Module: 2
What is information Security?

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

IT Security is information security applied to technology.

Information security also covers physical security, human resource security, legal & compliance, organizational, and process related aspects.

IT Security functions:

- Network security
- Systems security
- Application & database security
- Mobile security

InfoSec functions:

- Governance
- Policies & procedures
- Risk management
- Performance reviews

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

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

Module:3
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.

- 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

Recent Cyber Attack – May 2017


NHS

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

REF: TELEGRAPH

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

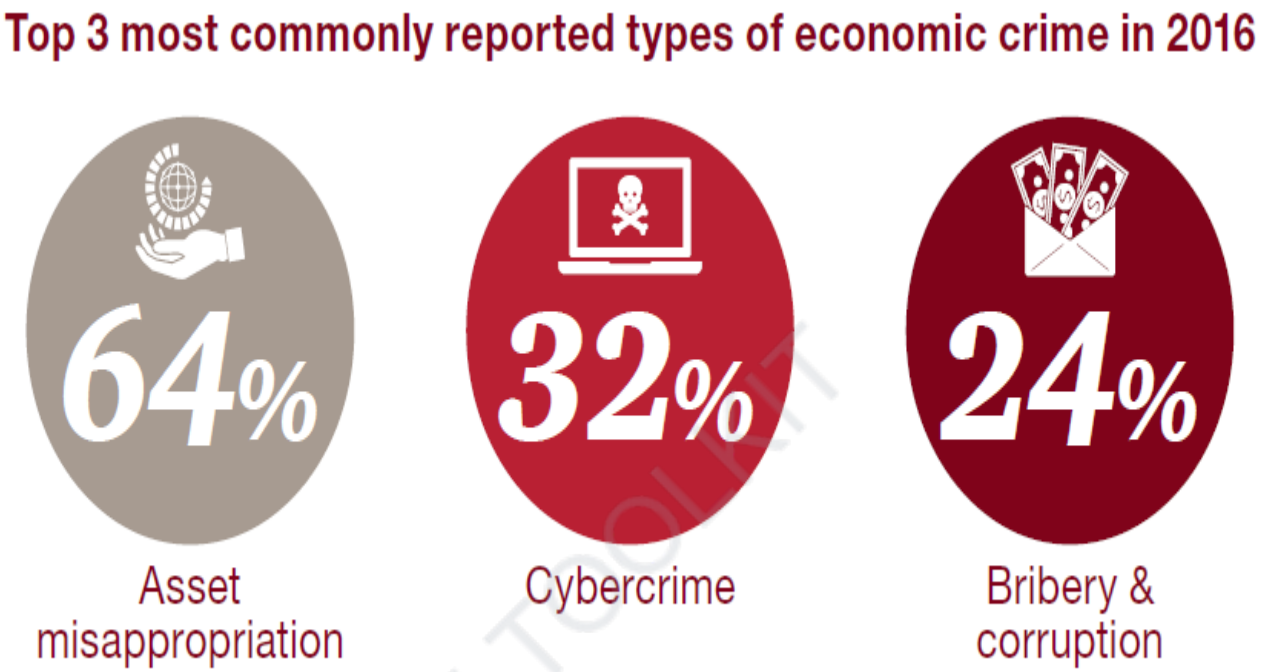
REF: GUARDIAN

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

IMPORTANCE OF INFORMATION SECURITY



- 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

Module:4
Who is information security for?

Personal:

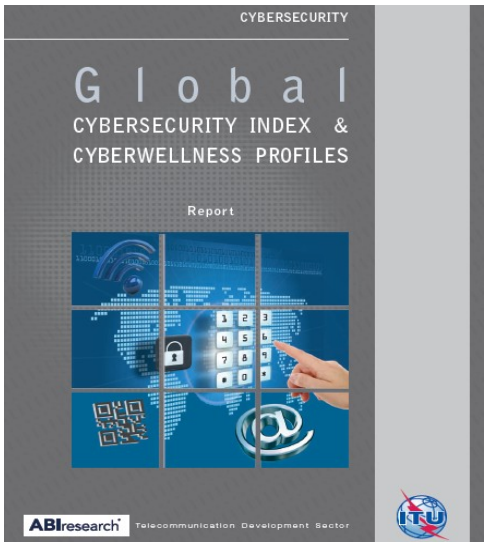
- Social media passwords and safe usage
- Online banking and email account passwords
- Home PC/laptop security
- Mobile security

Organizational:

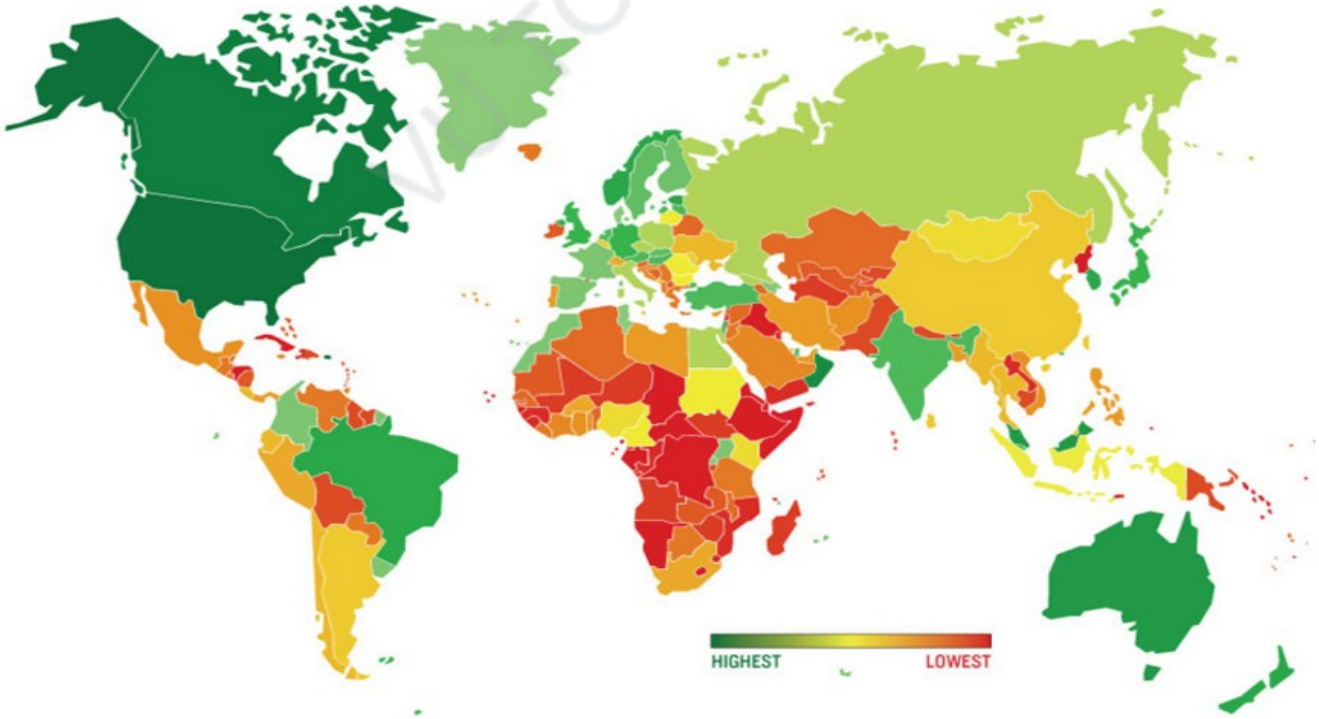
- Board and executive leadership (management commitment)
- CISO (responsible to drive security program)
- IT staff and business users (following information security policies & procedures)

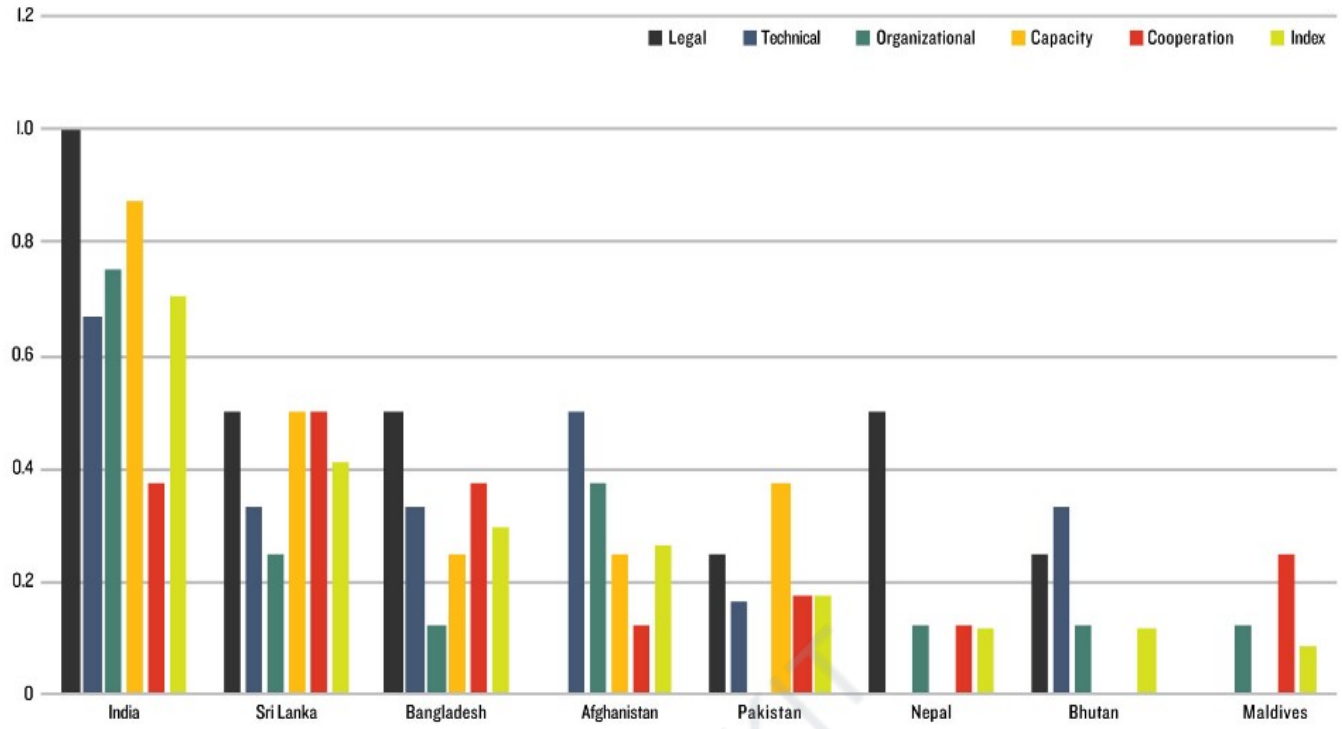
Govt and national:

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



- Legal
- Technical
- Organizational
- Capacity building
- Cooperation





Source: ABI Research, ITU, Global Security Index

- 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

Module:5
How is information security implemented?

