-I

Three Lines of Cyber
Defense:

<https://securityintelligence.com/take-a-load-off-delegate-cyber-risk-management-using-the-three-lines-of-defense-model/>

RISK MANAGEMENT & INTERNAL AUDIT-I



<https://info.knowledgeleader.com/what-is-internal-audits-role-in-cyber-security>

RISK MANAGEMENT & INTERNAL AUDIT-I

1. Business & IT Functions (Management Control):

The first line encompasses the information security department as well as various business units that own their cyber risks. These entities need to understand how their assets are vulnerable and actively manage their cyber risks within...

RISK MANAGEMENT & INTERNAL AUDIT-I

1. Business & IT Functions (Management Control):

... organizationally acceptable tolerances. Sometimes called management control, this function is tasked with managing cyber risks by executing various controls. This means handling risk events, updating key risk indicators (KRIs), and...

RISK MANAGEMENT & INTERNAL AUDIT-I

1. Business & IT Functions (Management Control):

... deploying and managing controls that affect people, processes and technology.

2. Risk Management

- The second line of defense is composed of risk managers looking at aggregate risks at an enterprise level. It is often simply termed risk management but can also include compliance, legal, quality control and financial control.

RISK MANAGEMENT & INTERNAL AUDIT-I

2. Risk Management

- The second line looks at cybersecurity control frameworks, defines KRIs and metrics, creates [risk assessments](#), and tests and reviews conformance by tracking the actions of the first line of defense and analyzing the...

2. Risk Management

- ...impact of those actions to determine their effectiveness in mitigating cyber risks. In other words, this function monitors how management is doing in its handling of cyber risks by determining the extent that risks are actively monitored and appropriately managed.

2. Risk Management

- It is often performed under an umbrella of senior management and some board directors or a board-level committee, such as the audit committee or a risk committee. And, importantly, this second line can challenge the first line.

ISSUES WITH RISK MANAGEMENT IN PAKISTAN

1. Risk Management hierarchy not trained in IT
2. Separate Dept – not suitable given security maturity level
3. Seen as outsider
4. Low cooperation levels with IT

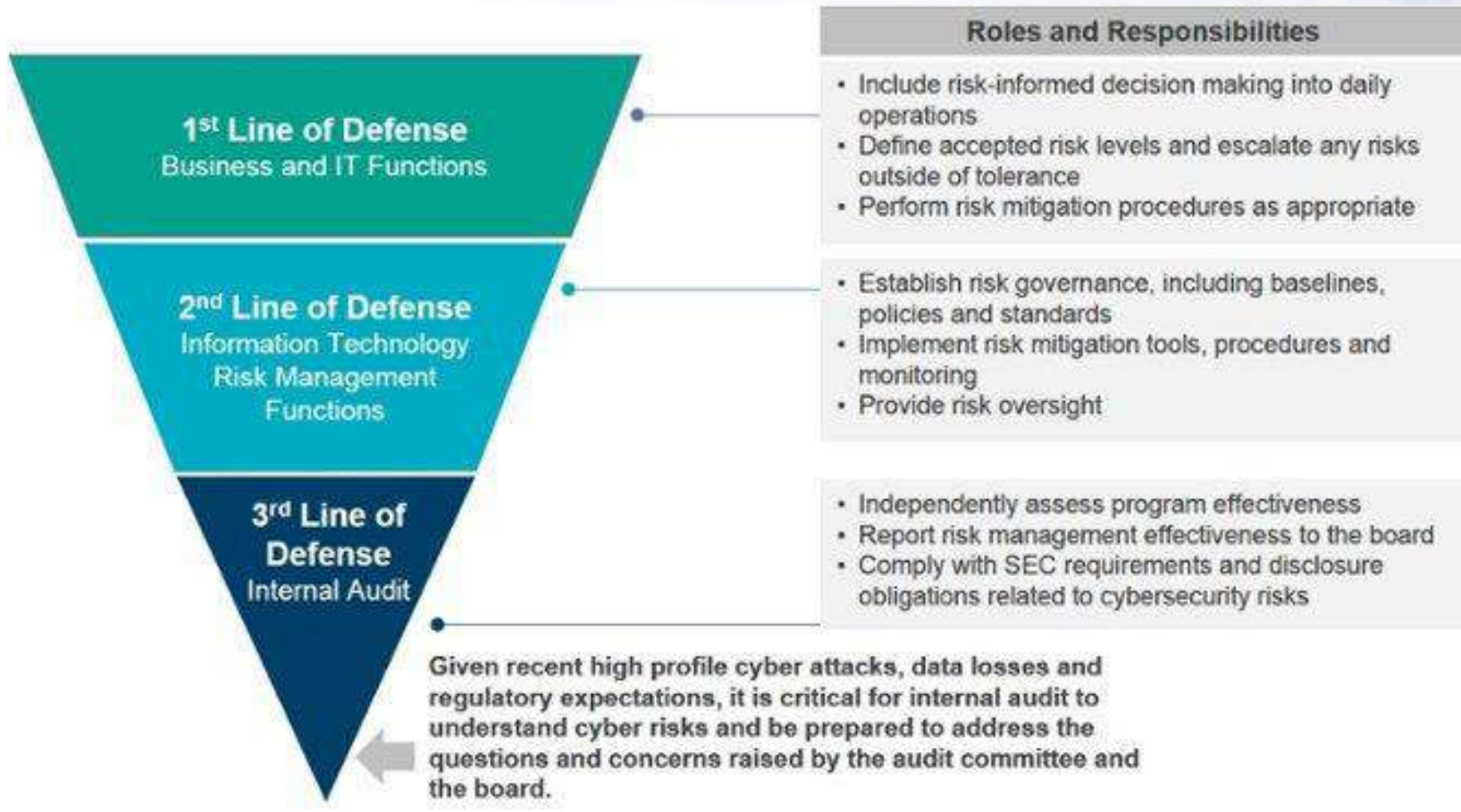
END

RISK MANAGEMENT & INTERNAL AUDIT-II

Three Lines of Cyber
Defense:

<https://securityintelligence.com/take-a-load-off-delegate-cyber-risk-management-using-the-three-lines-of-defense-model/>

RISK MANAGEMENT & INTERNAL AUDIT-II



<https://info.knowledgeleader.com/what-is-internal-audits-role-in-cyber-security>

INTERNAL AUDIT

3. Internal Audit

- The third line of defense is internal audit. It may also include input from external auditors and/or regulators. This function, sometimes termed independent assurance, evaluates the overall process of cyber risk governance for the entire organization.

INTERNAL AUDIT

3. Internal Audit

- It ensures that the organization's internal control framework is adequate for dealing with the risks the organization faces.

INTERNAL AUDIT

3. Internal Audit

- As with the second line of defense, the third line can push back on the assertions of the previous lines regarding the adequacy of the controls in place. This function usually reports directly to the board or the audit committee.

INTERNAL AUDIT

Issues With Internal Audit In Pakistan

- a. Not on the same page with other Depts
- b. KPI seems to be highest number of observations – not organizational benefit
- c. No common security vision in the organization

INTERNAL AUDIT

Issues With Internal Audit In Pakistan

d. Large number of point observations do not help to improve the security posture

e. Internal audit not aware of IT team or security team framework being adopted

END

MANAGEMENT REVIEW

How To Conduct ISO27001
Management Review

<https://www.isms.online/iso-27001/how-to-conduct-your-iso-27001-management-review/>

MANAGEMENT REVIEW

Purpose

- The purpose of the Management Review is to ensure the ISMS and its objectives continue to remain suitable, adequate and effective given the organisation's purpose, issues and risks.

MANAGEMENT REVIEW

Results

- The results of the management review will enable senior management to make well informed, strategic decisions that will have a material effect on information security and the way the organisation manages it.

MANAGEMENT REVIEW

What should be covered ?

- a) the status of actions from previous management reviews;
- b) changes in external and internal issues that are relevant to the information security management system;

MANAGEMENT REVIEW

What should be covered ?

c) feedback on the information security performance, including trends in:

- nonconformities and corrective actions;
- monitoring and measurement results;
- audit results; and
- fulfilment of information security objectives.

MANAGEMENT REVIEW

What should be covered ?

- d) feedback from interested parties;
- e) results of [risk assessment](#) and status of risk treatment plan; and
- f) opportunities for continual improvement.

MANAGEMENT REVIEW

Who Should Attend ?

- For the ISMS to be effective in an organisation, it needs senior management commitment and, as such, it makes sense for the members of an ISMS “Board” to have authority in matters pertaining to information security.

MANAGEMENT REVIEW

Who Should Attend ?

- Typically an ISMS Board might include the Chief Information Security Officer (CISO), Senior Information Risk Owner (SIRO), Chief Technical Officer and maybe even the CEO.

MANAGEMENT REVIEW

Who Should Attend ?

- The outputs of the management review will include decisions related to continual improvement opportunities and any needs for changes to the information security management system.

END

Human Resource Security

- In this module, let's look at human resource security...

Human Resource Security

- **Prior to employment (ISO27001):**
 - Screening
 - Terms & conditions of employment

Human Resource Security

- **ISO27002 guidance (Screening):**
 - availability of satisfactory **character references**, e.g. one **business** and one **personal**;
 - **a verification** (for completeness and accuracy) **of the applicant's CV**;

Human Resource Security

- **ISO27002 guidance (Screening):**
 - **confirmation of claimed academic and professional qualifications;**
 - **independent identity verification (passport or similar document);**

Human Resource Security

- **ISO27002 guidance (Screening):**
 - more detailed verification, such as **credit review or review of criminal records**

Human Resource Security

- **During employment (ISO27001):**
 - Management responsibilities
 - Awareness, education, and training
 - Disciplinary process

Human Resource Security

- **ISO27002 guidance**
(Disciplinary Process):
 - The disciplinary process **should not be commenced without prior verification** that an infosec breach has occurred

Human Resource Security

- **ISO27002 guidance**
(Disciplinary Process):
 - The formal disciplinary process should ensure **correct and fair treatment for employees** who are suspected of committing breaches of info security

Human Resource Security

- **ISO27002 guidance**
(Disciplinary Process):
 - The formal disciplinary process should provide for a **graduated response that takes into consideration factors such as the nature and gravity of the breach** and its impact on business;

Human Resource Security

- Termination or change of employment (ISO27001):

- Infosec responsibilities & duties are defined, communicated to employee or contractor & enforced

Human Resource Security

- **ISO27002 guidance (termination/change):**
 - The communication of termination responsibilities should include **on-going infosec reqmts & legal responsibilities** &, where appropriate, responsibilities...

Human Resource Security

- **ISO27002 guidance (termination/change):**
 - ... contained within any **confidentiality agreement & the terms & conditions of employment** continuing for a defined period after the end of the employee's or contractor's employment

Human Resource Security

- As you can see, human resource security has quite a bit of detail
- **ISO27002 provides very useful guidance and elaborates the ISO27001 controls**

END

SBP CIRC. # 5, TECHNOLOGY GOVERNANCE FRAMEWORK

SBP TECHNOLOGY GOVERNANCE AND RISK MANAGEMENT FRAMEWORK

SBP CIRC. # 5, TECHNOLOGY GOVERNANCE FRAMEWORK

1. IT GOVERNANCE IN FIs

- 1.1 Tech. Gov, Framework
- 1.2 IT Strategy
- 1.3 Digital Strategy
- 1.4 Roles & Responsibilities
- 1.5 Org Structure
- 1.6 Policies, Standards, Procedures
- 1.7 Management Information Systems (MIS)
- 1.8 Capacity Building/ Training

2. INFORMATION SECURITY

- 2.1 Info/Cyber Security Management Framework
- 2.2 Identification & Prioritization Of IT Assets
- 2.3 InfoSec Risk Management
- 2.4 Security Controls Implementation
- 2.5 Cyber Security Action Plan
- 2.6 Incident Reporting
- 2.7 Security Requirements & Testing
- 2.8 Risk Monitoring & Reporting
- 2.9 Threat Intelligence & Industry Collaboration

3. IT SERVICE DELIVERY & OPERATIONS MANAGEMENT

- 3.1 IT Service Mngmt Frame.
- 3.2 Preventive Maint. Plan
- 3.3 Event & Problem Mngmt
- 3.4 Patch Management
- 3.5 Capacity Planning
- 3.6 Data Center
- 3.7 User Support / Helpdesk

6. IT AUDIT PROGRAM

- 6.1 IT Audit Program
- 6.2 Scope Of IT Audit
- 6.3 Reporting Methodology
- 6.4 Post-Closing/Monit. Activ.

4. ACQUISITION & IMPLEMENTATION OF IT SYSTEMS

- 4.1 Tech Project Management Framework
- 4.2 System Dev. & Acquisition Framework
- 4.3 Outsourcing Of IT Services

5. DISASTER RECOVERY & BUSINESS CONTINUITY

- 5.1 BC & DR Framework
- 5.2 BC Planning Process
- 5.3 Disaster Recovery

SBP CIRC. # 5, TECHNOLOGY GOVERNANCE FRAMEWORK

OBJECTIVES

- The framework aims to provide enabling regulatory environment for managing risks associated with the acquisition, development, deployment and use of technology and shall serve as **SBP's baseline requirements for all FI(s).**

SBP CIRC. # 5, TECHNOLOGY GOVERNANCE FRAMEWORK

OBJECTIVES

- The FI(s) shall **upgrade their systems, controls and procedures to ensure compliance** with this framework latest by **June 30, 2018.**

SBP CIRC. # 5, TECHNOLOGY GOVERNANCE FRAMEWORK

OBJECTIVES

- The FI(s) shall assess and conduct a **gap analysis** between their current status & this framework and draw a **time-bound action plan to address the gaps and comply** with the guidelines in this framework

SBP CIRC. # 5, TECHNOLOGY GOVERNANCE FRAMEWORK

OVERVIEW

- The instructions are focused on **enhancing the proactive and reactive environments** in FI(s) to various facets and dimensions of technology including information security, technology operations, audit, business continuity, ...

SBP CIRC. # 5, TECHNOLOGY GOVERNANCE FRAMEWORK

OVERVIEW

- ... project/performance management and related domains (pg 5)
- FI(s) shall adopt an **integrated risk management approach to identify, measure, monitor and control technology risks** (page 5)

SBP CIRC. # 5, TECHNOLOGY GOVERNANCE FRAMEWORK

OVERVIEW

- The Framework consists of **6 domains and 35 sub-domains**
- Overall the **Framework is a combination of COBIT, ITIL, and ISO27001:2013 (ISMS)**

SBP CIRC. # 5, TECHNOLOGY GOVERNANCE FRAMEWORK

Implementation Mechanism

- a. Gap analysis
- b. Documentation
- c. Implementation

END

CYBER SECURITY MATURITY MATRIX - OVERVIEW

- In this module we will introduce the Cyber Security Maturity Matrix (CSMM)

CYBER SECURITY MATURITY MATRIX - OVERVIEW

SECURITY MATURITY LEVEL
VI. SECURED
V. MONITORED
IV. PROTECTED
III. HARDENED
II. FUNDAMENTALS
I. FOUNDATION

VI. SECURED

V. MONITORED

IV. PROTECTED

III. HARDENED

II. FUNDAMENTALS

I. FOUNDATION

CYBER SECURITY MATURITY MATRIX - OVERVIEW

Industry Security Challenges:

- Grass-roots security controls have not been implemented
- Haphazard, reactive security approach
- Not following any structured security architecture or framework

CYBER SECURITY MATURITY MATRIX - OVERVIEW

What challenges does CSMM address ?

- 5 characteristics of Information Security in Pakistan:
 - Reactive
 - Superficial
 - Box approach
 - Contention
 - Governance overkill

CYBER SECURITY MATURITY MATRIX - OVERVIEW

How is the local industry coping with security implementation?

- a. Large organizations
- b. Medium sized organizations
- c. Small organizations

CYBER SECURITY MATURITY MATRIX - OVERVIEW

Issues with large organizations:

1. Missed out on security hardening
2. Vulnerability management effectively not being done as per Int'l best-practice
3. Attempting automation or box approach

CYBER SECURITY MATURITY MATRIX - OVERVIEW

Issues with medium sized organizations:

1. Don't have sufficient security expertise and knowledge
2. Security was never a focus
3. Have built insecure IT networks just like the large organizations
4. VM and hardening missing here too

CYBER SECURITY MATURITY MATRIX - OVERVIEW

Issues with smaller organizations:

1. Mostly have pirated software
2. Enterprise antivirus and Microsoft Active Directory (AD) mostly missing
3. Not enough budget for security
4. No personnel allocated for security

CYBER SECURITY MATURITY MATRIX - OVERVIEW

The industry status:

1. Industry lacks a standard & authentic roadmap of how to achieve security
2. No mechanism to measure or certify security
3. Divergent understanding of how security will be achieved

CYBER SECURITY MATURITY MATRIX - OVERVIEW

SECURITY MATURITY LEVEL	MINIMUM CHARACTERISTICS
VI. SECURED	Red Team Penetration Testing
	Security Orchestration, Automation, & Incident Response
	Threat Protection
	Threat Simulation
V. MONITORED	Security Operations Center (SOC) Implementation
	Critical Data Encryption
	Data Loss Prevention (DLP) Solution
	SIEM Solution For Security Events Detection
IV. PROTECTED	ISO27001:2013 (ISMS) Certification
	External/Internal Penetration Test (Critical Assets)
	Software Source Code Review For Critical Applications
	CIS 20 Critical Security Controls
III. HARDENED	Software Security Hardening Program
	NGN FW At Data Center Entry Point With Filtering
	CIS Security Benchmarks Hardening Of All IT Assets
	Min Monthly Credential Based VM Cycle
II. FUNDAMENTALS	Network Segmentation With VLANs By Dept/Service, & DMZ
	Edge NGN FW With Web, Email, Anti-malware Filtering
	Min Quarterly Credential Based VM Cycle
	Licensed Or Open Source VM Tool
I. FOUNDATION	Edge FW With Filtering
	Active Directory (WS/S)
	Licensed Enterprise AV (WS/S)
	Licensed Windows OS (WS/S) Or Open Source

CYBER SECURITY MATURITY MATRIX - OVERVIEW

How does CSMM help ?

- Offers a proactive, structured, sequential model to implement security
- Model is certifiable
- Cyber Security Certification Board (CSCB) will certify security status of organizations

END

CSMM - LAYER 1 - FOUNDATION

- In this module we will introduce the Cyber Security Maturity Matrix (CSMM): layer 1

CSMM - LAYER 1 - FOUNDATION

SECURITY MATURITY LEVEL	MINIMUM CHARACTERISTICS
VI. SECURED	Red Team Penetration Testing
	Security Orchestration, Automation, & Incident Response
	Threat Protection
	Threat Simulation
V. MONITORED	Security Operations Center (SOC) Implementation
	Critical Data Encryption
	Data Loss Prevention (DLP) Solution
	SIEM Solution For Security Events Detection
IV. PROTECTED	ISO27001:2013 (ISMS) Certification
	External/Internal Penetration Test (Critical Assets)
	Software Source Code Review For Critical Applications
	CIS 20 Critical Security Controls
III. HARDENED	Software Security Hardening Program
	NGN FW At Data Center Entry Point With Filtering
	CIS Security Benchmarks Hardening Of All IT Assets
	Min Monthly Credential Based VM Cycle
II. FUNDAMENTALS	Network Segmentation With VLANs By Dept/Service, & DMZ
	Edge NGN FW With Web, Email, Anti-malware Filtering
	Min Quarterly Credential Based VM Cycle
	Licensed Or Open Source VM Tool
I. FOUNDATION	Edge FW With Filtering
	Active Directory (WS/S)
	Licensed Enterprise AV (WS/S)
	Licensed Windows OS (WS/S) Or Open Source

VI. SECURED

V. MONITORED

IV. PROTECTED

III. HARDENED

II. FUNDAMENTALS

I. FOUNDATION

CSMM - LAYER 1 - FOUNDATION

CSMM LAYER 1: FOUNDATION

I. FOUNDATION	Edge FW With Filtering
	Active Directory (WS/S)
	Licensed Enterprise AV (WS/S)
	Licensed Windows OS (WS/S) Or Open Source

CSMM - LAYER 1 - FOUNDATION

1.1: LICENSED WINDOWS OR OPEN SOURCE

- Licensed windows (MS)
- Ubuntu open source
- Other numerous open source alternatives
- Basic requirement for a secure IT setup
- Pirated software infested with malware

CSMM - LAYER 1 - FOUNDATION

1.2: LICENSED ENTERPRISE ANTI-VIRUS

- Users usually do not update their AV
- Visibility dashboard, & central mngmt reqd
- Consistent mngmt of hundreds or thousands of anti-virus agents
- Many anti-virus agents are out-of-synch with the update-server

CSMM - LAYER 1 - FOUNDATION

1.3: ACTIVE DIRECTORY (AD)

- Active Directory (AD) is essential not only to regulate account management (authentication and authorization) but also to enforce and manage security controls

CSMM - LAYER 1 - FOUNDATION

1.4: Edge FW With Filtering

- Forms first line of perimeter defense
- Filtering of incoming and outgoing traffic
- DMZ for hosted services
- Policy enforcement for security

END

CSMM - Layer 2 - Fundamentals

- In this module we will introduce the Cyber Security Maturity Matrix (CSMM), layer 2

CSMM - Layer 2 - Fundamentals

SECURITY MATURITY LEVEL	MINIMUM CHARACTERISTICS
VI. SECURED	Red Team Penetration Testing
	Security Orchestration, Automation, & Incident Response
	Threat Protection
	Threat Simulation
V. MONITORED	Security Operations Center (SOC) Implementation
	Critical Data Encryption
	Data Loss Prevention (DLP) Solution
	SIEM Solution For Security Events Detection
IV. PROTECTED	ISO27001:2013 (ISMS) Certification
	External/Internal Penetration Test (Critical Assets)
	Software Source Code Review For Critical Applications
	CIS 20 Critical Security Controls
III. HARDENED	Software Security Hardening Program
	NGN FW At Data Center Entry Point With Filtering
	CIS Security Benchmarks Hardening Of All IT Assets
	Min Monthly Credential Based VM Cycle
II. FUNDAMENTALS	Network Segmentation With VLANs By Dept/Service, & DMZ
	Edge NGN FW With Web, Email, Anti-malware Filtering
	Min Quarterly Credential Based VM Cycle
	Licensed Or Open Source VM Tool
I. FOUNDATION	Edge FW With Filtering
	Active Directory (WS/S)
	Licensed Enterprise AV (WS/S)
	Licensed Windows OS (WS/S) Or Open Source

VI. SECURED

V. MONITORED

IV. PROTECTED

III. HARDENED

II. FUNDAMENTALS

I. FOUNDATION

CSMM - LAYER 2 - FUNDAMENTALS

CSMM LAYER 2: FUNDAMENTALS

II. FUNDAMENTALS	Network Segmentation With VLANs By Dept/Service, & DMZ
	Edge NGN FW With Web, Email, Anti-malware Filtering
	Min Quarterly Credential Based VM Cycle
	Licensed Or Open Source VM Tool

CSMM - LAYER 2 - FUNDAMENTALS

2.1: LICENSED OR OPEN SOURCE VM TOOL

- Vulnerability management or patch management is a foundational layer of security practice
- Open source: OpenVAS
- Licensed: **Qualys**, Nessus, Rapid7

CSMM - LAYER 2 - FUNDAMENTALS

2.2: MIN QUARTERLY CREDENTIAL BASED VM CYCLE

- For those organizations that have not conducted VM practice before
- International best-practice is weekly VM cycle

CSMM - LAYER 2 - FUNDAMENTALS

2.3: Edge NGN FW With Web, Email, Anti-malware Filtering

- Typical NGN FW: Fortinet
- Features: VPNs, web filtering, email anti-spam filtering, Antivirus, anti-malware, application visibility & control, access-lists

CSMM - LAYER 2 - FUNDAMENTALS

2.4. Network Segmentation With VLANs by Dept./Service & DMZ

- Network segmentation helps create separate broadcast domains
- Separate policies and filtering possible for each separate VLAN
- Helps manage traffic
- Segregates traffic into traffic-types

END

CSMM - LAYER 3: HARDENED

- In this module we will introduce the Cyber Security Maturity Matrix (CSMM), layer 3

CSMM - LAYER 3: HARDENED

SECURITY MATURITY LEVEL	MINIMUM CHARACTERISTICS
VI. SECURED	Red Team Penetration Testing
	Security Orchestration, Automation, & Incident Response
	Threat Protection
	Threat Simulation
V. MONITORED	Security Operations Center (SOC) Implementation
	Critical Data Encryption
	Data Loss Prevention (DLP) Solution
	SIEM Solution For Security Events Detection
IV. PROTECTED	ISO27001:2013 (ISMS) Certification
	External/Internal Penetration Test (Critical Assets)
	Software Source Code Review For Critical Applications
	CIS 20 Critical Security Controls
III. HARDENED	Software Security Hardening Program
	NGN FW At Data Center Entry Point With Filtering
	CIS Security Benchmarks Hardening Of All IT Assets
	Min Monthly Credential Based VM Cycle
II. FUNDAMENTALS	Network Segmentation With VLANs By Dept/Service, & DMZ
	Edge NGN FW With Web, Email, Anti-malware Filtering
	Min Quarterly Credential Based VM Cycle
	Licensed Or Open Source VM Tool
I. FOUNDATION	Edge FW With Filtering
	Active Directory (WS/S)
	Licensed Enterprise AV (WS/S)
	Licensed Windows OS (WS/S) Or Open Source

VI. SECURED

V. MONITORED

IV. PROTECTED

III. HARDENED

II. FUNDAMENTALS

I. FOUNDATION

CSMM - LAYER 3: HARDENED

CSMM LAYER 3: HARDENED

III. HARDENED	Software Security Hardening Program
	NGN FW At Data Center Entry Point With Filtering
	CIS Security Benchmarks Hardening Of All IT Assets
	Min Monthly Credential Based VM Cycle

CSMM - LAYER 3: HARDENED

3.1: Minimum Monthly Credential Based VM Scan

- Now moved to monthly scan from quarterly scan
- Credential based scan from non-credential scan

CSMM - LAYER 3: HARDENED

3.2: CIS BENCHMARKS HARDENING OF ALL IT ASSETS

- Hardening covered in detail in this course
- Planning, pilot, production implementation
- Usually takes 6-8 months depending upon size of organization

CSMM - LAYER 3: HARDENED

3.3: NGN FW At Datacenter Entry Point With Filtering

- Filtering and malware protection at datacenter entry point often ignored
- All traffic including internal user traffic entering or exiting data center needs to be filtered

CSMM - LAYER 3: HARDENED

3.4: Software Security Hardening Program

- Software security program needs to be developed
- Software security hardening: controls identification, pilot controls implementation, validation, testing, change mngmt, PROD

END

CSMM - LAYER 4: PROTECTED

- In this module we will introduce the Cyber Security Maturity Matrix (CSMM), layer 4

CSMM - LAYER 4: PROTECTED

SECURITY MATURITY LEVEL	MINIMUM CHARACTERISTICS
VI. SECURED	Red Team Penetration Testing
	Security Orchestration, Automation, & Incident Response
	Threat Protection
	Threat Simulation
V. MONITORED	Security Operations Center (SOC) Implementation
	Critical Data Encryption
	Data Loss Prevention (DLP) Solution
	SIEM Solution For Security Events Detection
IV. PROTECTED	ISO27001:2013 (ISMS) Certification
	External/Internal Penetration Test (Critical Assets)
	Software Source Code Review For Critical Applications
	CIS 20 Critical Security Controls
III. HARDENED	Software Security Hardening Program
	NGN FW At Data Center Entry Point With Filtering
	CIS Security Benchmarks Hardening Of All IT Assets
	Min Monthly Credential Based VM Cycle
II. FUNDAMENTALS	Network Segmentation With VLANs By Dept/Service, & DMZ
	Edge NGN FW With Web, Email, Anti-malware Filtering
	Min Quarterly Credential Based VM Cycle
	Licensed Or Open Source VM Tool
I. FOUNDATION	Edge FW With Filtering
	Active Directory (WS/S)
	Licensed Enterprise AV (WS/S)
	Licensed Windows OS (WS/S) Or Open Source

VI. SECURED

V. MONITORED

IV. PROTECTED

III. HARDENED

II. FUNDAMENTALS

I. FOUNDATION

CSMM - LAYER 4: PROTECTED

CSMM LAYER 4: PROTECTED

IV. PROTECTED	ISO27001:2013 (ISMS) Certification
	External/Internal Penetration Test (Critical Assets)
	Software Source Code Review For Critical Applications
	CIS 20 Critical Security Controls

CSMM - LAYER 4: PROTECTED

4.1: CIS 20 CRITICAL SECURITY CONTROLS

- Aggregate control set covering all aspects of IT
- CIS benchmarks covered individual asset hardening
- Excellent set of security controls
- Sets out International best-practices

CSMM - LAYER 4: PROTECTED

4.2: Software Source Code Review For Critical Applications

- Source code review is a specialized activity which may be conducted in a manual or automated manner
- Specific to the software technology platform
- Peer or third-party

CSMM - LAYER 4: PROTECTED

4.3: External/Internal Penetration Test (Critical Assets):

- Penetration test most beneficial after the internal VM program is functional, and security hardening has been performed
- Third-party review of vulnerabilities and hacker-view of assets

CSMM - LAYER 4: PROTECTED

4.4: ISO27001:2013 (ISMS) Certification

- Global gold standard for Information Security governance
- Needs to be wisely used as it is both deep and broad
- Utilize as security governance framework leveraging VM and security hardening

END

CSMM - LAYER 5: MONITORED

- In this module we will introduce the Cyber Security Maturity Matrix (CSMM), layer 5

CSMM - LAYER 5: MONITORED

SECURITY MATURITY LEVEL	MINIMUM CHARACTERISTICS
VI. SECURED	Red Team Penetration Testing
	Security Orchestration, Automation, & Incident Response
	Threat Protection
	Threat Simulation
V. MONITORED	Security Operations Center (SOC) Implementation
	Critical Data Encryption
	Data Loss Prevention (DLP) Solution
	SIEM Solution For Security Events Detection
IV. PROTECTED	ISO27001:2013 (ISMS) Certification
	External/Internal Penetration Test (Critical Assets)
	Software Source Code Review For Critical Applications
	CIS 20 Critical Security Controls
III. HARDENED	Software Security Hardening Program
	NGN FW At Data Center Entry Point With Filtering
	CIS Security Benchmarks Hardening Of All IT Assets
	Min Monthly Credential Based VM Cycle
II. FUNDAMENTALS	Network Segmentation With VLANs By Dept/Service, & DMZ
	Edge NGN FW With Web, Email, Anti-malware Filtering
	Min Quarterly Credential Based VM Cycle
	Licensed Or Open Source VM Tool
I. FOUNDATION	Edge FW With Filtering
	Active Directory (WS/S)
	Licensed Enterprise AV (WS/S)
	Licensed Windows OS (WS/S) Or Open Source