Three pillars of information security:

- People
- Process
- Technology

Leadership commitment:

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

Information Security Manager or CISO:

- Heads department responsible for implementing information security program
- Directs planning, implementation, measurement, review, and continual improvement of program

IT user:

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

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

Information security program

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

Module:6
Who are the players of information security?

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

Government:

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

Industry & sectors:

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

International organizations:

- APCERT (www.apcert.org)
- European Union Agency for Network & Information Security - ENISA (www.enisa.org)
- ITU IMPACT (http://www.impact-alliance.org)

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

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/

Academia & research organizations:

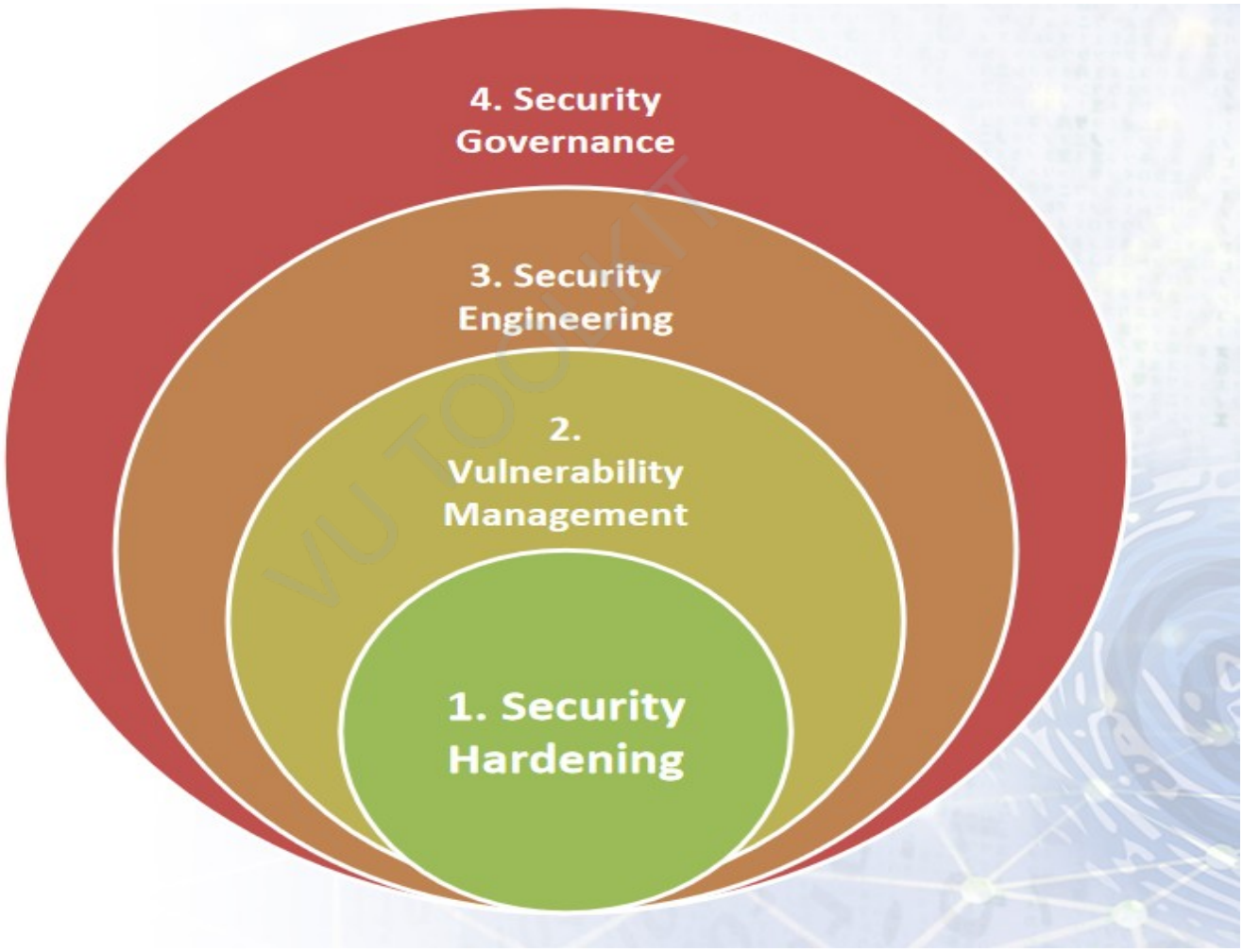
- Universities and research programs
- SANS (www.sans.org)
- Center for Internet Security (www.cisecurity.org)

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

Module:7

What are the four layers of information security transformation framework?

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



1: Security hardening:

- Compile IT assets
- Establish minimum security baseline (MSB)
- Research security controls and benchmarks

- Pilot (test)
- Implement controls
- Monitor and update controls

2: Vulnerability management:

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

3: Security engineering:

- Assess risk profile
- Research security solutions
- Design security architecture
- Implement security controls & solutions
- Test and validate security posture

4: Security governance:

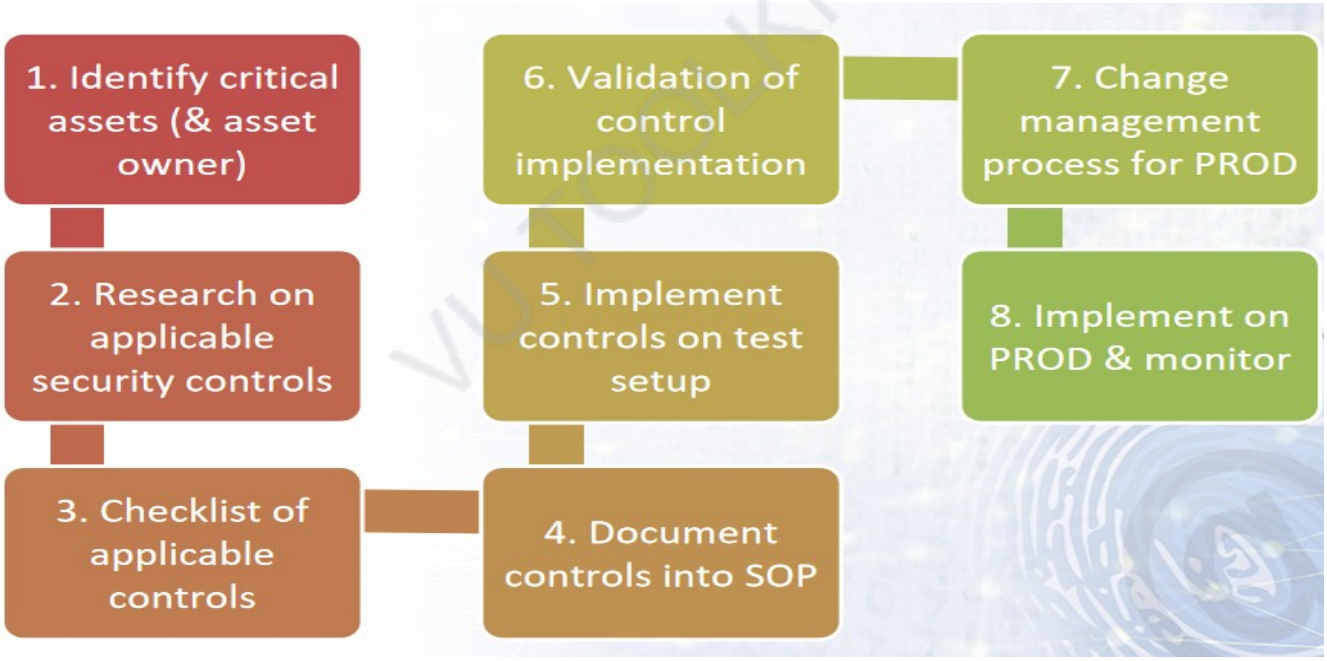
- Policies and procedures
- Risk management
- Core governance activities (change management, incident management, internal audit)
- Training & awareness
- Performance reviews

Modules:8
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

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



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

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

Module:9
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

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, ensuring that objectives are achieved, ascertaining that risks are managed appropriately and verifying that the enterprise's resources are used responsibly."

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

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

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

Module:10
What is the difference between an information security policy, SOP, and guideline?

Policy:

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

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

Policy:

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

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

Guideline:

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

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

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

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)

Examples:

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

Module: 11
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

Program definition:

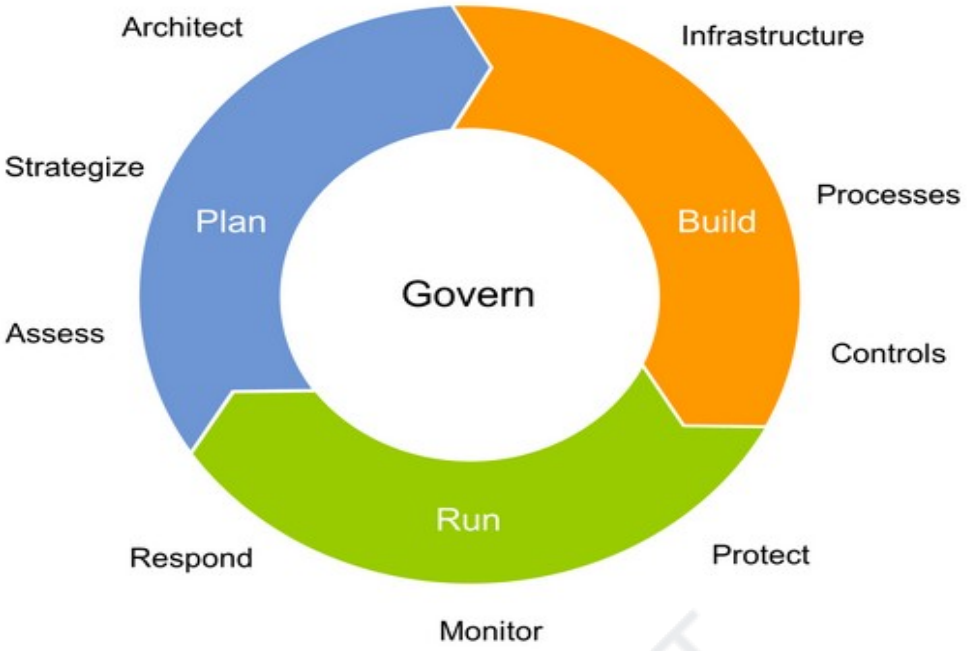
A program is defined as a group of related projects managed in a coordinated way to obtain benefits not available from managing the projects individually.