VI. SECURED

V. MONITORED

IV. PROTECTED

III. HARDENED

II. FUNDAMENTALS

I. FOUNDATION

CSMM - LAYER 5: MONITORED

CSMM LAYER 5: MONITORED

V. MONITORED	Security Operations Center (SOC) Implementation
	Critical Data Encryption
	Data Loss Prevention (DLP) Solution
	SIEM Solution For Security Events Detection

CSMM - LAYER 5: MONITORED

5.1: SIEM SOLUTION FOR SECURITY EVENTS DETECTION

- SIEM solutions provide security log collection, dashboard reporting, root-cause analysis, and correlation
- Leading SIEM solutions: LogRhythm, IBM Q-Radar, Splunk, Elastic Search

CSMM - LAYER 5: MONITORED

5.2: DATA LOSS PREVENTION (DLP) SOLUTION

- Classification, visibility, and control of data
- Monitoring and blocking of data leakage and data exfiltration
- Network DLP and system DLP (agent)

CSMM - LAYER 5: MONITORED

5.3: CRITICAL DATA ENCRYPTION

- Protect intellectual property and confidential information
- Confidentiality and integrity of data
- Encrypt data at rest, in transit, and in use
- Laptop HDD and removable media

CSMM - LAYER 5: MONITORED

5.4: SECURITY OPERATIONS CENTER (SOC) IMPLEMENTATION

- After implementation of the first four layers, its time to consolidate security operations
- People, process, and technology/tools
- Similar to a NOC but for security purposes
- SIEM is starting point

END

CSMM - LAYER 6: SECURED

- In this module we will introduce the Cyber Security Maturity Matrix (CSMM), layer 6

CSMM - LAYER 6: SECURED

SECURITY MATURITY LEVEL	MINIMUM CHARACTERISTICS
VI. SECURED	Red Team Penetration Testing
	Security Orchestration, Automation, & Incident Response
	Threat Protection
	Threat Simulation
V. MONITORED	Security Operations Center (SOC) Implementation
	Critical Data Encryption
	Data Loss Prevention (DLP) Solution
	SIEM Solution For Security Events Detection
IV. PROTECTED	ISO27001:2013 (ISMS) Certification
	External/Internal Penetration Test (Critical Assets)
	Software Source Code Review For Critical Applications
	CIS 20 Critical Security Controls
III. HARDENED	Software Security Hardening Program
	NGN FW At Data Center Entry Point With Filtering
	CIS Security Benchmarks Hardening Of All IT Assets
	Min Monthly Credential Based VM Cycle
II. FUNDAMENTALS	Network Segmentation With VLANs By Dept/Service, & DMZ
	Edge NGN FW With Web, Email, Anti-malware Filtering
	Min Quarterly Credential Based VM Cycle
	Licensed Or Open Source VM Tool
I. FOUNDATION	Edge FW With Filtering
	Active Directory (WS/S)
	Licensed Enterprise AV (WS/S)
	Licensed Windows OS (WS/S) Or Open Source

VI. SECURED

V. MONITORED

IV. PROTECTED

III. HARDENED

II. FUNDAMENTALS

I. FOUNDATION

CSMM - LAYER 6: SECURED

CSMM LAYER 6: SECURED

VI. SECURED	Red Team Penetration Testing
	Security Orchestration, Automation, & Incident Response
	Threat Protection
	Threat Simulation

CSMM - LAYER 6: SECURED

6.1: THREAT SIMULATION

- Platform such as Redwolf Security (www.redwolfsecurity.com)
- Security testing, load testing, and DDOS testing
- Misconfigured security devices and incident response

CSMM - LAYER 6: SECURED

6.2: THREAT PROTECTION

- Various threat protection solutions
- Best solutions will map to the vulnerability condition of your IT assets e.g. Qualys Threat Protect
- Helps to pinpoint most critical assets and prioritize patching

CSMM - LAYER 6: SECURED

6.2: THREAT PROTECTION

- Qualys Threat Protection Live Threat Intelligence Feed displays the latest vulnerability disclosures and maps them to your impacted IT assets. You can see the number of assets affected by each threat, and drill down into asset details.

CSMM - LAYER 6: SECURED

6.3: SECURITY ORCHESTRATION, AUTOMATION, AND INCIDENT RESPONSE

- Solution such as Cybersponse (www.cybersponse.com)

CSMM - LAYER 6: SECURED

6.3: SECURITY ORCHESTRATION, AUTOMATION, AND INCIDENT RESPONSE

- From triaging and investigating alerts to collaboration and remediation between team members, CyberSponse takes your security operation team to the next level.

CSMM - LAYER 6: SECURED

6.4: RED TEAM PENETRATION TESTING

- Red team and blue team
- Attack & defense simulation
- Continuously find holes in security defenses
- Uncover security vulnerabilities before hackers exploit them

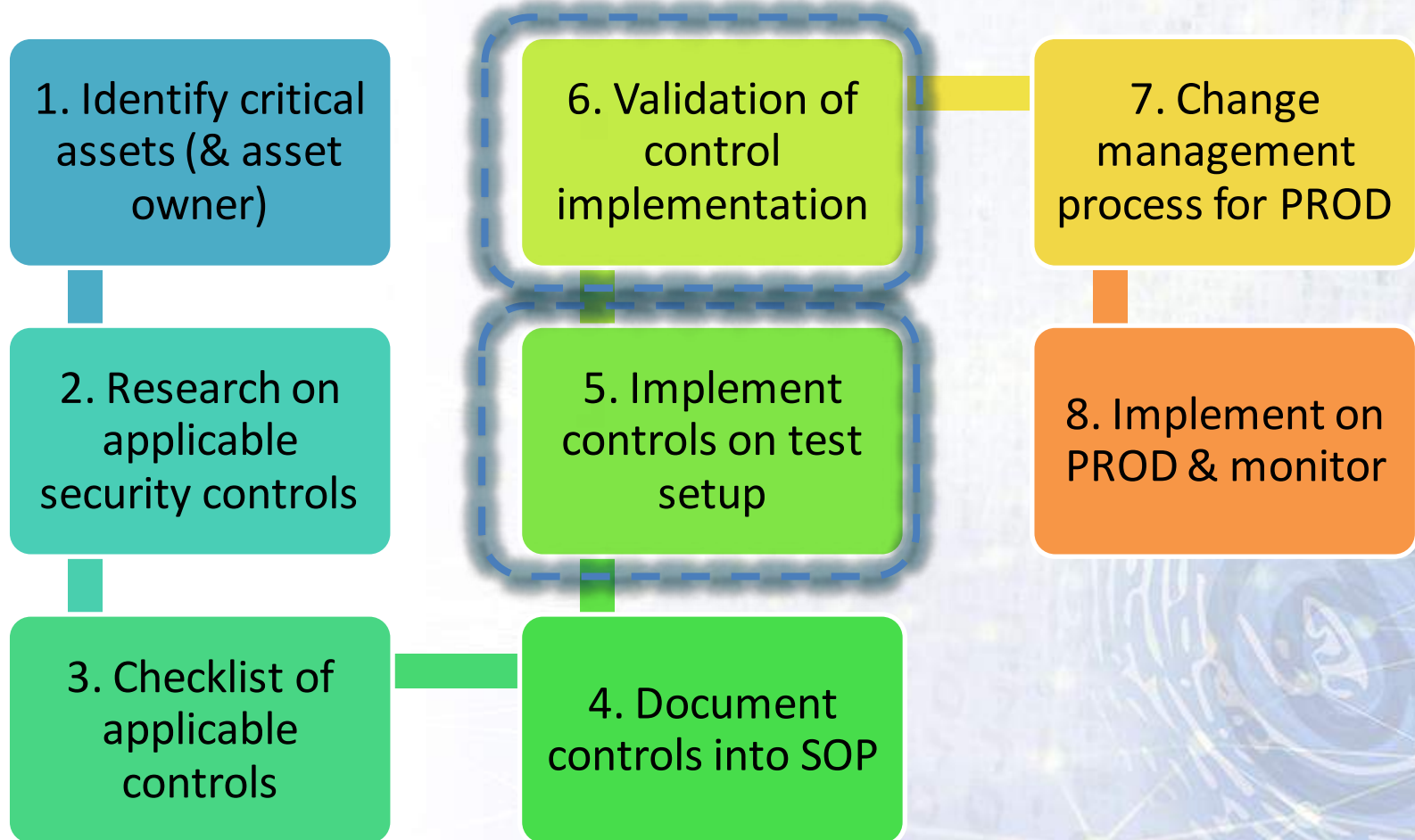
END

InfoSecurity Lifecycle – Security Validation

- Lets have a re-look at the 8-Step Security Hardening Methodology

InfoSecurity Lifecycle – Security Validation

8 STEP METHODOLOGY FOR SECURITY HARDENING



InfoSecurity Lifecycle – Security Validation

- Validation during security hardening:
 - Purpose here is to only **validate or confirm** that the intended controls have **been correctly and completely applied** in the pilot setup

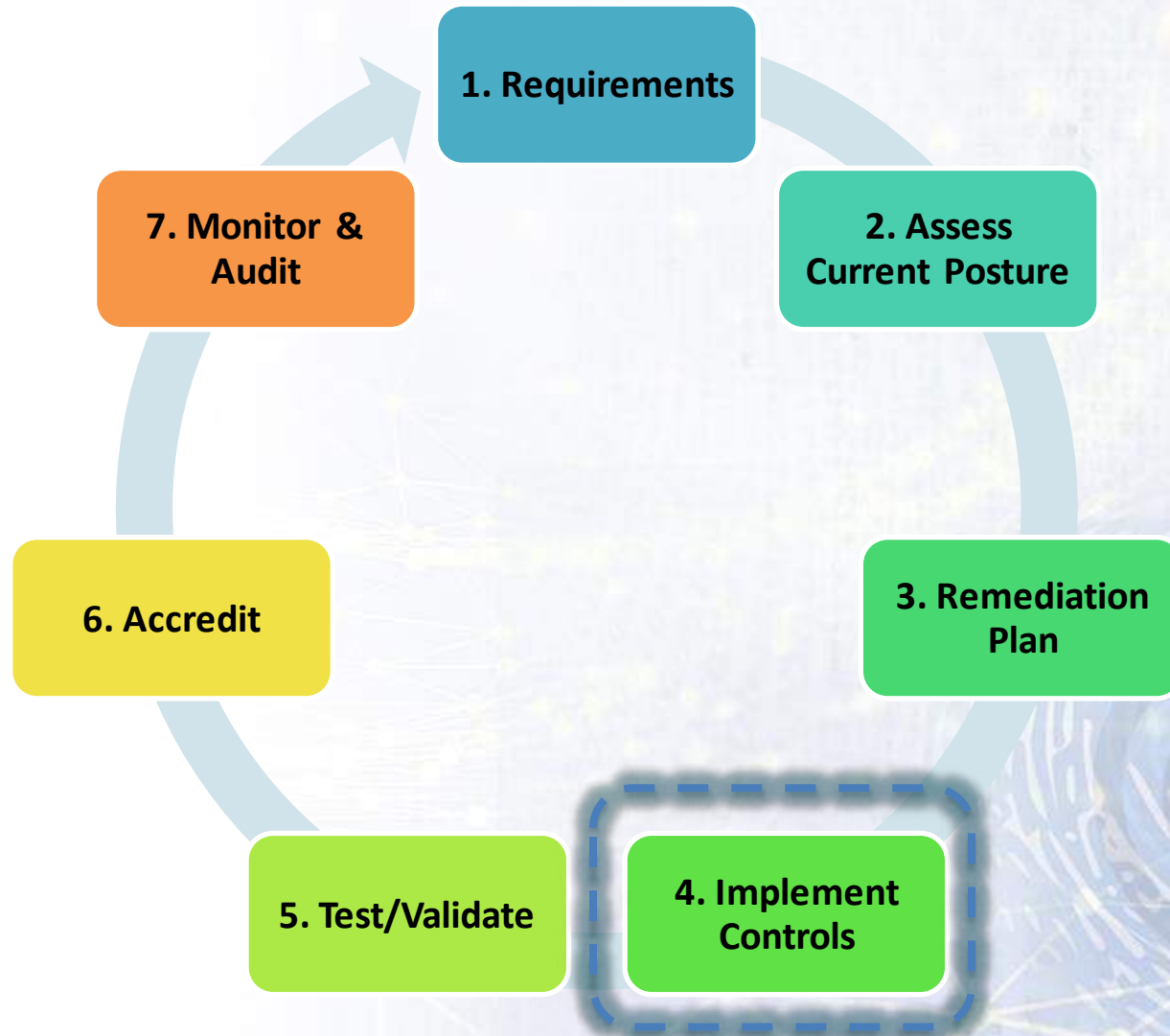
InfoSecurity Lifecycle – Security Validation

- **Validation during security hardening:**
 - Nothing mentioned for production environment
 - Nothing mentioned for **BUSINESS LAUNCH (GO-LIVE)**

InfoSecurity Lifecycle – Security Validation

- Now lets look at the more comprehensive Information Security Lifecycle (7 stages) which is not specific to security hardening

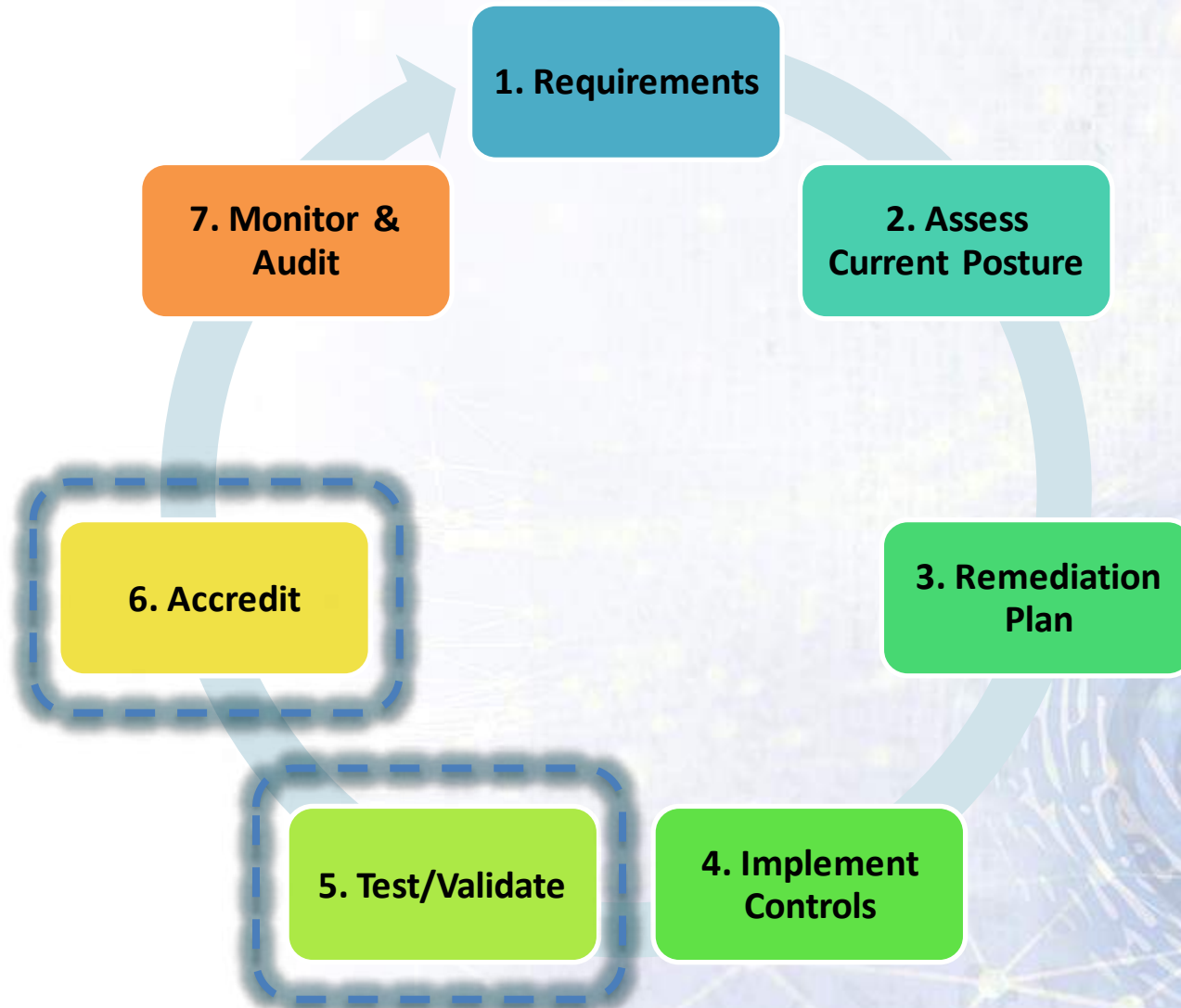
InfoSecurity Lifecycle – Security Validation



InfoSecurity Lifecycle – Security Validation

- In the Information Security Lifecycle chart, we have already gone into production **“environment”** with Stage 4
- However, formal approval for **BUSINESS LAUNCH** (GO-LIVE) has not yet been issued
- **Security accreditation has not taken place**

InfoSecurity Lifecycle – Security Validation



InfoSecurity Lifecycle – Security Validation

- In the Information Security Lifecycle chart Stage 5 & 6:
- ... Refer to activities carried out in PRODUCTION “environment”
- ... But before Business launch (GO-LIVE) has taken place

InfoSecurity Lifecycle – Security Validation



InfoSecurity Lifecycle – Security Validation

- The formal **business launch or GO-LIVE** only takes place after Information Security team **accredits** that the new application/portal or service is secure
- Business launch or GO-LIVE also has business related activities as dependencies such as marketing, & other

InfoSecurity Lifecycle – Security Validation

- Business launch or GO-LIVE **dependencies:**
 - UAT & application **bug testing and feature testing**
 - **Facilities** readiness
 - **Sales & marketing** Launch **ceremony**
 - **Partner** readiness
 - Org **service** **readiness**

InfoSecurity Lifecycle – Security Validation

- Lets look at the following steps in more detail and granularity in the following modules:
 - Security **validation**
 - Security **testing**
 - Security **accreditation**

What is Security Validation ?

- What does security validation mean ?
 - To confirm via **walk-through of system or device** that the security controls implemented by an IT team have **actually been implemented correctly**

What is Security Validation ?

- Who implements the security controls ?
 - **Under the Security Transformation Model, security controls are implemented by the IT teams**

What is Security Validation ?

- Who conducts security validation?
 - Security controls are validated by the **Information Security team or by a third-party consultant** following the principle of **segregation of duty**

What is Security Validation ?

- Why do we need to validate security controls?
 1. To check the **completeness** of the controls
 2. To check the **correctness** of the controls
 3. As an overall **assurance**

What is Security Validation ?

1. To check the **completeness** of the controls:
 - Usually **100's of controls** need to be implemented
 - There may be **genuine omissions** by technical team members
 - There may have been **errors** made

What is Security Validation ?

2. To check the **correctness** of controls:
- Technical **capabilities** of **teams** vary
 - Technical capabilities of **team members** vary
 - A technical issue may not have been understood correctly

What is Security Validation ?

3. As an overall **assurance**:

- IT team may not have **sufficient resources** to ensure 100% completeness and correctness
- Implementation by IT and validation by Information Security team forms a **healthy team relationship**

What is Security Validation ?

3. As an overall **assurance**:

- This is also referred to as **maker-checker** principal
- Some of the controls may have been designated as **“not-applicable”** or **“not possible”** and the reasons and justification needs to be reviewed

What is Security Validation ?

3. As an overall **assurance**:

- **Significant resources are allocated** to the security transformational program; **even one control missed** may affect the security posture
- **Uncovered** at the time of **hack/attack**

What is Security Validation ?

3. As an overall **assurance**:

- **Ability, integrity and diligence** of team members are key factors

<http://whatis.techtarget.com/definition/four-eyes-principle>

- **Healthy technical debate and cross-checks** have a **positive outcome** on the program

What is Security Validation ?

- The Information Security team or the ISMC is tasked with the **overall responsibility** of the success of the program
- Any **lapses discovered later** fall **squarely** under the **responsibility of InfoSec/ISMC**

What is Security Validation ?

- Security validation becomes an **essential activity** and needs to be established in an environment of **healthy & professional commitment** to ensure the **100% complete and correct implementation & upkeep** of the controls

END...

How is Security Validation Performed ?

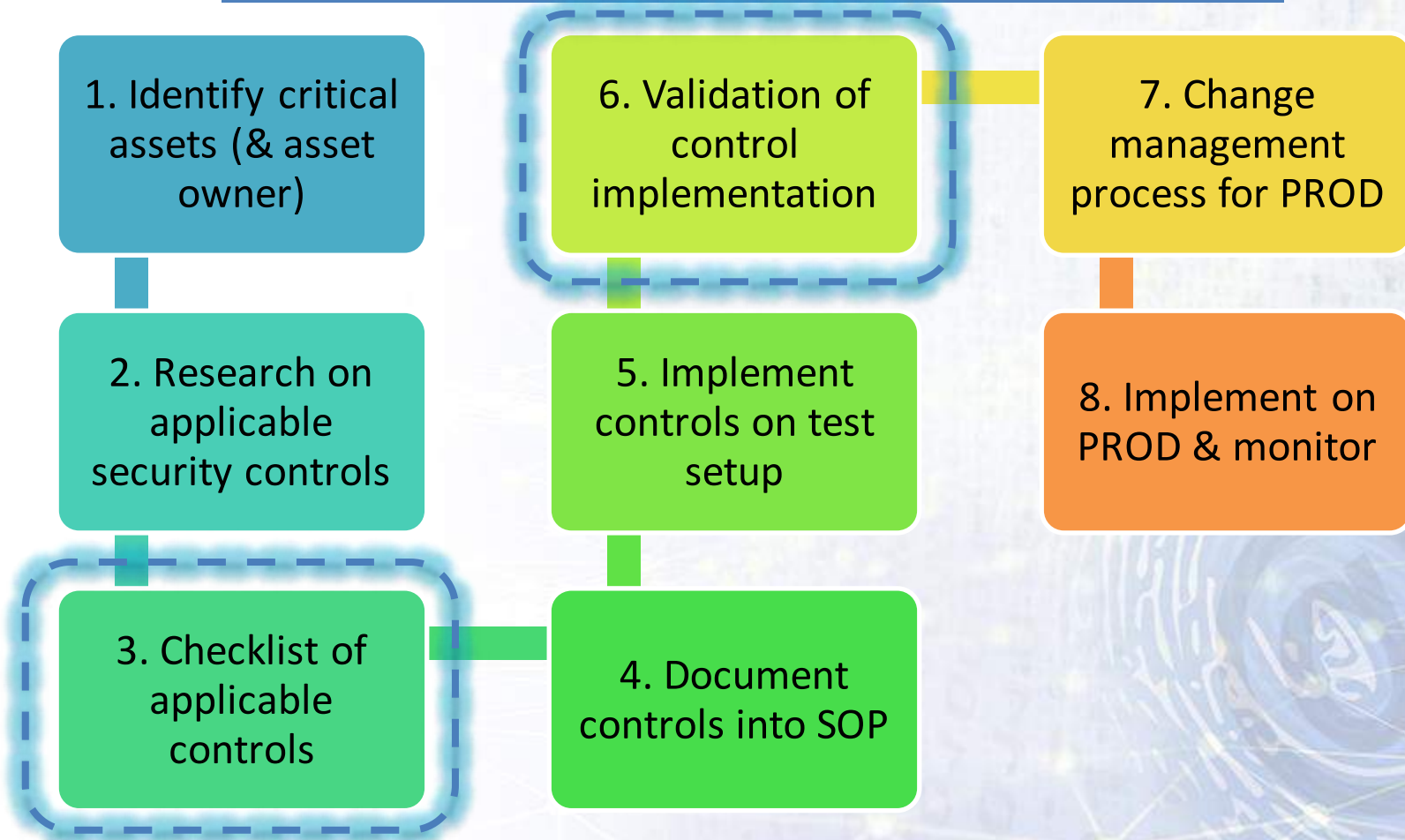
- **Ownership** of security validation lies with Information Security team, alternately with an Information Security consultant
- **Driven by ISMC or Head of Information Security**

How is Security Validation Performed ?

- **Security validation is the same** irrespective if performed specific to 8-Step Security Hardening (Model) or to the Information Security Lifecycle

How is Security Validation Performed ?

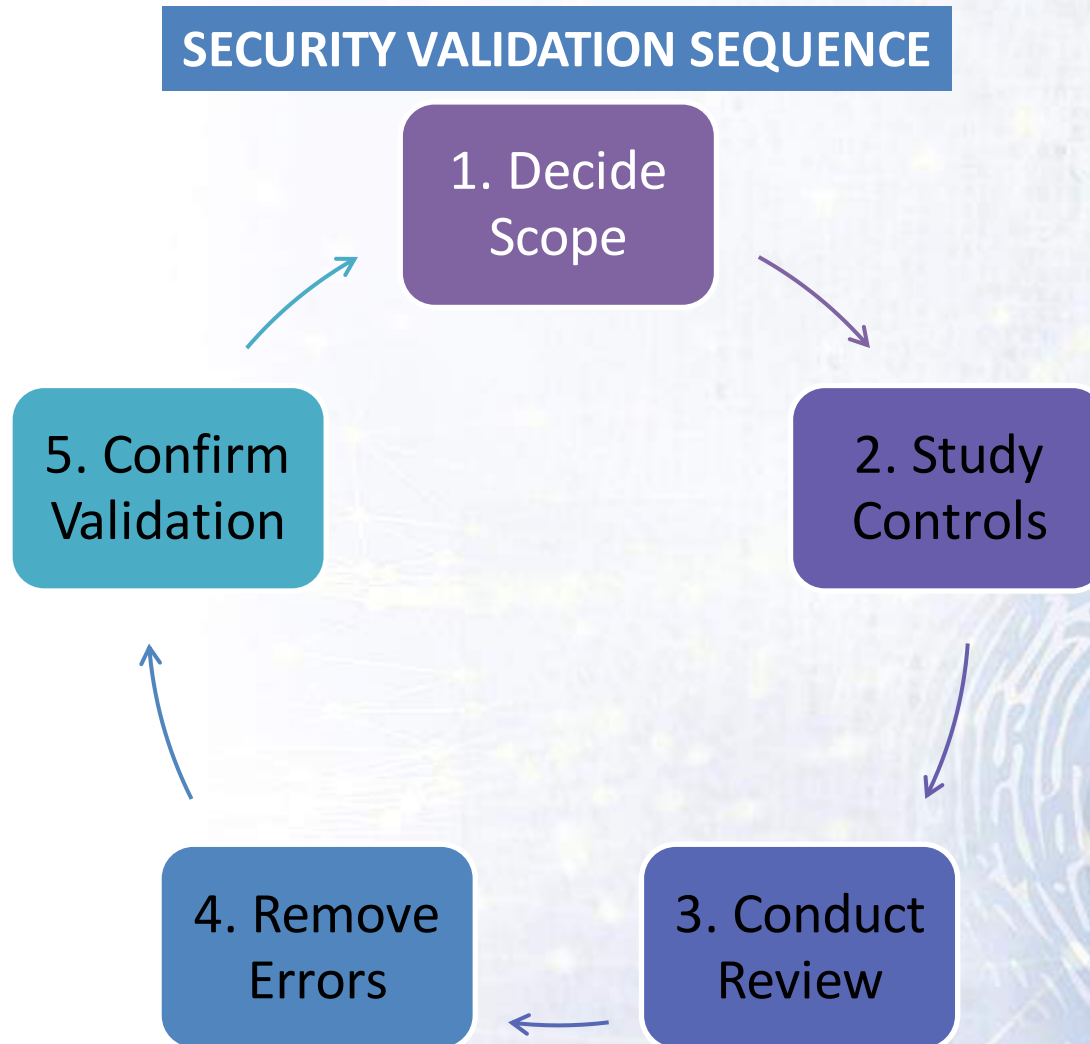
8 STEP METHODOLOGY FOR SECURITY HARDENING



How is Security Validation Performed ?

STEP	DESCRIPTION	PERFORMED BY	FACILITATED BY
1	IDENTIFY CRITICAL ASSETS (& ASSET OWNER)	ISMC	HEAD OF IT SECTION
2	RESEARCH APPLICABLE SECURITY CONTROLS	INFOSEC TEAM	ISMC
3	CHECKLIST OF APPLICABLE SECURITY CONTROLS	INFOSEC TEAM	TEAM LEAD
4	DOCUMENT CONTROLS INTO SOP	TEAM LEAD	INFOSEC TEAM
5	IMPLEMENT CONTROLS ON TEST SETUP	IT OPERATIONS TEAM	TEAM LEAD
6	VALIDATION OF CONTROL IMPLEMENTATION	INFOSEC TEAM	IT OPERATIONS TEAM
7	CHANGE MANAGEMENT PROCESS FOR PRODUCTION	TEAM LEAD	ISMC
8	PRODUCTION & MONITOR	IT OPERATIONS TEAM	TEAM LEAD

How is Security Validation Performed ?



How is Security Validation Performed ?

1. Decide Scope
 - Acquire checklist of applied controls from IT team
 - Decide stakeholders who will conduct review (IT & InfoSec)
 - Schedule the review and send formal email to IT (plus calendar invite)

How is Security Validation Performed ?

2. Study Controls

- Information Security team to acquire original controls from CIS/DISA/other
- Study & understand the controls
- Mark the checklist & ensure correctness
- Prepare docs & notes for actual review

How is Security Validation Performed ?

3. Conduct Review

- One person to conduct review & one to take notes
- Walkthrough of each control
- Random sampling of controls (20-30%)
- Agree on any action items for shortcomings with timeline

How is Security Validation Performed ?

- Important to discuss & understand controls marked by IT team as:
 - Not-applicable
 - Not-possible
- Understand reasoning
- Verify dependencies if any
- Challenge the IT team view wherever appropriate

How is Security Validation Performed ?

4. Remove Errors:

- IT team to remove any shortcomings or omissions in control implementation
- IT team reports back to InfoSec team when all shortcomings fixed

How is Security Validation Performed ?

5. Confirm Validation

- InfoSec team schedules another session with IT team to confirm that all shortcomings have been removed
- InfoSec team adds a confirmation column & comments column to checklist

How is Security Validation Performed ?

5. Confirm Validation

- Status of validation communicated to relevant IT teams & stakeholders
- Records updated to register the validation activity
- Project management stats updated accordingly (% complete)

END

What Is Security Testing ?

- **What is security testing ?**
 - Security testing is a process intended to reveal flaws in the security mechanisms of an information system that protect data and maintain functionality as intended

What Is Security Testing ?

- Security testing is not validation
 - Security testing consists of running tests through a manual process or automated tools to discover weaknesses, flaws, or bugs in the software, application or device

What Is Security Testing ?

- Types of security testing:
 - Vulnerability assessment (VA)
 - Penetration testing (PT)
 - Other security tests through various automated tools
 - Code review (initiated in test environment)

What Is Security Testing ?