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

Security program:

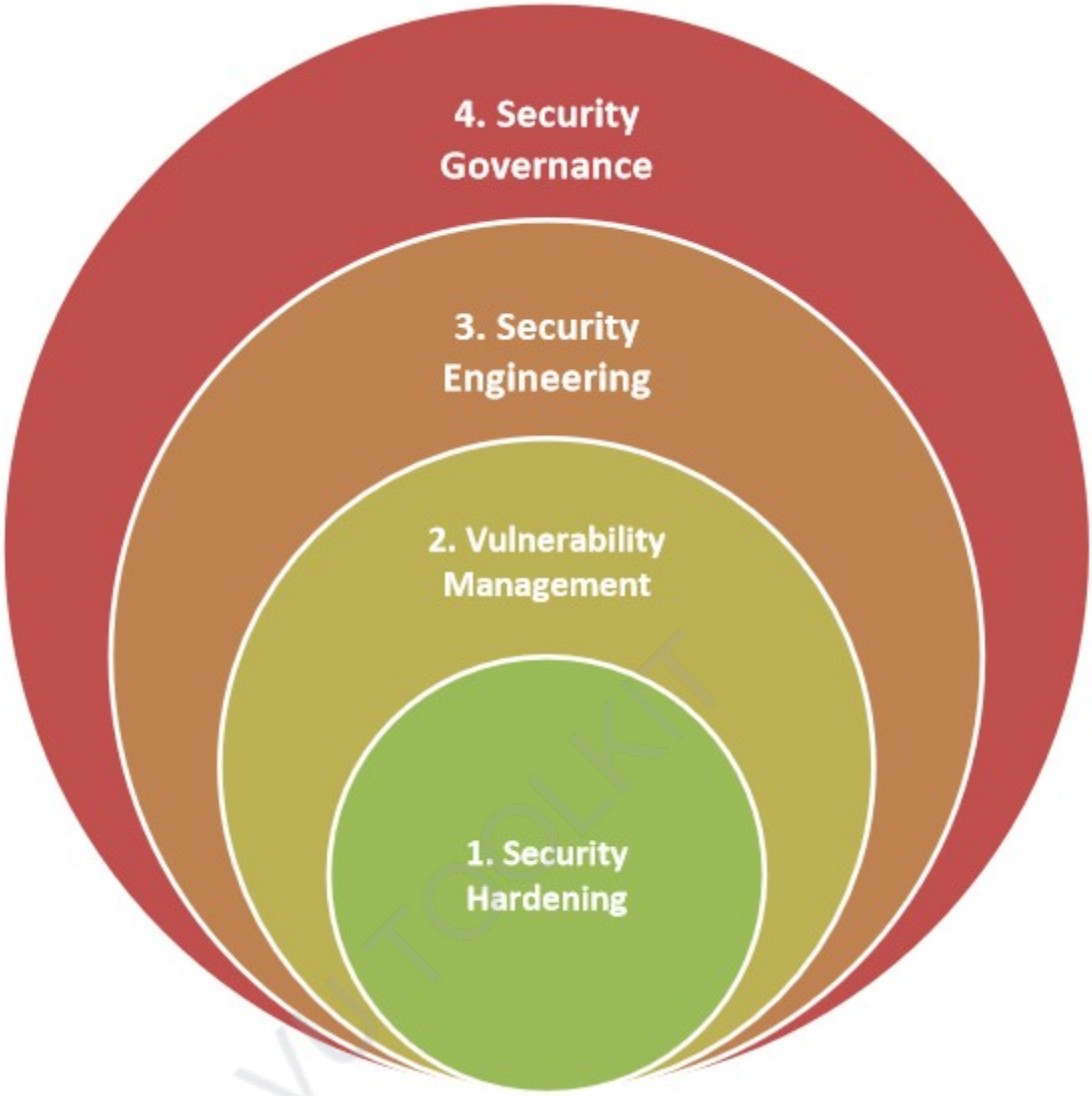
Sum-total of all activities planned and executed by the organization to meet its security objectives.

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



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

4 Layer Security Transformation Model



- 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

Module: 12
What is the role of people, process, and technology in information security?

- 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

People:

People must be trained to effectively & correctly follow policies, information security processes, and implement technology.

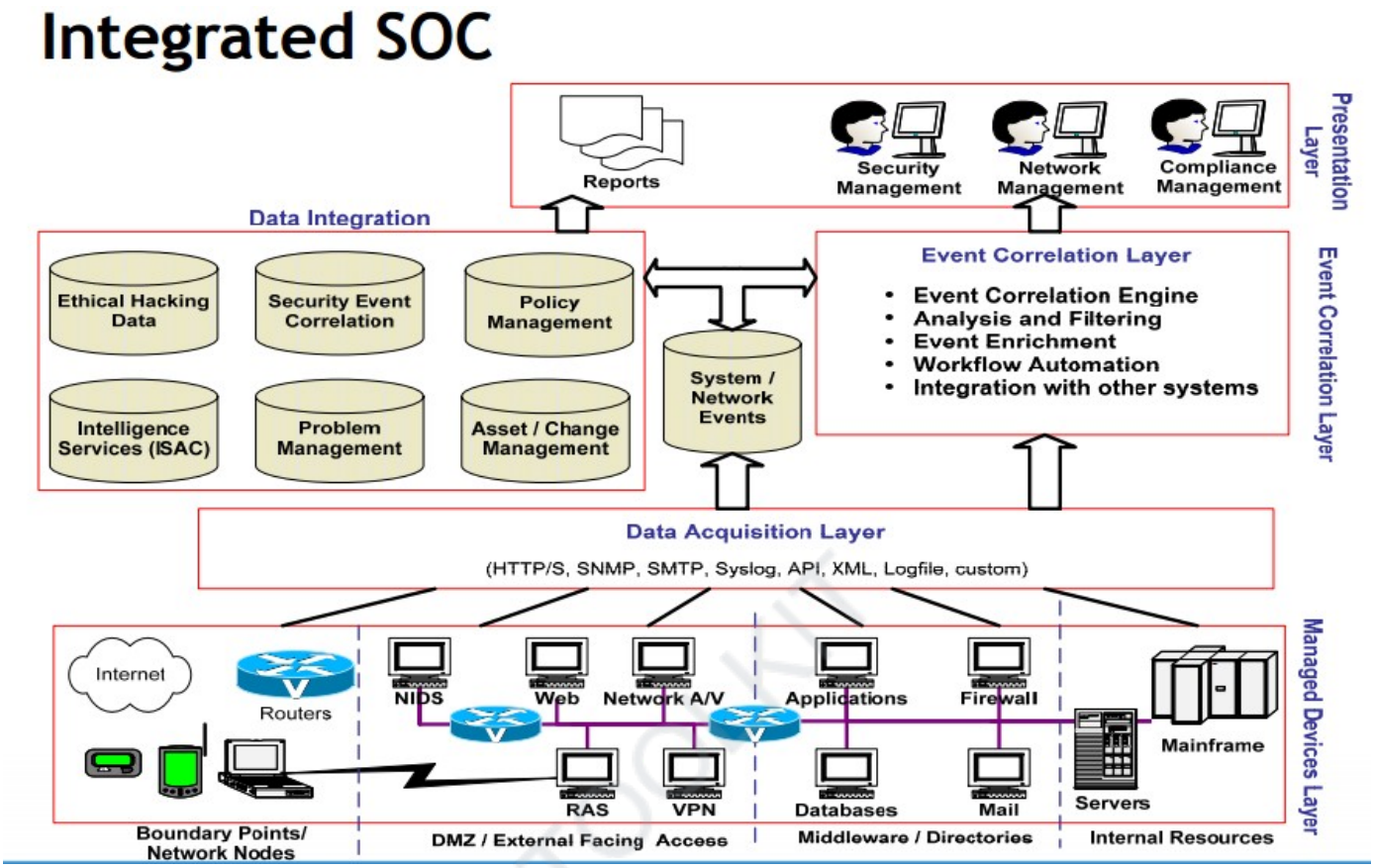
Social engineering and phishing are aspects that people must be trained to handle appropriately.

Processes are fundamental to effective information security

- User access management
- Backups
- Incident management
- Change management
- Vulnerability management
- Risk management

Technology plays a central role in the Information Security program:

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



https://www.rsaconference.com/writable/presentations/file_upload/tech-203.pdf

Module: 13
What is the role of 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.
- 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.

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

InfoSec Manager Tasks:

- Develop policy
- Training & awareness
- Design security architecture
- Design security controls
- Ensure controls are implemented

- Conduct risk assessment
- Conduct security testing
- Monitor vulnerability management program
- Facilitate incident management process
- Sign-off critical change management activities

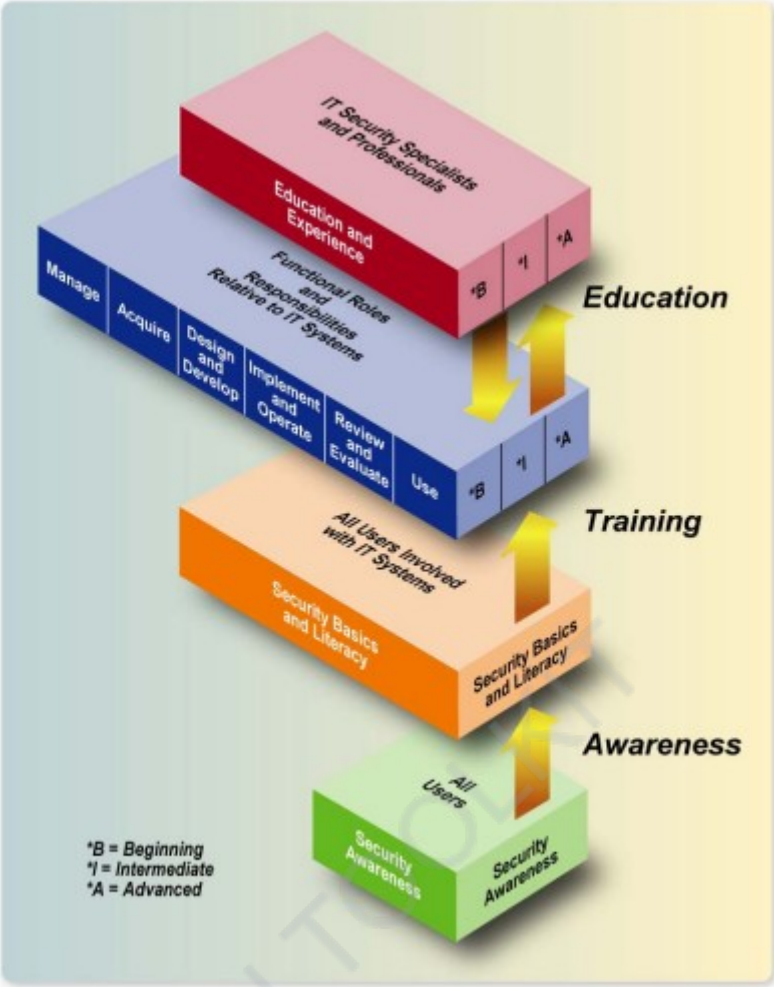
Module: 14
What is information security awareness?