1. Vulnerability assessment:
 - VA scanners have various tests built-in such as for malware, vulnerabilities, web application flaws (e.g. OWASP top ten)
 - Compliance scanning against CIS/DISA benchmarks

What Is Security Testing ?

2. Penetration Testing:

- Penetration testing (also called pen testing) is the practice of testing a computer system, network or Web application to find vulnerabilities that an attacker could exploit.

<http://searchsoftwarequality.techtarget.com/definition/penetration-testing>

What Is Security Testing ?

2. Penetration Testing:

- Usually outsourced to a third-party depending on nature and criticality of the application or service being launched
- Highly specialized skill not commonly found in-house

What Is Security Testing ?

2. Penetration Testing:

- Pen tests can be automated with software applications or they can be performed manually. Either way, the process includes gathering information about...

<http://searchsoftwarequality.techtarget.com/definition/penetration-testing>

What Is Security Testing ?

2. Penetration Testing:

- ... the target before the test (reconnaissance), identifying possible entry points, attempting to break in (either virtually or for real) and reporting back the findings

<http://searchsoftwarequality.techtarget.com/definition/penetration-testing>

What Is Security Testing ?

3. Other security tests:

- If the testing is being conducted in-house, the tests should be conducted in the pilot/testing/staging environment and re-validated in the Production environment

What Is Security Testing ?

3. Other security tests:

- If the testing is being conducted by a third-party specialist (such as for penetration testing), it will normally be conducted only in the Production environment (prior to GO-LIVE)

What Is Security Testing ?

3. Other security tests (in-house):

- In-house testing capability & experience
- Conduct the tests (e.g. OWASP ZAP tool)
- Report findings
- Re-confirm once remediation done by IT

What Is Security Testing ?

3. Other security tests (outsourced):

- As mentioned, will most likely be conducted in Production environment, prior to GO-LIVE
- Follow same sequence as for in-house testing

What Is Security Testing ?

4. Code review:

- Code review examines flaws and vulnerabilities in programming source code
- A complete cycle, initiated early and in pilot testing phase
- May be conducted for production applications as well

What Is Security Testing ?

4. Code review:

- Requires a mature internal process, experience and capability
- May be integrated with software QA testing

END

What Is Security Accreditation ?

- What is security accreditation?
 - Accreditation is the formal acceptance of the adequacy of the system's overall security by the management (SANS)

<https://www.sans.org/reading-room/whitepapers/accreditation/introduction-certification-accreditation-1259>

What Is Security Accreditation ?

- Lets have another look at the Information Security Lifecycle...

What Is Security Accreditation ?



What Is Security Accreditation ?

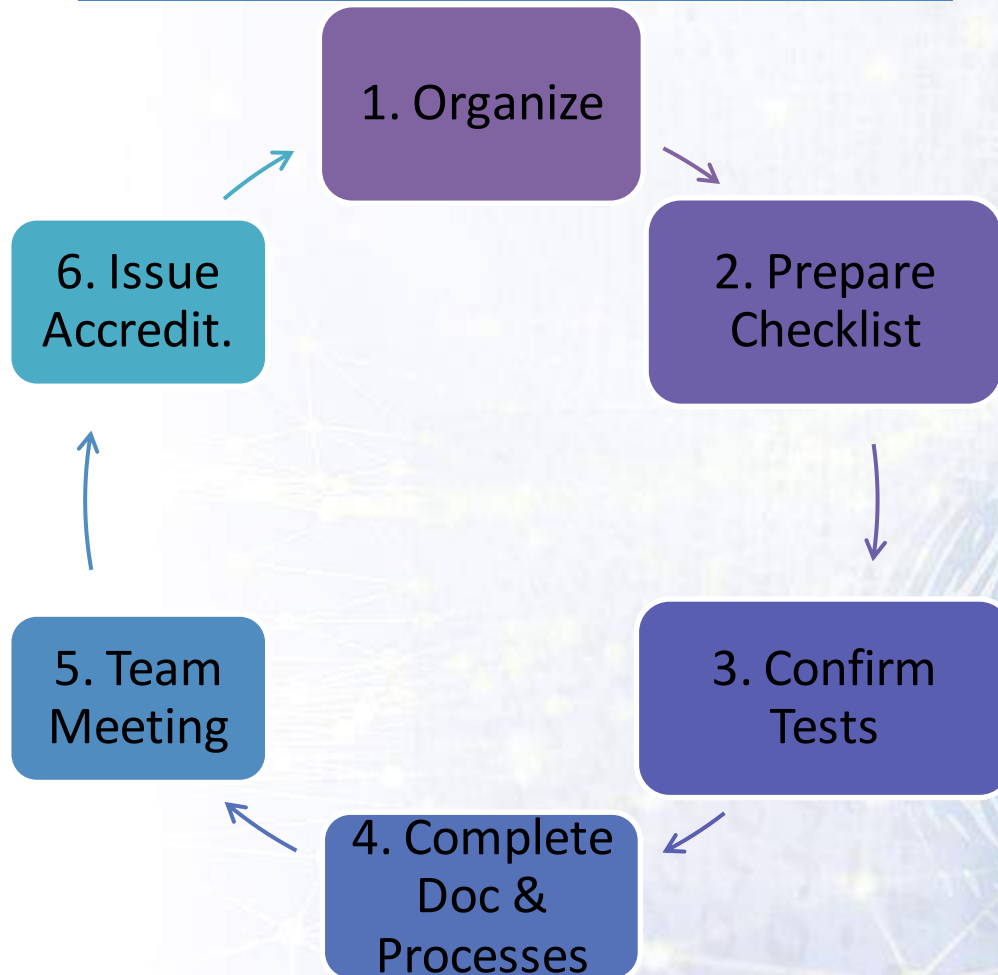
- Whenever a new, significant portal, application, or service is launched, management requires Information Security team to certify after carrying out the required security validation & security testing that the...

What Is Security Accreditation ?

- Security of the new portal/application or service has been **thoroughly examined & tested** and **meets the min requirements** as per **organizational security policy**
- That the new portal/application is safe & secure & is **free from security risks**

What Is Security Accreditation ?

SECURITY ACCREDITATION SEQUENCE



What Is Security Accreditation ?

Security Accreditation Sequence

1. Organize

- Collect all security **requirements**, related security **policy & SOPs**, hardening checklists, validation **status reports**, **test reports**, completion status reports

What Is Security Accreditation ?

Security Accreditation Sequence

1. ...Organize

- Information Security team ensures that the full context of the security risks/impact are understood
- Subsequent security hardening & testing has been fully covered

What Is Security Accreditation ?

Security Accreditation Sequence

2. Prepare Checklist & Share With Stakeholders

- Checklist should cover all activities & their status for completion of accreditation
- Share with stakeholders for feedback

END

What Is Security Accreditation – Part 2 ?

- What is security accreditation?
 - Accreditation is the **formal acceptance of the adequacy** of the system's overall security by the management (SANS)

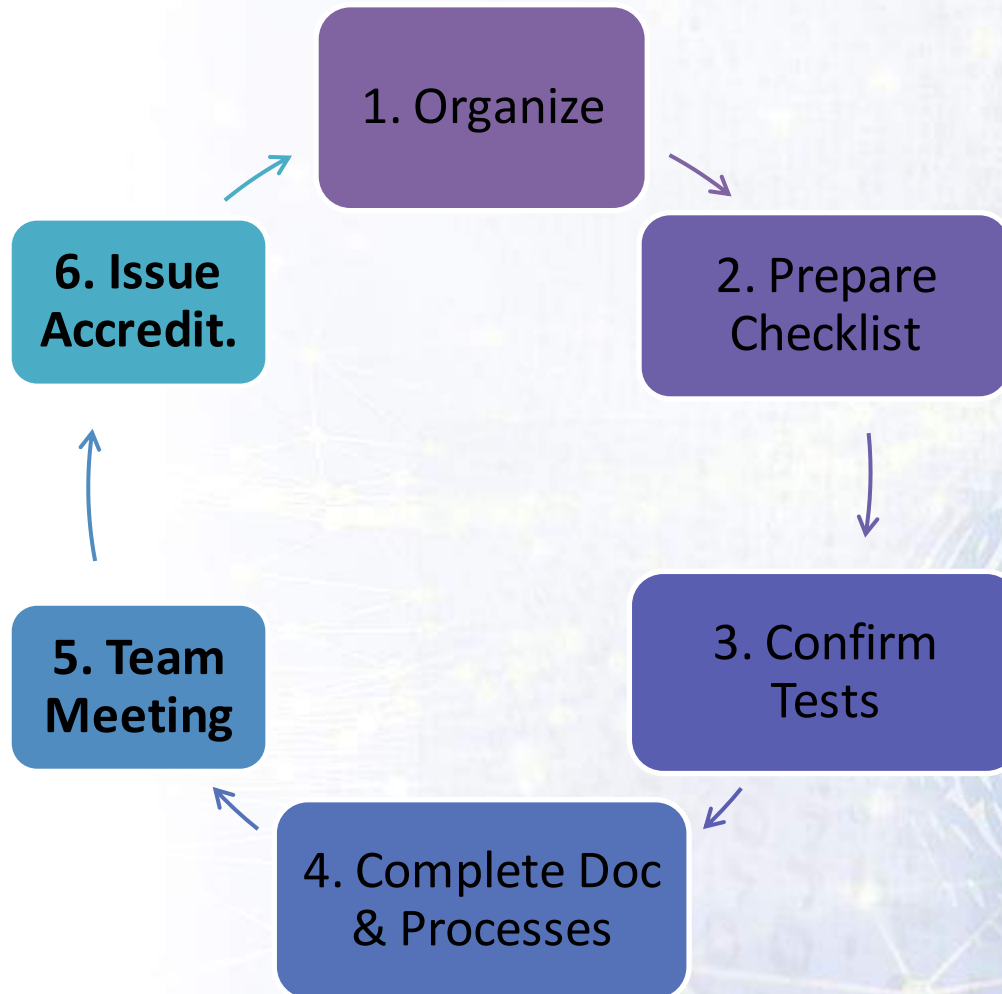
<https://www.sans.org/reading-room/whitepapers/accreditation/introduction-certification-accreditation-1259>

What Is Security Accreditation – Part 2 ?

- Lets have another look at the Security Accreditation Sequence...

What Is Security Accreditation – Part 2 ?

SECURITY ACCREDITATION SEQUENCE



What Is Security Accreditation – Part 2 ?

Security Accreditation Sequence

3. Confirm Tests

- Core activity: confirm that **all test reports are satisfactory**
- **All tests and follow-up remediation measures have been completed**

What Is Security Accreditation – Part 2 ?

Security Accreditation Sequence

4. Documentation & Processes (Complete)

- Reconfirm **correct versions**
- Re-check **checklists, SOPs**
- **Backups & DR**
- All **change control measures & sign-offs**

What Is Security Accreditation – Part 2 ?

Security Accreditation Sequence

4. Documentation & Processes (Complete)

- Re-check all **management approvals**
- Re-check **UATs**, customer sign-offs
- Check **application performance** issues

What Is Security Accreditation – Part 2 ?

Security Accreditation Sequence

5. Team Meeting

- Call team meeting and **report status** of all activities
- List any **snags** & decide completion dates
- Seek **stakeholder sign-off** on accreditation form

What Is Security Accreditation – Part 2 ?

Security Accreditation Sequence

5. Team Meeting

- Clarify & recap security requirements & SOPs
- Clarify **what actions will invalidate** the security accreditation

What Is Security Accreditation – Part 2 ?

Security Accreditation Sequence

6. Issue Accreditation

- Once all details completed on accreditation sign-off form issue accreditation
- Business has GO-LIVE permission using tested versions

What Is Security Accreditation – Part 2 ?

Security Accreditation Sequence

6. Issue Accreditation

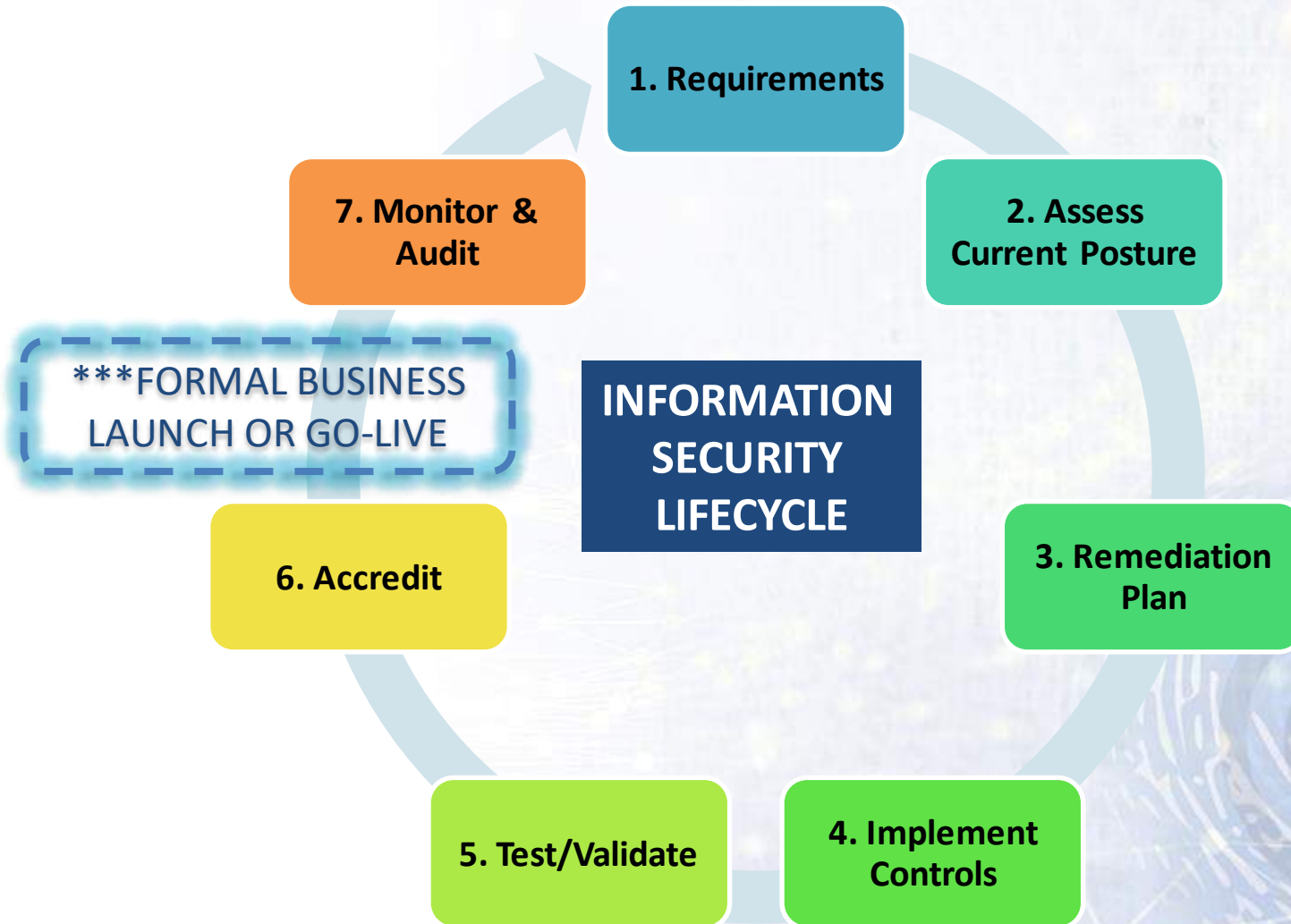
- Enter activities for accredited IT assets into **IT audit program**
- **Update Operations teams, incident management, and risk management register**

END

Embedding InfoSec Lifecycle Into SDLC

- The systems development life-cycle (SDLC) should embed the Information Security activities forming a sec-SDLC (secure SDLC)

Embedding InfoSec Lifecycle Into SDLC



Embedding InfoSec Lifecycle Into SDLC

- Software Assurance Maturity Model (SAMM) developed by OWASP
 - A guide to building security into software development
 - 96 page PDF

<http://www.opensamm.org/downloads/SAMM-1.0.pdf>

Embedding InfoSec Lifecycle Into SDLC

This is an OWASP Project



OWASP

The Open Web Application Security Project

SAMM Overview

Business Functions

Security Practices



Embedding InfoSec Lifecycle Into SDLC

- Four **critical business functions**
- For each business function there are **three security practices**
- For each security practice, **three maturity levels as objectives**

<http://www.opensamm.org/downloads/SAMM-1.0.pdf> (PAGE 3)

Embedding InfoSec Lifecycle Into SDLC

- The Software Assurance Maturity Model (SAMM) is an **open framework** to help organizations formulate and implement a strategy for software security that is tailored to the specific risks facing the organization.

<http://www.opensamm.org/downloads/SAMM-1.0.pdf> (PAGE 3)

Embedding InfoSec Lifecycle Into SDLC

This is an OWASP Project



OWASP

The Open Web Application Security Project



Governance

Strategy &
Metrics

Education &
Guidance

Policy &
Compliance

Embedding InfoSec Lifecycle Into SDLC

This is an OWASP Project



OWASP

The Open Web Application Security Project



Construction

Security
Requirements

Threat
Assessment

Secure
Architecture

Embedding InfoSec Lifecycle Into SDLC

This is an OWASP Project



OWASP

The Open Web Application Security Project



Verification

Design
Review

Security
Testing

Code
Review

Embedding InfoSec Lifecycle Into SDLC

This is an OWASP Project



OWASP

The Open Web Application Security Project



Deployment

Environment
Hardening

Vulnerability
Management

Operational
Enablement

Embedding InfoSec Lifecycle Into SDLC

Maturity Levels

Each of the twelve Security Practices has three defined Maturity Levels and an implicit starting point at zero. The details for each level differs between the Practices, but they generally represent:

- 0** Implicit starting point representing the activities in the Practice being unfulfilled
- 1** Initial understanding and ad hoc provision of Security Practice
- 2** Increase efficiency and/or effectiveness of the Security Practice
- 3** Comprehensive mastery of the Security Practice at scale

This is an OWASP Project



OWASP

The Open Web Application Security Project

Embedding InfoSec Lifecycle Into SDLC

- The SAMM document sections:
 1. Understanding the model
 2. Applying the model
 3. Security practices
 4. Case studies

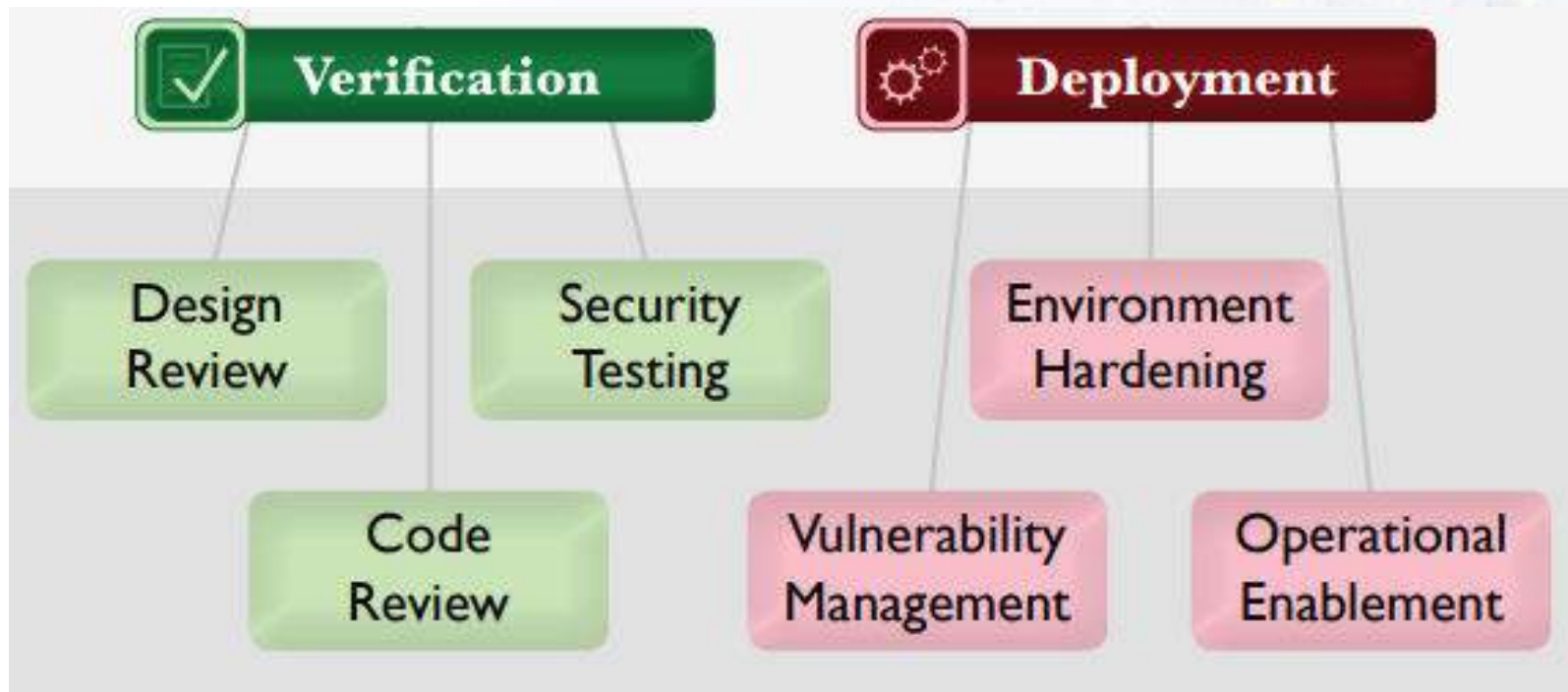
<http://www.opensamm.org/downloads/SAMM-1.0.pdf>

END

Software Security Testing & Validation–1

- The OWASP Software Assurance Maturity Model (SAMM) undertakes software security testing & validation during the following phases:
 - **Verification**
 - Deployment

Software Security Testing & Validation-1



Software Security Testing & Validation–1

- OWASP Software Assurance Maturity Model (SAMM)
Verification Phase:
 - Design Review
 - Code Review
 - Security Testing

Software Security Testing & Validation–1

- Design Review:
 - Focused on assessment of **software design and architecture** for security-related problems
 - Detect **architecture-level issues early** in software...

Software Security Testing & Validation–1

- Design Review:
 - ... development and thereby **avoid potentially large costs** from refactoring later due to security concerns

Software Security Testing & Validation-1

Design Review

...more on page 58



OBJECTIVE

Support ad hoc reviews of software design to ensure baseline mitigations for known risks

Offer assessment services to review software design against comprehensive best practices for security

Require assessments and validate artifacts to develop detailed understanding of protection mechanisms

ACTIVITIES

- A. Identify software attack surface
- B. Analyze design against known security requirements

- A. Inspect for complete provision of security mechanisms
- B. Deploy design review service for project teams

- A. Develop data-flow diagrams for sensitive resources
- B. Establish release gates for design review

Software Security Testing & Validation–1

- Code Review:
 - Focused on **inspection of software at the source code level** in order to find security vulnerabilities.
 - Code-level vulnerabilities are generally simple to understand...

Software Security Testing & Validation–1

- Code Review:
 - ... conceptually, but even **informed developers can easily make mistakes** that leave software open to potential compromise.

Software Security Testing & Validation-1

Code Review

...more on page 62



OBJECTIVE

Opportunistically find basic code-level vulnerabilities and other high-risk security issues

Make code review during development more accurate and efficient through automation

Mandate comprehensive code review process to discover language-level and application-specific risks

ACTIVITIES

- A. Create review checklists from known security requirements
- B. Perform point-review of high-risk code

- A. Utilize automated code analysis tools
- B. Integrate code analysis into development process

- A. Customize code analysis for application-specific concerns
- B. Establish release gates for code review

Software Security Testing & Validation–1

- Security Testing:
 - Focused on **inspection of software in the runtime environment** in order to find security problems.
 - These testing activities bolster the assurance case for software by...

Software Security Testing & Validation–1

- Security Testing:
 - ... **checking it in the same context in which it is expected to run**, thus making visible **operational misconfigurations or errors in business logic** that are difficult to otherwise find.

Software Security Testing & Validation-1

Security Testing

...more on page 66



OBJECTIVE

Establish process to perform basic security tests based on implementation and software requirements

Make security testing during development more complete and efficient through automation

Require application-specific security testing to ensure baseline security before deployment

ACTIVITIES

- A. Derive test cases from known security requirements
- B. Conduct penetration testing on software releases

- A. Utilize automated security testing tools
- B. Integrate security testing into development process

- A. Employ application-specific security testing automation
- B. Establish release gates for security testing

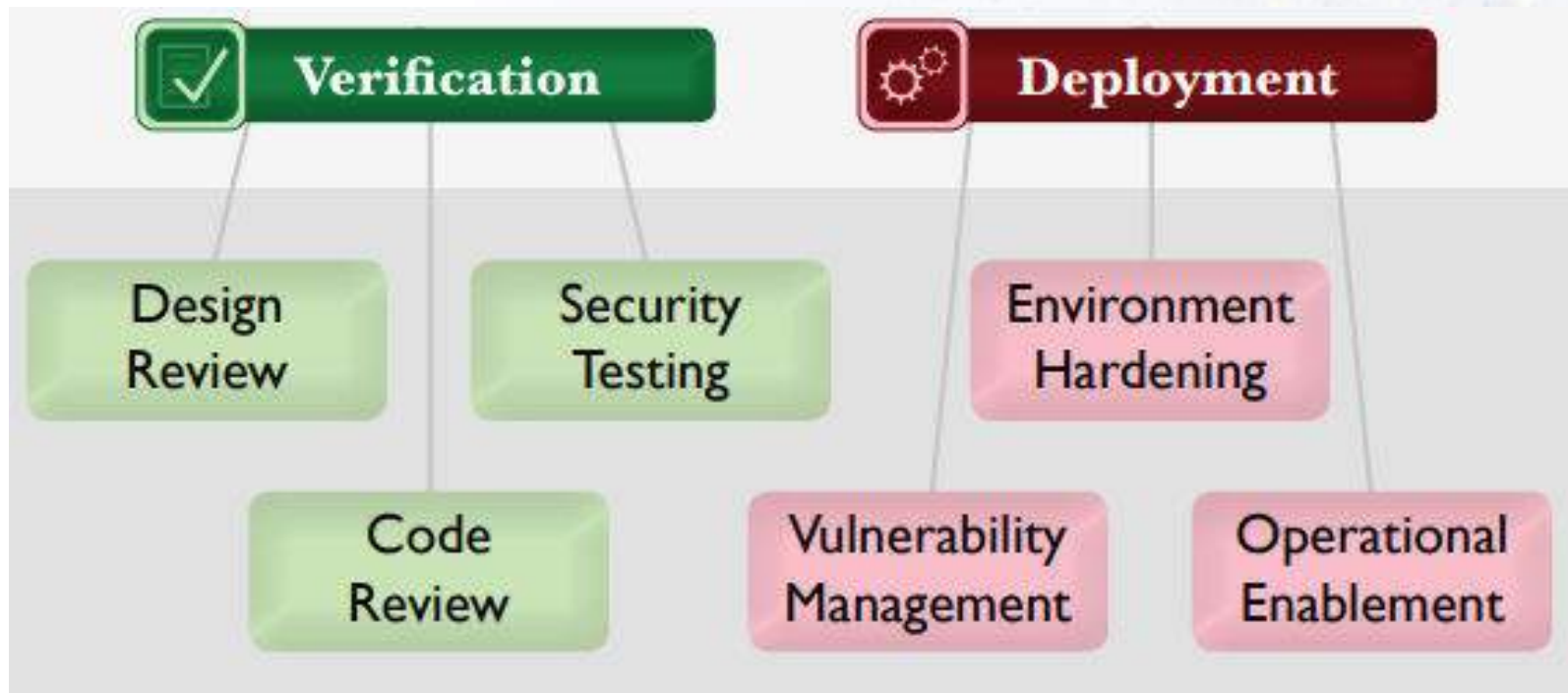
Software Security Testing & Validation-1

- Lets look at SAMM Deployment Phase in the next module...

Software Security Testing & Validation–2

- The OWASP Software Assurance Maturity Model (SAMM) undertakes software security testing & validation during the following phases:
 - Verification
 - **Deployment**

Software Security Testing & Validation-2



Software Security Testing & Validation–2

- OWASP Software Assurance Maturity Model (SAMM)
Deployment Phase:
 - Environment Hardening
 - Vulnerability Management
 - Operational Enablement

Software Security Testing & Validation–2

- **Environment Hardening:**
 - Focused on **building assurance for the runtime environment** that hosts the organization's software.
 - Since secure operation of an application can be...

Software Security Testing & Validation–2

- **Environment Hardening:**
 - ... **deteriorated by problems in external components,** hardening this **underlying infrastructure directly improves the overall security posture** of the software

Software Security Testing & Validation–2

Environment Hardening			
	 EH 1	 EH 2	 EH 3
OBJECTIVE	Understand baseline operational environment for applications and software components	Improve confidence in application operations by hardening the operating environment	Validate application health and status of operational environment against known best practices
ACTIVITIES	A. Maintain operational environment specification B. Identify and install critical security upgrades and patches	A. Establish routine patch management process B. Monitor baseline environment configuration status	A. Identify and deploy relevant operations protection tools B. Expand audit program for environment configuration

Software Security Testing & Validation–2

- **Vulnerability Management:**
 - Focused on the processes within an organization with respect to handling vulnerability reports and operational incidents.
 - By having these processes in place, an organization's

Software Security Testing & Validation–2

- **Vulnerability Management:**
 - ... projects will have consistent expectations and increased efficiency for handling these events, rather than chaotic and uninformed responses.

Software Security Testing & Validation-2

Vulnerability Management				...more on page 70
	 VM1	 VM2	 VM3	
OBJECTIVE	Understand high-level plan for responding to vulnerability reports or incidents	Elaborate expectations for response process to improve consistency and communications	Improve analysis and data gathering within response process for feedback into proactive planning	
ACTIVITIES	A. Identify point of contact for security issues B. Create informal security response team(s)	A. Establish consistent incident response process B. Adopt a security issue disclosure process	A. Conduct root cause analysis for incidents B. Collect per-incident metrics	

Software Security Testing & Validation–2

- **Operational Enablement:**
 - Focused on gathering security critical information from the project teams building software and communicating it to the users and operators of the software.

Software Security Testing & Validation–2

- **Operational Enablement:**
 - Without this information, even the most securely designed software carries undue risks since important security characteristics and choices will not be known at a deployment site.