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/



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

- Awareness
- Training
- Education

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

Training:

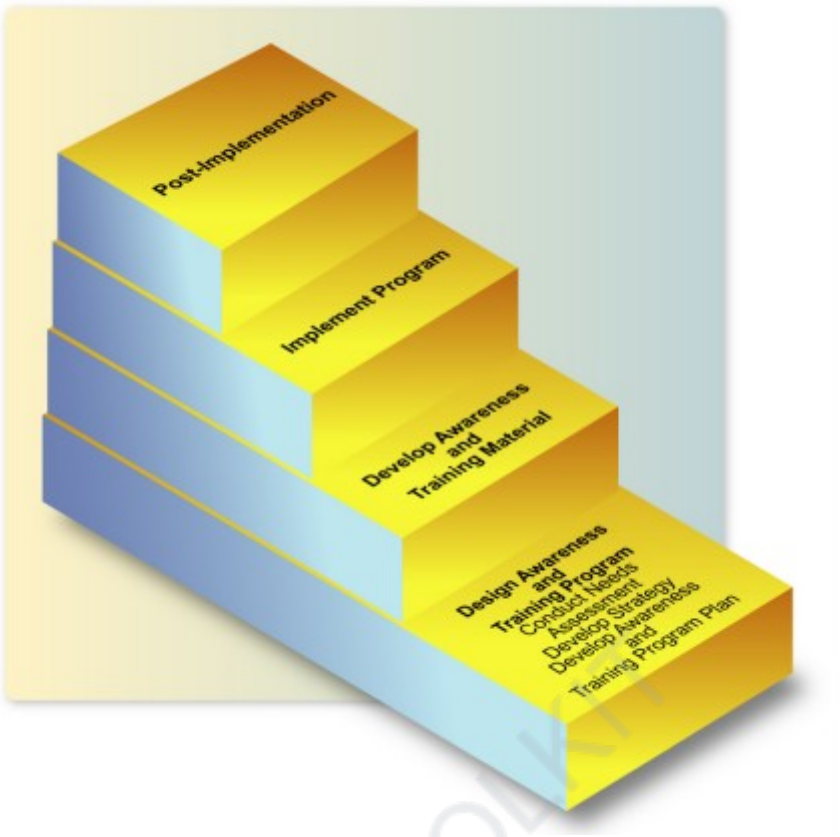
- “Strives to produce relevant and needed security skills and competencies”
- Seeks to teach skills
- E.g. IT Security course for system administrators covering all security aspects

REF: NIST SP800-50, PAGE 9

Education:

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

NIST-SP-800-50



IMPLEMENTATION STEPS

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

Module: 15
What are the leading information security standards and frameworks?

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

ISO27001:2013 (ISMS)

- Specifies the requirements for establishing, implementing, maintaining and continually improving an information security management system
- Ten short clauses
- Long annex

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

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

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

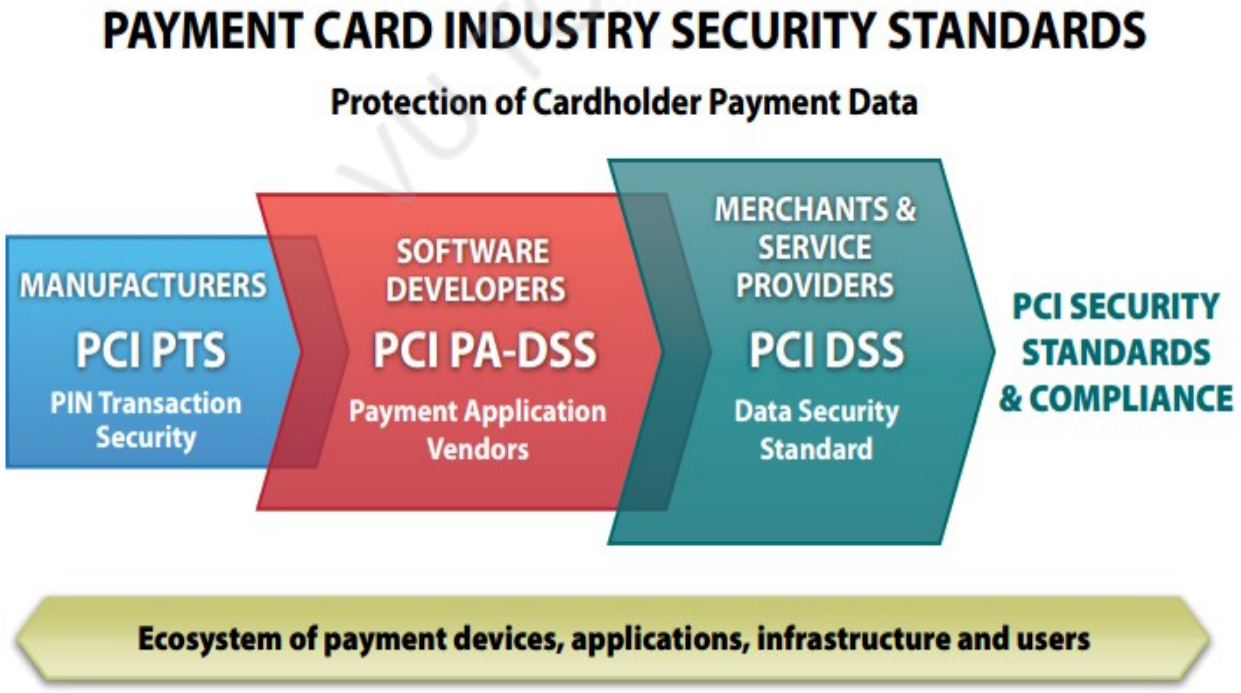
https://www.pcicomplianceguide.org/pci-faqs-2/

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/



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

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

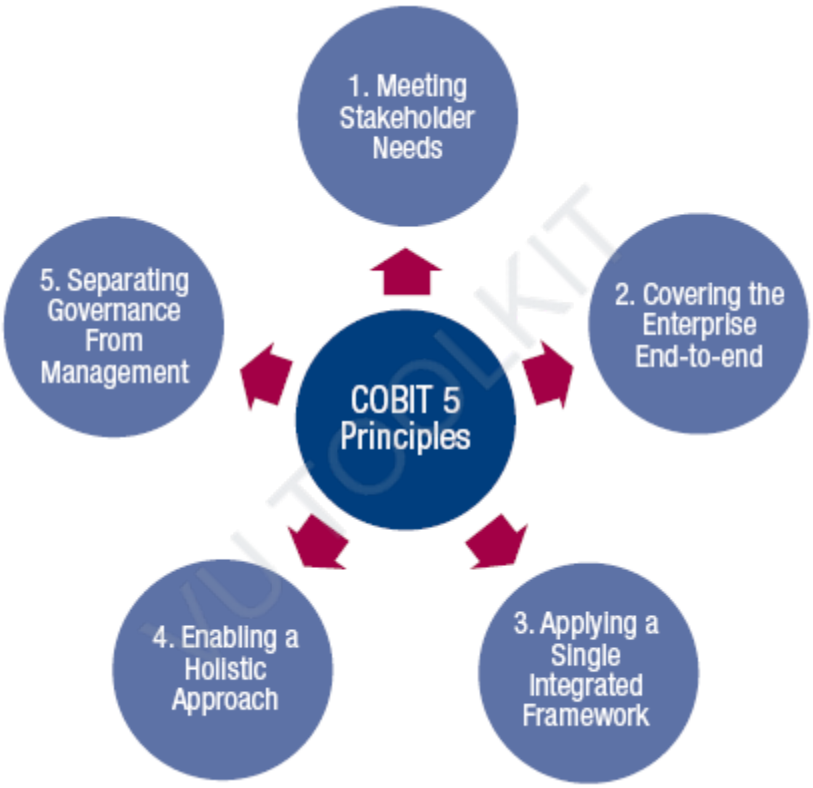
https://www.pcisecuritystandards.org/documents/PCI%20SSC%20Quick%20Reference%20Guide.pdf