Software Security Testing & Validation-2

Operational Enablement			...more on page 78
	 OE 1	 OE 2	 OE 3
OBJECTIVE	Enable communications between development teams and operators for critical security-relevant data	Improve expectations for continuous secure operations through provision of detailed procedures	Mandate communication of security information and validate artifacts for completeness
ACTIVITIES	A. Capture critical security information for deployment B. Document procedures for typical application alerts	A. Create per-release change management procedures B. Maintain formal operational security guides	A. Expand audit program for operational information B. Perform code signing for application components

Software Security Testing & Validation–2

- SAMM is an excellent model for software (security) assurance
- **OWASP** also has a multitude of additional materials, guidance, and tools for software and web application security

END

Embedding InfoSec Into Project Management

- PMIs five phases of project management:
 - Initiate
 - Plan
 - Executing
 - Controlling
 - Closing

<https://project-management.com/top-5-project-management-phases/>

Embedding InfoSec Into Project Management

Initiate

Project sponsorship, requirement gathering & analysis, develop project charter

SECURITY TASKS:

- Security requirements study
- Security impact assessment
- Security section in project charter

Embedding InfoSec Into Project Management

Plan

Build project plan and identify resources & schedule for the project

SECURITY TASKS:

- Identify security role, team, and resources
- Risk management plan
- Embed security tasks into phased project plan

Embedding InfoSec Into Project Management

Executing

Execute the project, project performance review & corrections

SECURITY TASKS:

- Track security tasks
- Security dashboard
- Weekly, monthly, quarterly progress reports

Embedding InfoSec Into Project Management

Controlling

Project controlling, monitoring & corrections

SECURITY TASKS:

- Utilize contingency if required
- Prioritize remaining tasks
- Re-plan phases & cover for delays

Embedding InfoSec Into Project Management

Closing

Launch product or solution, relieve resources

SECURITY TASKS:

- Security accreditation
- Identify operational measures
- SOPs, incident management, internal audit, monitoring

Embedding InfoSec Into Project Management

- Senior management needs to ensure that security is integrated with IT project plans
- Sufficient security resources should be made available to manage the security aspects of projects

END

How To Conduct Internal Security Assessment

- What is an internal security assessment?
 - An effort to assess the security posture, risks, or vulnerabilities for any project, service, application, or device

How To Conduct Internal Security Assessment

- When is an internal security assessment required?
 - Launch of a new IT project or service
 - When an incident has occurred
 - On change of leadership
 - Regulatory or compliance reqmts

How To Conduct Internal Security Assessment

- Sequence of security assessment:
 1. Management approval or communication
 2. Assign resources
 3. Build plan, scope and objectives
 4. Conduct assessment
 5. Report findings & remediation measures

How To Conduct Internal Security Assessment

1. Management approval or communication:
 - Authority of the assessment
 - Cooperation from stakeholders
 - Determine & communicate timeline
 - Determine appropriate report format

How To Conduct Internal Security Assessment

2. Assign resources:
 - Assign information security resources with relevant experience
 - Identify respective resources for IT asset to be assessed
 - Hold initial meeting with respective stakeholder POC

How To Conduct Internal Security Assessment

3. Build plan, scope & objectives
 - Study IT asset & gather background security docs
 - Clear scope boundary
 - Clear objectives
 - Determine assessment method based on report format
 - Build plan

How To Conduct Internal Security Assessment

4. Conduct assessment:
 - Conduct the necessary activities such as system walkthrough, vulnerability assessment, security testing, evaluation of security controls, review of process and documentation, etc

How To Conduct Internal Security Assessment

5. Report findings & remediation measures
 - Assimilate and analyze findings
 - Determine level of severity, risk and appropriate remediation
 - Tailor findings to report format & appropriate to forum
 - Share report

How To Conduct Internal Security Assessment

- A few pointers:
 - Security should not be reactive
 - Security transformation project should address security loopholes
 - Align the security assessment with benchmarks established already

END

Different Types Of Security Assessments

- Vulnerability assessment
- Penetration test
- Audits
- Whitebox/greybox/blackbox assessments
- Risk assessment
- Threat assessment
- Bug bounty
- Red team

<https://danielmiessler.com/study/security-assessment-types/#gs.NdADAuQ>

Different Types Of Security Assessments

- Vulnerability assessment:
 - Technical assessment to yield as many vulnerabilities as possible in an environment along with severity and remediation priority information

<https://danielmiessler.com/study/security-assessment-types/#gs.NdADAuQ>

Different Types Of Security Assessments

- Vulnerability assessment:
 - **Best when** security maturity is low to medium, need a prioritized list of everything that's wrong, goal is to fix as many things as possible as efficiently as possible

Different Types Of Security Assessments

- Penetration test:
 - A Penetration Test is a technical assessment designed to achieve a specific goal, e.g., to steal customer data, to gain domain administrator, or to modify sensitive salary information

<https://danielmiessler.com/study/security-assessment-types/#gs.NdADAuQ>

Different Types Of Security Assessments

- Penetration test:
 - Penetration Tests are for testing security that is assumed to be strong
 - No point in wasting the effort if hardening and vulnerability assessment have not been done

Different Types Of Security Assessments

- VA & PT difference:
 - Vulnerability assessments look for security problems when you know/assume they exist, and penetration testing validates a configuration when you believe it to be secure

Different Types Of Security Assessments

- Audit:
 - An audit can be technical and/or documentation-based, and focuses on how an existing configuration compares to a desired standard

<https://danielmiessler.com/study/security-assessment-types/#gs.NdADAuQ>

Different Types Of Security Assessments

- Audit:
 - Orgs use audits to demonstrate compliance
 - Importantly, compliance should not be used to demonstrate security
 - Compliant orgs more likely to be secure

Different Types Of Security Assessments

- Audit:
 - Secure orgs are significantly more likely to be compliant (if checked), but compliant orgs should lay no claims to being secure just because they are in accordance with standard X or Y.

Different Types Of Security Assessments

- Lets look at the following in the next modules:
 - Whitebox/greybox/blackbox assessments
 - Risk assessment
 - Threat assessment
 - Bug bounty
 - Red team

END

<https://danielmiessler.com/study/security-assessment-types/#gs.NdADAuQ>

Types Of Security Assessments-Part 2

- Vulnerability assessment
- Penetration test
- Audits
- Whitebox/greybox/blackbox assessments
- Risk assessment
- Threat assessment
- Bug bounty
- Red team

<https://danielmiessler.com/study/security-assessment-types/#gs.NdADAuQ>

Types Of Security Assessments-Part 2

TYPE OF ASSESSMENT	DESCRIPTION	BEST USED WHEN
WHITEBOX	Tester has full access to all internal information available, such as network diagrams, source code, etc.	Best used with vulnerability assessments because you want to find as many issues as possible

<https://danielmiessler.com/study/security-assessment-types/#gs.NdADAuQ>

Types Of Security Assessments-Part 2

TYPE OF ASSESSMENT	DESCRIPTION	BEST USED WHEN
GREYBOX	Tester has some information but not all	You want to give some information to the tester but not all

<https://danielmiessler.com/study/security-assessment-types/#gs.NdADAuQ>

Types Of Security Assessments-Part 2

TYPE OF ASSESSMENT	DESCRIPTION	BEST USED WHEN
BLACKBOX	Tester is given no knowledge about the network – “attackers perspective”	Performing a penetration test

<https://danielmiessler.com/study/security-assessment-types/#gs.NdADAuQ>

Types Of Security Assessments-Part 2

- Risk assessment:
 - Should involve determining what the current level of acceptable risk is, measuring the current risk level, and then determining what can be done to bring these two in ...

<https://danielmiessler.com/study/security-assessment-types/#gs.NdADAuQ>

Types Of Security Assessments-Part 2

- Risk assessment:
 - ...line where there are mismatches.
Risk Assessments commonly involve the rating of risks in two dimensions: probability, and impact.

<https://danielmiessler.com/study/security-assessment-types/#gs.NdADAuQ>

Types Of Security Assessments-Part 2

- Risk assessment:
 - Umbrella term for determining what you have of value, how it can be attacked, what you would lose if those attacks were successful, and what should be done to address the issues.

<https://danielmiessler.com/study/security-assessment-types/#gs.NdADAuQ>

Types Of Security Assessments-Part 2

- Threat assessment:
 - The driver for the assessment is to determine how many resources—if any—should be spent on addressing the issue in question.

<https://danielmiessler.com/study/security-assessment-types/#gs.NdADAuQ>

Types Of Security Assessments-Part 2

- Threat assessment:
 - A threat assessment is best used in situations where someone has made a claim around performing an attack in the future, or such a potential is uncovered somehow.

<https://danielmiessler.com/study/security-assessment-types/#gs.NdADAuQ>

Types Of Security Assessments-Part 2

- Threat assessment:
 - Lets look at red team exercises and bug bounty programs in the next module

END

Types Of Security Assessments-Part 3

- Vulnerability assessment
- Penetration test
- Audits
- Whitebox/greybox/blackbox assessments
- Risk assessment
- Threat assessment
- Bug bounty
- Red team

<https://danielmiessler.com/study/security-assessment-types/#gs.NdADAuQ>

Types Of Security Assessments-Part 3

- Bug bounty:
 - A Bug Bounty is a type of technical security assessment that leverages crowdsourcing to find vulnerabilities in a system. The central concept is simple: security testers, regardless of quality, have their

<https://danielmiessler.com/study/security-assessment-types/#gs.NdADAuQ>

Types Of Security Assessments-Part 3

- Bug bounty:
 - ... own set of strengths, weaknesses, experiences, biases, & preferences, & these combine to yield different findings for the same system when tested by different people.

<https://danielmiessler.com/study/security-assessment-types/#gs.NdADAuQ>

Types Of Security Assessments-Part 3

- Bug bounty:
 - Best used when you have done multiple Vulnerability Assessments already and have already found the easy stuff. Bug Bounties excel at finding issues not found using other methods.

<https://danielmiessler.com/study/security-assessment-types/#gs.NdADAuQ>

Types Of Security Assessments-Part 3

- Red team assessment:
 - “Red team” is: an independent group that challenges an organization to improve its (security) effectiveness
 - Services should be continuous rather than point-in-time

<https://danielmiessler.com/study/security-assessment-types/#gs.NdADAuQ>

Types Of Security Assessments-Part 3

- Red team assessment:
 - Best used when an org has covered the basics of strong vulnerability management and has at least some capability to detect and respond to malicious or suspicious behavior in the environment

Types Of Security Assessments-Part 3

- Note: the term red team is taken from the military maneuvers where a red team simulates attacks and a blue team takes evasive measures against those attacks

Types Of Security Assessments-Part 3

- In the next module lets take a brief summary of all the various assessment types...

END

<https://danielmiessler.com/study/security-assessment-types/#gs.NdADAuQ>

Types Of Security Assessments-Part 4

- Lets take a look at a brief summary of all the assessment types...

<https://danielmiessler.com/study/security-assessment-types/#gs.NdADuQ>

Types Of Security Assessments-Part 4

TYPE	SUMMARY	OUTPUT
VA	Designed to find as many vulnerabilities as possible for the purpose of prioritizing remediation efforts	The output is a list of prioritized issues.
PT	Designed to determine whether an attacker can achieve specific goals when facing your current security posture, such as stealing sensitive data or other activities that would harm the org	Report stating whether the goals were achieved or not

Types Of Security Assessments-Part 4

TYPE	SUMMARY	OUTPUT
Audit	Designed to determine how a given organization measures against a given standard. Audits, as a rule, do not test security directly, but rather test compliance with a standard.	List of areas that must be fixed in order to achieve compliance

<https://danielmiessler.com/study/securityassessment-types/#gs.NdADAuQ>

Types Of Security Assessments-Part 4

TYPE	SUMMARY
White Box, Grey Box, Black Box Assess- ments	Measure of how much information is being provided to a security testing organization during an assessment. These can be internal, external, application-based, network-based, with or without exploitation, etc

<https://danielmiessler.com/study/securityassessment-types/#gs.NdADAuQ>

Types Of Security Assessments-Part 4

TYPE	SUMMARY	OUTPUT
Risk Assessment	determining the most important risks facing a given organization for the purposes of ensuring that they are brought within acceptable levels for the business.	List of prioritized risks followed by recommendations.

<https://danielmiessler.com/study/securityassessment-types/#gs.NdADAuQ>

Types Of Security Assessments-Part 4

TYPE	SUMMARY	OUTPUT
Threat Assessment	Determining whether a given threat is worth spending limited resources on.	Recommendation of what—if any—amount of effort should be dedicated to the issue

<https://danielmiessler.com/study/securityassessment-types/#gs.NdADAuQ>

Types Of Security Assessments-Part 4

TYPE	SUMMARY
Bug Bounties	Crowdsourcing for the discovery of vulnerabilities in a system. Utilizes large collection of independent researchers who all bring their own perspectives to the testing

<https://danielmiessler.com/study/securityassessment-types/#gs.NdADAuQ>

Types Of Security Assessments-Part 4

TYPE	SUMMARY
Red Team Assessment	Continuously and effectively emulate an organization's real-world attackers for the purpose of improving its defensive capabilities. Red Teams operate continuously, with near-full-scope and very limited restrictions, and constantly evolve their approaches to match and/or exceed the capabilities of the organization's actual attackers.

Types Of Security Assessments-Part 4

- Vulnerability assessment
- Penetration test
- Audits
- Whitebox/greybox/blackbox assessments
- Risk assessment
- Threat assessment
- Bug bounty
- Red team

END

<https://danielmiessler.com/study/security-assessment-types/#gs.NdADAuQ>

STAGES OF 3RD PARTY PENETRATION TEST

1. SYSTEM PORT SCANNING
2. IDENTIFICATION OF SYSTEM SERVICES
3. IDENTIFICATION & VERIFICATION OF SYSTEM VULNERABILITIES
4. PENETRATION TESTING (SYSTEM EXPLOITATION)

STAGES OF 3RD PARTY PENETRATION TEST

1. SYSTEM PORT SCANNING

- Port scanning is one of the most important phases of a vulnerability assessment exercise prior to a penetration test.
- This will be the first tool used by an attacker once he has identified the IP address to be targeted.

STAGES OF 3RD PARTY PENETRATION TEST

1. SYSTEM PORT SCANNING...

- The key part here is to use a multiple of port-scanning tools in order to ensure the least false positives and the maximum information that can be gathered.

STAGES OF 3RD PARTY PENETRATION TEST

2. IDENTIFICATION OF SYSTEM SERVICES

- Once the open ports have been enumerated, it is important to determine the services that are keeping those ports open.
- This is typically done by analyzing the banners thrown back when a default connection is made to the open port.

STAGES OF 3RD PARTY PENETRATION TEST

2. IDENTIFICATION OF SYSTEM SERVICES...

- The latest nmap version allows this to be done using the `-sV` switch.

STAGES OF 3RD PARTY PENETRATION TEST

3. IDENTIFICATION & VERIFICATION OF SYSTEM VULNERABILITIES

- During vulnerability identification, an assessor will perform several activities to detect exploitable weak points.

STAGES OF 3RD PARTY PENETRATION TEST

3. IDENTIFICATION & VERIFICATION OF SYSTEM VULNERABILITIES

These activities include:

- Identify vulnerable services using service banners.
- Perform vulnerability scan to search for known vulnerabilities. Information regarding known vulnerabilities...

STAGES OF 3RD PARTY PENETRATION TEST

3. IDENTIFICATION & VERIFICATION OF SYSTEM VULNERABILITIES

- Information regarding known vulnerabilities can be obtained from the vendors' security announcements, or from public databases such as SecurityFocus, CVE or CERT advisories.

STAGES OF 3RD PARTY PENETRATION TEST

3. IDENTIFICATION & VERIFICATION OF SYSTEM VULNERABILITIES

- Perform false positive and false negative verification (e.g. by correlating vulnerabilities with each other and with previously acquired information).

STAGES OF 3RD PARTY PENETRATION TEST

3. IDENTIFICATION & VERIFICATION OF SYSTEM VULNERABILITIES

- Enumerate discovered vulnerabilities.
- Estimate probable impact (classify vulnerabilities found).
- Identify attack paths and scenarios for exploitation.

STAGES OF 3RD PARTY PENETRATION TEST

4. PENETRATION TESTING (SYSTEM EXPLOITATION)

-Following the approvals of individual attacks by Customer, the assessor tries to gain unauthorized access by circumventing the security measures in place and tries to reach as wide a level of access as possible. This process will have the following steps:

STAGES OF 3RD PARTY PENETRATION TEST

4. PENETRATION TESTING (SYSTEM EXPLOITATION)

- Find proof of concept code/tool
- Find proof of concept code available in your own repository or from publicly available sources to test for vulnerabilities. If the code is from your own trusted repository and...

STAGES OF 3RD PARTY PENETRATION TEST

4. PENETRATION TESTING (SYSTEM EXPLOITATION)

... thoroughly tested, you can use it, otherwise test it in an isolated environment.

- Develop tools/scripts
- Under some circumstances it will be necessary (and cost effective) for assessors to create their own tools and scripts.

STAGES OF 3RD PARTY PENETRATION TEST

4. PENETRATION TESTING (SYSTEM EXPLOITATION)

- ... Test proof of concept code/tool in an isolated environment
- The proof of concept code/tool is used against the target to gain as many points of unauthorized access as possible.
- Document findings

END

Security Transformation: Failure ?

- Let us examine the reasons for proposing a security transformation in the first place:
 - Information security almost one generation behind
 - Arduous to catch up with Information Security posture unless there is a “transformation”

Security Transformation: Failure ?

- Guaranteed failure:
 1. Cosmetic commitment
 2. Not willing to invest in resources
 3. Deficient program structure
 4. Lack of effective project management

Security Transformation: Failure ?

1. Cosmetic Commitment:
 - Lack of awareness & understanding
 - Short-term vision
 - Lack of priority
 - Poorly managed organization

Security Transformation: Failure ?

2. Not Willing To Invest In Resources:
 - Deficient allocation of funds for Information Security Program
 - Not willing to allocate time for IT to perform security tasks
 - Loss-making organization

Security Transformation: Failure ?

3. Deficient Program Structure:

- Ineffective Information Security Management Committee (ISMC)
- Not taking along other stakeholders
- Inexperienced IT or security leadership
- IT team not incentivized

Security Transformation: Failure ?

- 4. Lack Of Effective Project Management:
 - Any project will fail without effective project management
 - Effective planning, execution, monitoring, and reporting
 - Experience & domain knowledge

Security Transformation: Failure ?

- Conclusion:
 - The Information Security Transformation requires a tremendous amount of hard work
 - Not possible without commitment, right strategy, correct structure, and effective execution

END

Benefits Of The Security Transformation

- Key Benefits:
 - Prevention of attacks
 - Prevention of fraud & pilferage
 - A reliable & robust IT setup

Benefits Of The Security Transformation

DAWN

HOME LATEST PAKISTAN TODAY'S PAPER OPINION WORLD SPORT BUSINESS MAGAZINES CULTURE BLOGS TECH POPULAR MULTIMEDIA ARCHIVE  

#RisingPakistan

Our Home.
Our Homeland

Government websites defaced by Indian hackers: reports

Dawn.com | Updated August 14, 2017

 104     19

Websites of multiple departments of the Government of Pakistan, including the Establishment Division, the law ministry, Ministry of Inter Provincial Cooperation, Ministry of Defence and Ministry of Information Technology were hacked on Monday, local news outlets reported.

DAWN
**GET
YOUR
NEWS**

Download the
DAWN.com
mobile app

Benefits Of The Security Transformation

THE EXPRESS
TRIBUNE

Sunday, 20 Aug 2017 | Today's Paper | Advertise

HOME PAKISTAN BUSINESS TECH VIDEOS WORLD OPINION LIFE & STYLE SPORTS
GAMES



Our Home,
Our Homeland

THE EXPRESS TRIBUNE TECHNOLOGY

What is 'WannaCry' and how does the ransomware work?

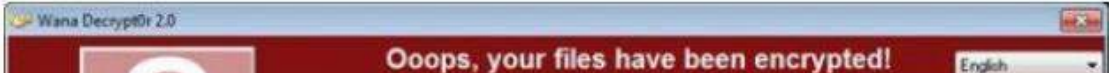
By Reuters Published: May 14, 2017

26 SHARES

f SHARE

🐦 TWEET

✉ EMAIL



Wana Decrypt0r 2.0

Ooops, your files have been encrypted!

English

Benefits Of The Security Transformation

- Impact of attacks:
 - Loss of market goodwill
 - Loss of customer confidence
 - Regulatory fines, legal consequences

Benefits Of The Security Transformation

- Prevention Of Fraud & Pilferage:
 - An effective Information Security Program makes it harder to conduct fraud, abuse, or misuse without getting detected
 - Controls in business process
 - Audits

Benefits Of The Security Transformation

- A Reliable & Robust IT Setup:
 - Business continuity & DR
 - Redundancy
 - Backups
 - Capacity management
 - Change management
 - Incident management

Benefits Of The Security Transformation

- Conclusion:
 - An effective Information Security Program (achieved through an Information Security Transformation) is essential wherever an IT setup exists
 - Not a luxury but an imperative

END

Security Transformation Timeline

- Recommended timeline for security transformation project

Security Transformation Timeline



Security Transformation Timeline

- Month 1: Planning
 - Understand organization & security issues
 - Develop ISMC
 - Identify stakeholders for InfoSec Steering Committee
 - Identify assets for various phases
 - Project kickoff and awareness trainings

Security Transformation Timeline

- Months 2-3: Pilot (Phase 1)
 - Perform hardening of key IT assets in test environment (Pilot)
 - Validate the hardening in the test environment
 - Prime IT & InfoSec teams for their roles
 - Vulnerability management pilot

Security Transformation Timeline



Security Transformation Timeline

- Months 4-5 (Phase 2):
 - Hardening of IT assets (minimum security baseline) identified for phase 2
 - Validation of hardening and moving the hardened IT assets to PROD environment through change management process

Security Transformation Timeline

- Months 6-7 (Phase 3):
 - Hardening of IT assets (minimum security baseline) identified for phase 3
 - Validation of hardening and moving the hardened IT assets to PROD environment through change management process

Security Transformation Timeline

- Months 8-10 (Phase 4):
 - Technical teams continue the IT assets hardening in phase 4
 - Raise vulnerability management program frequency to monthly
 - **Focus on governance (policies, SOPs, etc)**

Security Transformation Timeline

- Months 11-12 (Phase 5):
 - ISO27001:2013 stage 1 and stage 2 certification
 - Stage 1 mostly documentation review
 - Stage 2 mostly implementation review

END

Security Transformation Responsibility

- Responsibility for the security transformation is a balance between management & security team
- IT team led by the CIO plays an instrumental role in the success of the program

Security Transformation Responsibility

- Management role:
 - Commitment
 - Sets the tone at the top
 - Allocates resources
 - Assigns responsibility & roles
 - Conducts periodic performance review

Security Transformation Responsibility

- Information Security Team:
 - Builds an effective strategy & structure for the program
 - Identifies key players to enroll in ISMC
 - Ensures effective execution & project management
 - Conducts transparent reporting

Security Transformation Responsibility

- IT Team:
 - Mobilizes the resources for implementation of the security program
 - Ensures quality and process during the security transformation program
 - Resolves roadblocks in implementation

Security Transformation Responsibility

- Conclusion:
 - An effective Information Security Transformation can only be orchestrated through effective team work
 - All parts of the organization have to play their due role to make the program a success

END

Actions To Raise Management Support

- What can you do if your organizational management is not supporting for the Information Security Transformation Program ?

Actions To Raise Management Support

- a.** Understand the organizational business requirements and potential impact
- b.** Understand regulations & sector best-practices
- c.** Evaluate the security posture
- d.** Assess the extent of work and resources required
- e.** Present your report

Actions To Raise Management Support

- a. Understand the organizational business requirements & potential impact:
- Type of business/industry
 - Business requirements
 - Confidentiality, integrity, availability
 - What can go wrong and impact?

Actions To Raise Management Support

b. Understand regulations and sector best-practices

- Financial industry (SBP)
- Telecoms & IT industry (PTA/MOITT)
- Oil & Gas (OGRA)
- Look at standards & best-practices (quality & security)

Actions To Raise Management Support

c. Evaluate the security posture

- Evaluate security posture against each of the four layers of Transformation Model
- Any recent incidents ?
- Org culture ?
- Quality and improvement emphasis ?

Actions To Raise Management Support

d. Assess the extent of work and resources required

- Size of organization and size of IT ?
- Extent of IT assets ?
- Internal software development ?
- Evaluate team size required for InfoSec and consultant option

Actions To Raise Management Support

- e. Present your report
 - Take key stakeholders on board
 - Reach out to stakeholders before presentation
 - The better researched and prepared you are, the better your chances to convince

Actions To Raise Management Support

Conclusion:

- Many of the problems associated with weak security posture are actually due to poor awareness
- Put yourself in the shoes of your audience and explain the need for a security program from their perspective
- Keep it high level

END

Key Questions To Assess Security Posture

- What are the key questions that can be used to assess the security posture of the organization?

Key Questions To Assess Security Posture

SN	QUESTION	PTS
1	DESIGNATED HEAD OF INFORMATION SECURITY ?	30
2	INFORMATION SECURITY POLICY (AVAILABLE ON PORTAL) ?	20
3	INTERNAL VULNERABILITY MANAGEMENT PROGRAM (INTERNAL TOOL WITH MIN QTR SCANS)?	50
4	EXTERNAL PENETRATION TEST CONDUCTED MIN ONCE PER YEAR ?	50
5	IT ASSETS HARDENED WITH CIS/DISA OR OTHER INDUSTRY BEST-PRACTICE ?	100

Key Questions To Assess Security Posture

SN	QUESTION	PTS
6	ESTABLISHED INTERNAL PROCESSES FOR CHANGE MANAGEMENT, INCIDENT MANAGEMENT, CAPACITY PLANNING?	25
7	IS INFOSEC TEAM SIZE MIN 15% OF IT TEAM ?	25
8	DO YOU HAVE OPERATIONAL DR SITE ?	50
9	ALL SYSTEMS HAVE LICENSED OS ?	50
10	IS ACTIVE DIRECTORY AND LICENSED AV RUNNING ON ALL WORKSTATIONS ?	50

Key Questions To Assess Security Posture

SN	QUESTION	PTS
11	DOES NETWORK PERFORM FILTERING FOR WEB, AND ANTI-SPAM AT EDGE ?	20
12	FILTER TRAFFIC AT DATA CENTER SWITCH BASED ON ACCESS LIST ?	20
13	EDGE FIREWALL AND DMZ PRESENT ?	20
14	REGULAR BACKUPS OFFSITE AND PERFORM DR DRILL ON 2X YEAR BASIS ?	20
15	DOES MANAGEMENT REVIEW INFOSEC ON A QUARTERLY BASIS ?	20
	TOTAL	500

Key Questions To Assess Security Posture

SCORE RANGE	POSTURE	RECCOMENDED ACTIONS
LESS THAN 20%	SEVERE RISK	INFORMATION SECURITY TRANSFORMATION PROGRAM
20% TO 35%	HIGH RISK	INFORMATION SECURITY TRANSFORMATION PROGRAM
35% TO 50%	MEDIUM RISK	INFORMATION SECURITY TRANSFORMATION PROGRAM

Key Questions To Assess Security Posture

SCORE RANGE	POSTURE	RECCOMENDED ACTIONS
50% TO 70%	FURTHER IMPROVEMENTS REQUIRED	THIRD-PARTY SECURITY REVIEW
70% TO 85%	SATISFACTORY	THIRD-PARTY SECURITY REVIEW
HIGHER THAN 85%	VERY GOOD !	GO FOR ISO@7001:2013 CERTIFICATION !

Key Questions To Assess Security Posture

- By evaluating the security posture and comparing with a few other organizations (through a limited survey), the security posture can be portrayed in a quantitative manner
- The questions can be refined and customized for your organization

END

Key Leadership Qualities Of InfoSec Head

- Lets examine the key leadership qualities of the Information Security Head or the key resource driving the Security Transformation Program

Key Leadership Qualities Of InfoSec Head

- Authenticity
- Candidness
- Fairness & fair play
- Team environment
- Recognizing talent and hard work
- Celebrating success !

Key Leadership Qualities Of InfoSec Head

- Authenticity
 - IT is complex
 - No one person “knows-it-all”
 - Communicate that each individual has limitations
 - Admit mistakes and failures
 - Give credit where it is due

Key Leadership Qualities Of InfoSec Head

- Candidness:
 - Call a spade a spade
 - Honesty and straight-talk
 - Hear feedback and give respect to views of everyone

Key Leadership Qualities Of InfoSec Head

- Fairness & Fair Play:
 - Promote performance and merit
 - Adjust players in the right positions based on their strengths
 - Coach and guide team to perform and achieve results

Key Leadership Qualities Of InfoSec Head

- Team Environment:
 - Discourage solo-flight and promote team consensus, team reviews, and team achievements
 - Single out and coach individuals playing turf tactics

Key Leadership Qualities Of InfoSec Head

- Recognize Talent & Hard Work:
 - Identify self-promotion versus talent combined with hard work
 - Encourage hard workers who are team players

Key Leadership Qualities Of InfoSec Head

- Celebrate Success !
 - Hold team celebrations
 - Recognize quiet workers and background workers as well
 - Promote team achievements

END

COURSE WRAP UP

- **CONGRATULATIONS
ON REACHING THE
END OF THE COURSE !**

COURSE WRAP UP

CHAPTER 1: INTRO TO INFORMATION SECURITY

- Some basic terms and introduction to concepts
- Status of Information Security in Pakistan

COURSE WRAP UP

CHAPTER 2: TYPICAL ENTERPRISE IT ARCHITECTURE AND SECURITY OVERLAY

- What does IT enterprise topology look like ?
- Security tools overlay
- Structure of It teams and security roles in an enterprise

COURSE WRAP UP

CHAPTER 3: SECURITY TRANSFORMATION STAGE 1: SECURITY HARDENING

- Description of security hardening
- Security hardening case studies for a variety of IT assets through CIS benchmarks and DISA STIGs

COURSE WRAP UP

CHAPTER 4: SECURITY TRANSFORMATION STAGE 2: VULNERABILITY MANAGEMENT

- VM description and introduction
- VM demos (Qualys) & Other tools
- VM program best-practices

COURSE WRAP UP

CHAPTER 5: SECURITY TRANSFORMATION STAGE 3: SECURITY ENGINEERING

- Description of Security Engineering
- CIS 20 Critical Controls

COURSE WRAP UP

CHAPTER 6: SECURITY TRANSFORMATION STAGE 4: SECURITY GOVERNANCE

- Security governance introduction
- Different governance frameworks
- ISO27001:2013 (ISMS) appendix controls
- Cyber Security Maturity Matrix (CSMM)

COURSE WRAP UP

CHAPTER 7: SECURITY TESTING & VALIDATION

- Security assessments and validation description
- Security accreditation
- Software security testing & validation
- Stages of a third-party penetration test

COURSE WRAP UP

CHAPTER 8: SUCCESSFUL SECURITY TRANSFORMATION

- Security Transformation key success factors
- Security Transformation timeline
- Security Transformation benefits

COURSE WRAP UP

**BECOME A SECURITY
TRANSFORMATION
CHAMPION !**

Nahil.mahmood@gmail.com

nahil@deltatechglobal.net

Nahil Mahmood