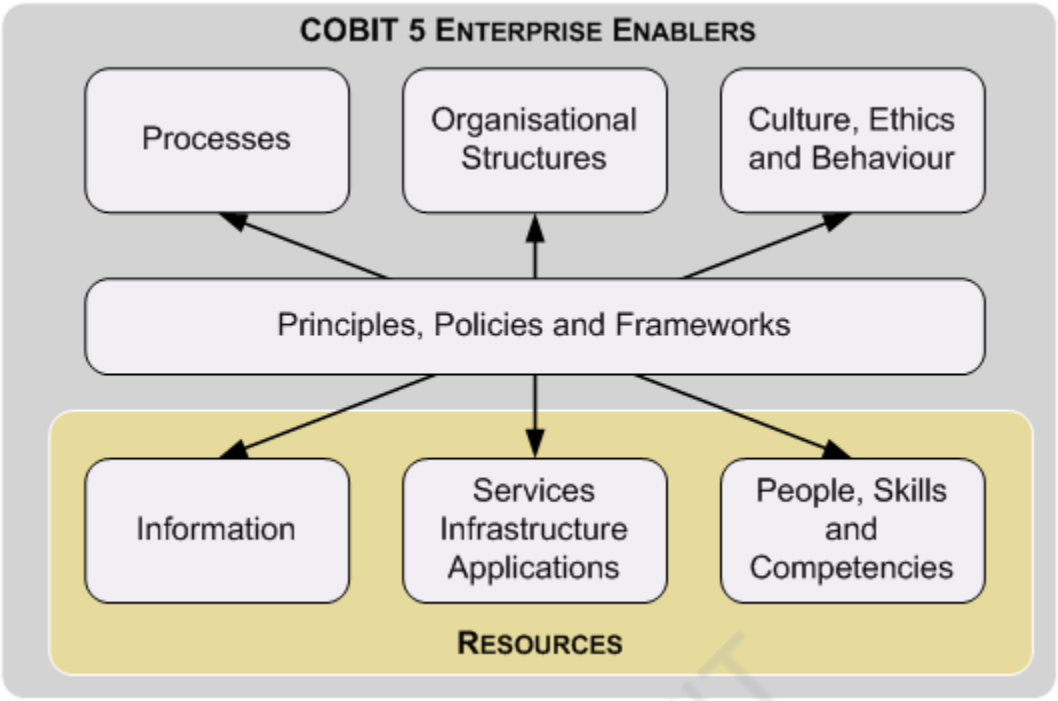
COBIT:

- ISACA framework for IT Governance
- COBIT 5 helps enterprises to create optimal value from IT by maintaining a balance between realizing benefits and optimizing risk levels and resource use (ISACA)
- 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 optimizes IT investment and use for the benefit of stakeholders (ISACA)

ISACA®

Trust in, and value from, information systems





Module: 16
What is information security risks?

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

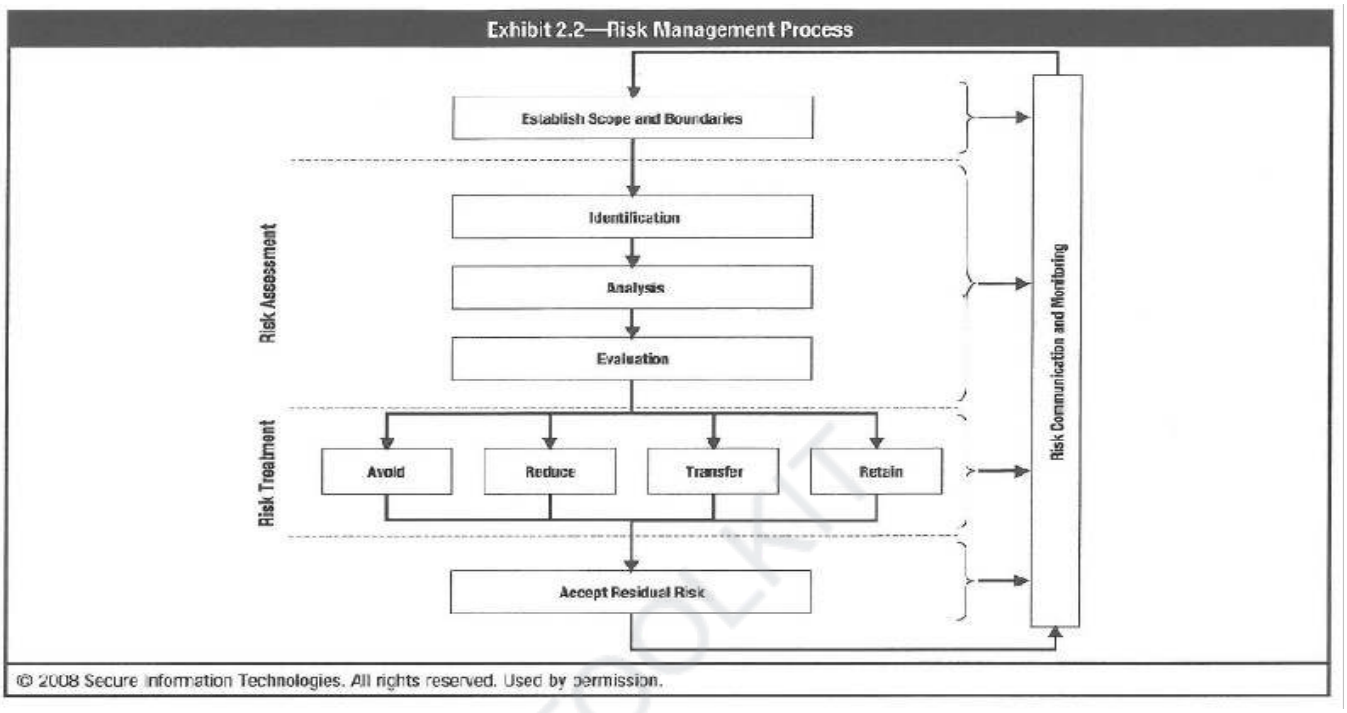
A process aimed at achieving an optimal balance between realizing opportunities for gain and minimizing vulnerabilities and loss

Usually accomplished by ensuring that impact of threats exploiting vulnerabilities is within acceptable limits at an acceptable cost

REF: ISACA CISM MANUAL

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

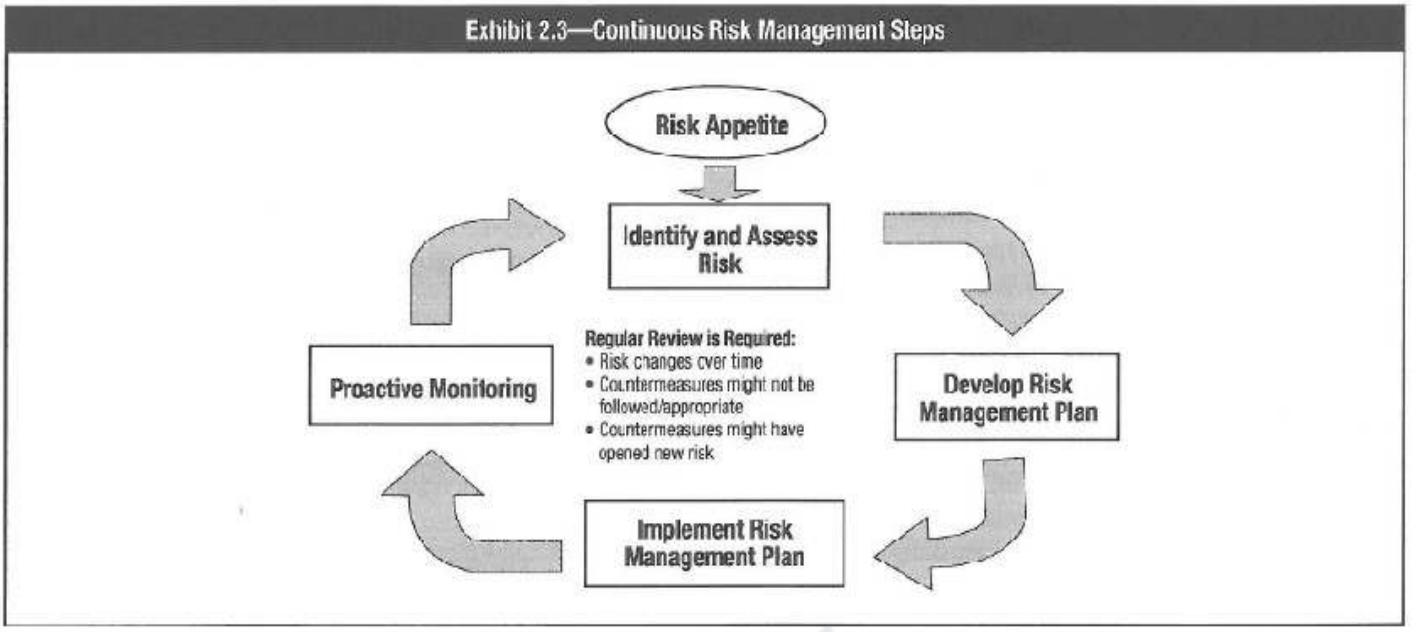


REF: ISACA CISM MANUAL

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



REF: ISACA CISM MANUAL

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

Module: 17
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

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
e. Intended outcomes are achieved
f. Directing and supporting persons
g. Promoting continual improvement
h. Supporting other management roles

“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

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

Module: 18
Whose responsibility is implementation of security?

Default organizational perception:

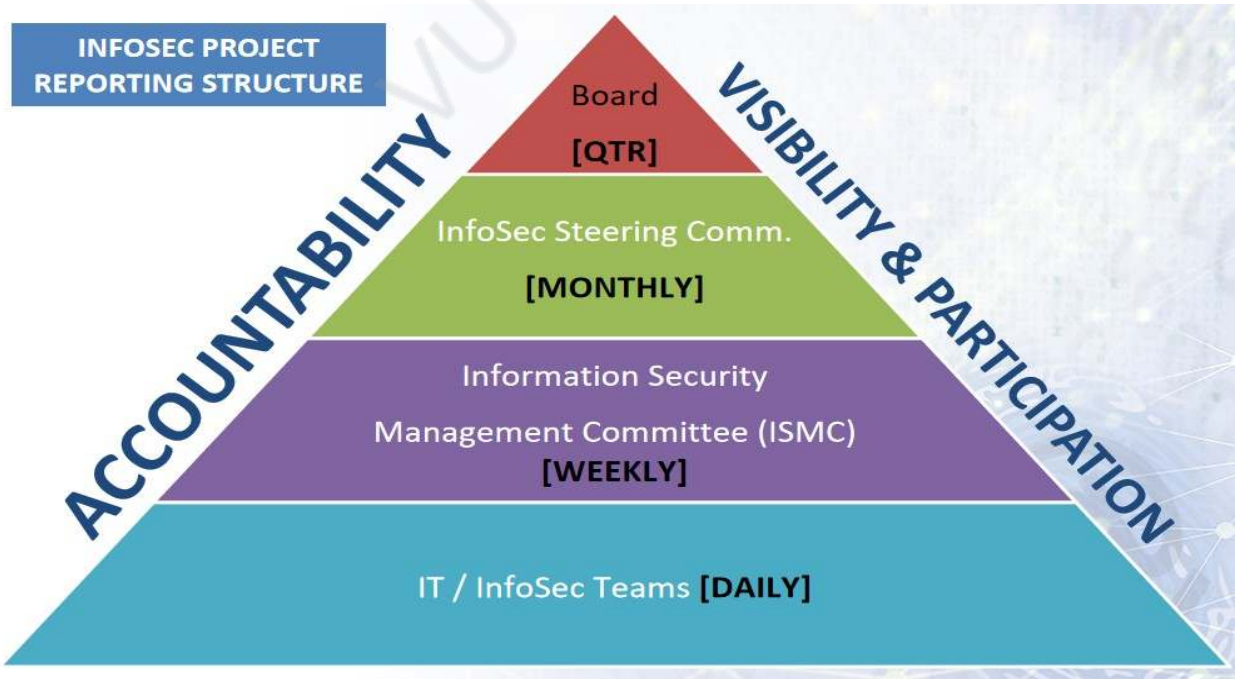
- Security is responsibility of one person or one department
- Can get away with “security as an after-thought”
- Reactive

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

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



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

Module: 19
What can happen if information security is not implemented

- Fox News Video: "World's Biggest Cyber Attacks"

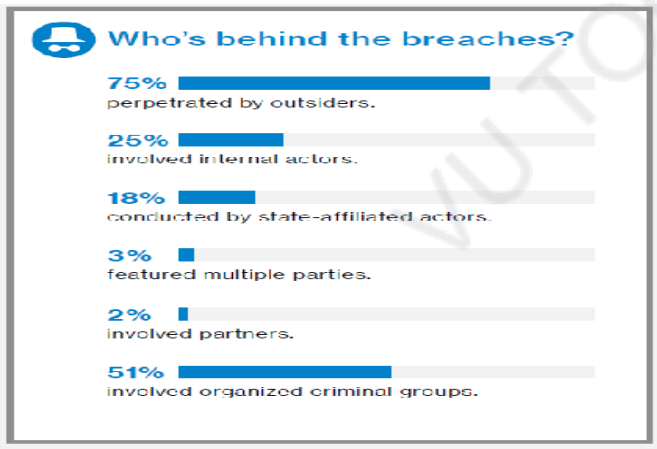
http://video.foxnews.com/v/5435057924001/?#sp=show-clips

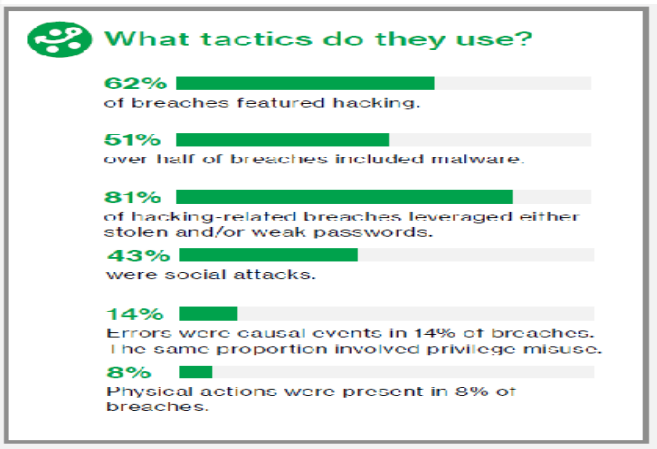
- World's Biggest Data Breaches:

http://www.informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/

Leading Global Reports:

- Verizon 2017 Data Breach Investigations Report (DBIR)
- Symantec 2017 Internet Security Threat Report (ISTR)





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.

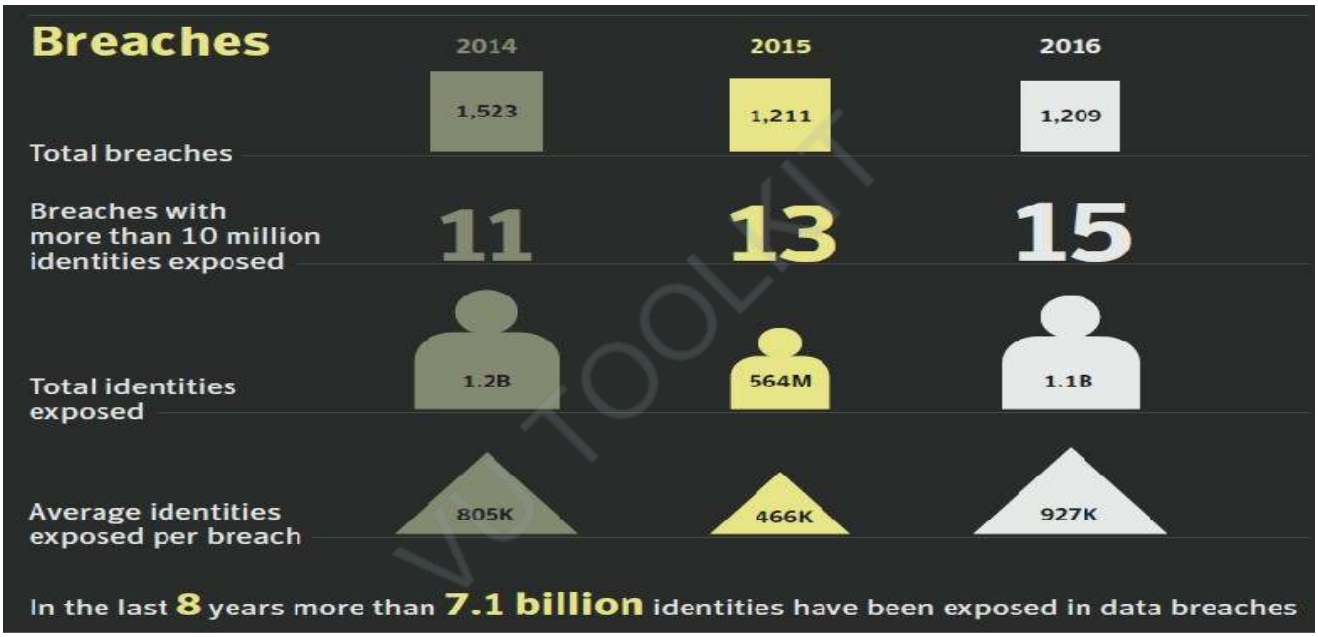
What else is common?

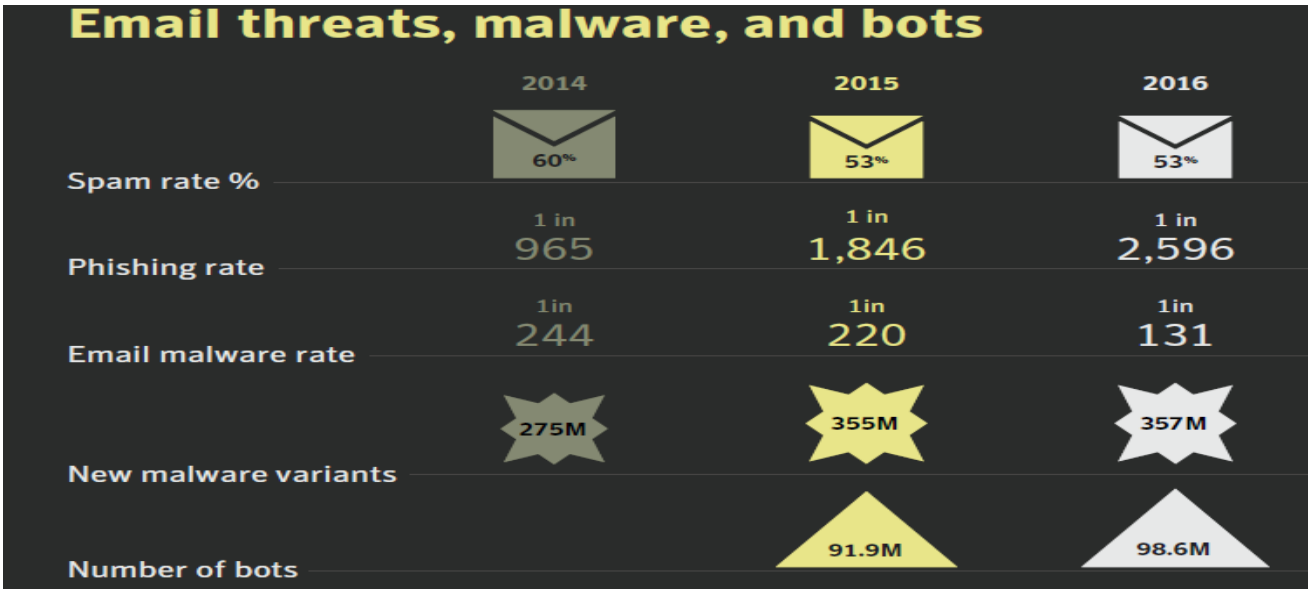
66% of malware was installed via malicious email attachments.

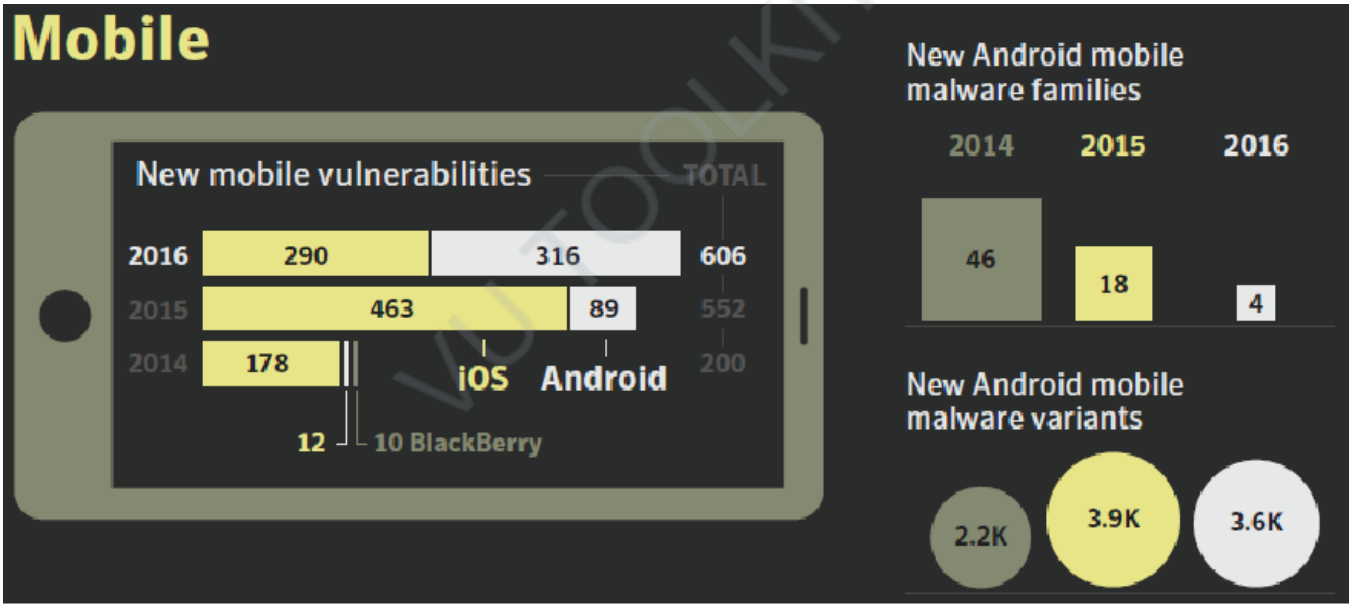
73% of breaches were financially motivated.

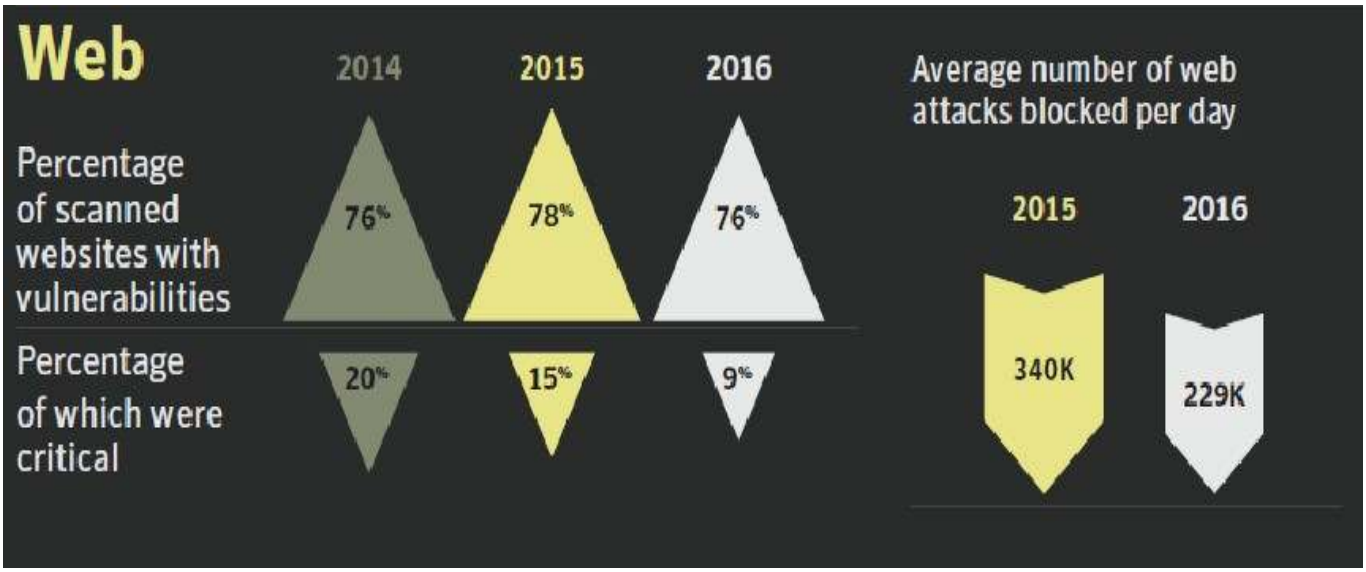
21% of breaches were related to espionage.

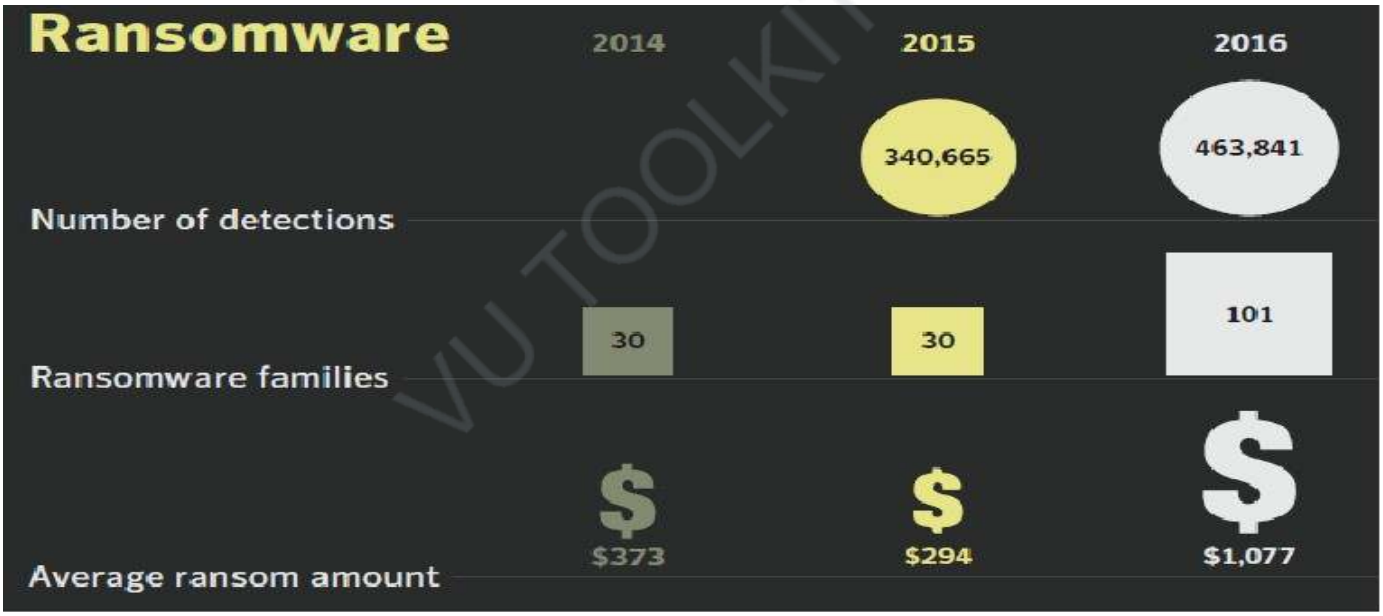
27% of breaches were discovered by third parties.







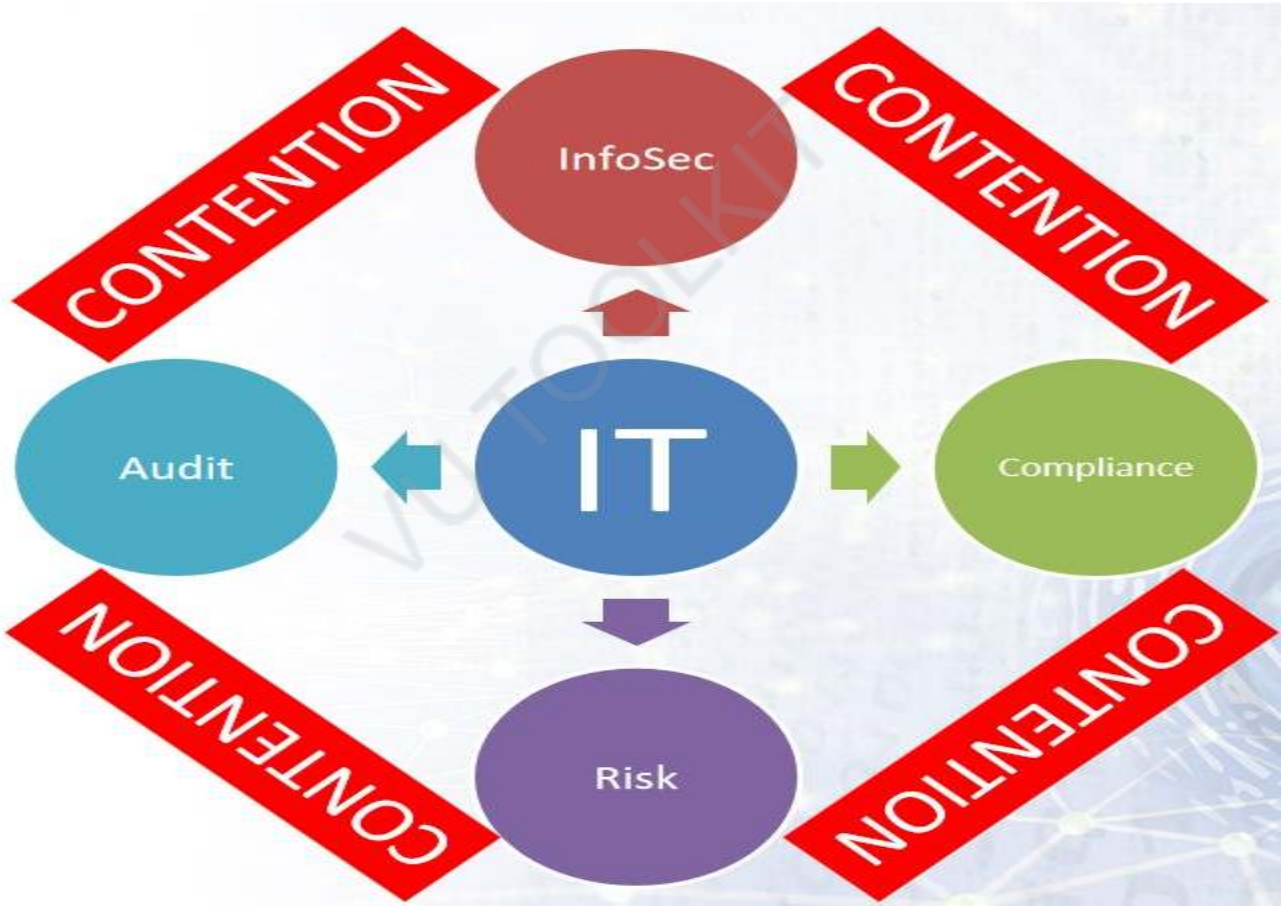




Module: 20
What are the challenges of information security implementation?

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:

- Silos & lack of coherent ownership
- Lot of time & energy wasted in traversing dept boundaries
- Enabling environment for tough security work missing

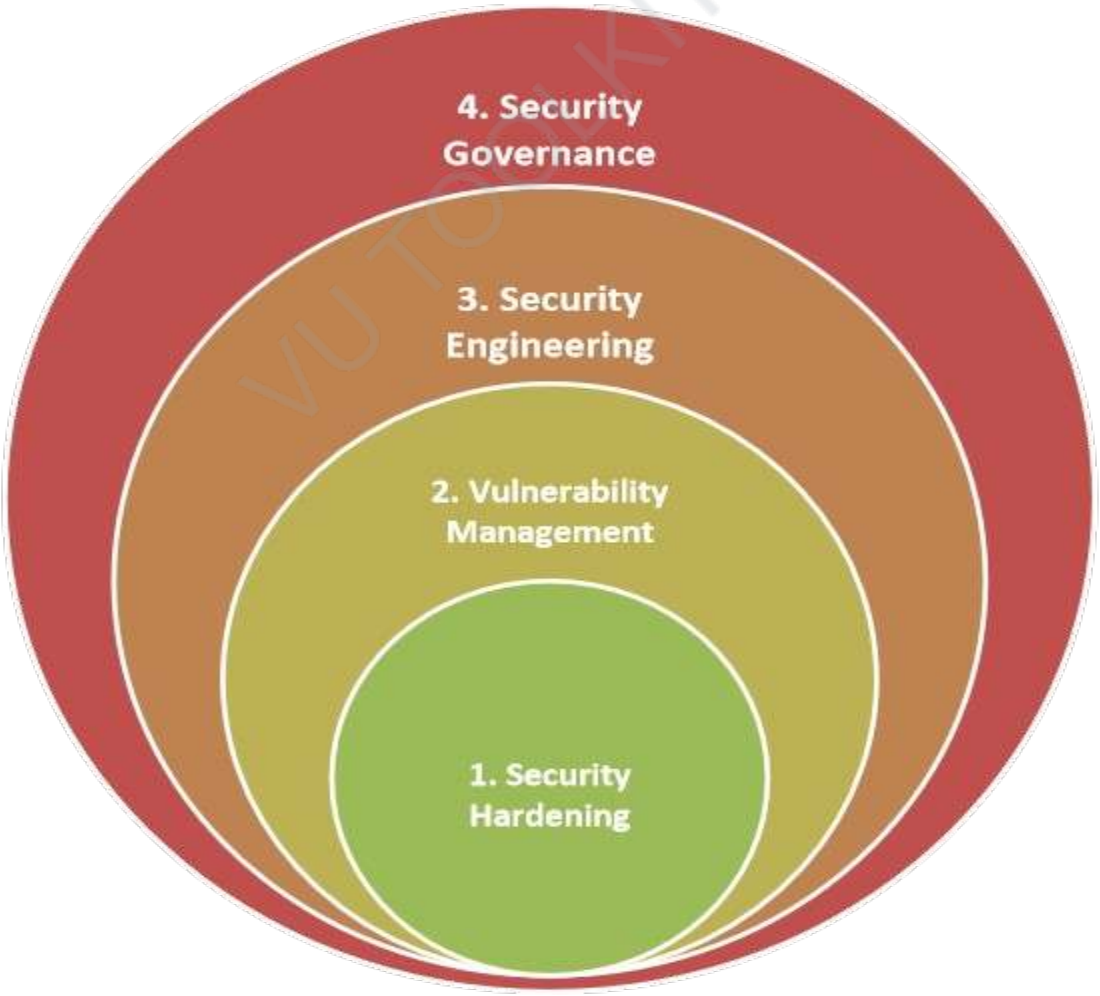
- Security hardening glaringly absent

Pakistan Industry Security Characteristics:

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

InfoSec

Transformation Model



Module: 21
What is the 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

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).

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 Regulator In Cyber Security:

- Regulations, guidelines, and audit
- Engagement of key stakeholders
- Technical and industry expertise
- Regional and international cooperation

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)

Singapore:

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

Pakistan; Ministry of IT (MOIT):

- National IT Policy 2016 (draft)
- Digital Pakistan Policy 2017

Pakistan; State Bank Of Pakistan (SBP):

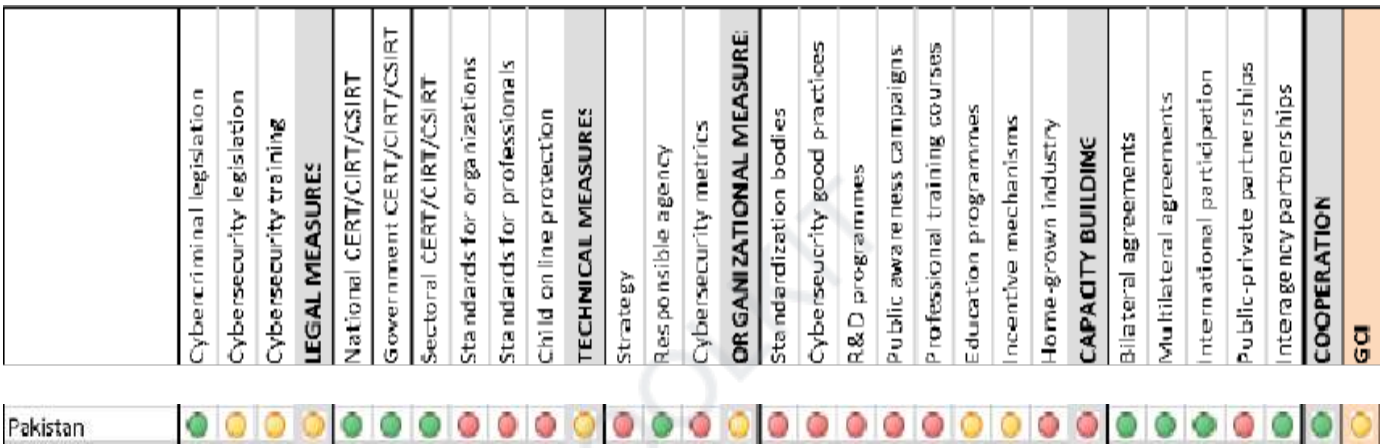
- Enterprise Technology Governance & Risk Management Framework for Financial Institutions (30 May 2017)

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)

Module: 22
What is the status of information security 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



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

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

Reasons for poor security posture:

- Archaic digitalization and commerce
- Perception that Pakistan is immune
- Lack of awareness and management commitment
- Lack of effective regulations

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

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

Module: 23
What is the solution for improvement of information security in Pakistan.

- 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

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

Solution for strong security posture:

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

Don’t repeat the same mistakes:

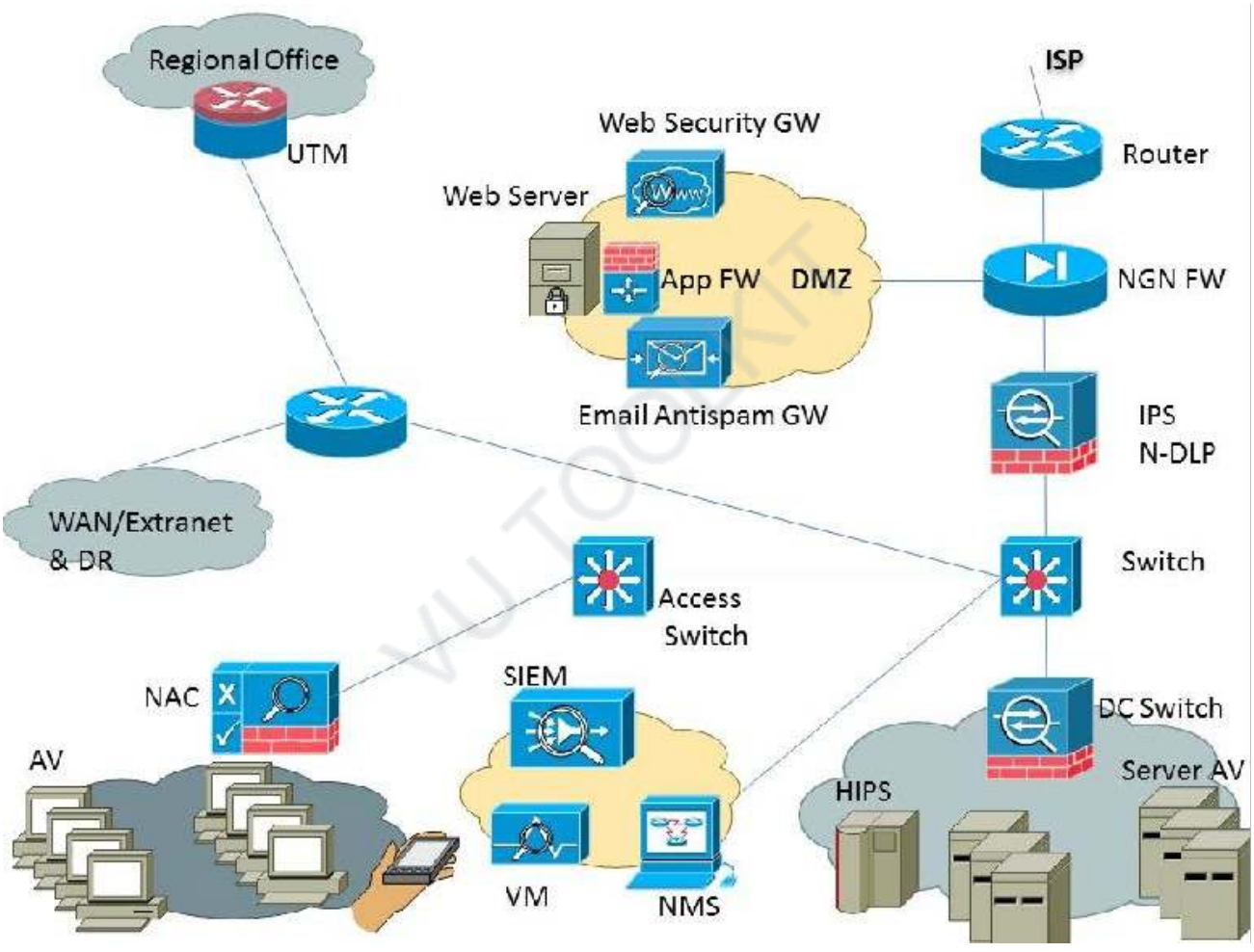
- Too much governance without the underlying security hardening
- Reactive rather than intrinsic
- Lack of resources (10% of what allocated for IT)
- Management interest

CHAPTER:2

Module: 24
What does the typical enterprise IT network look like?

Typical Enterprise IT Architecture & Security Overlay

What does a typical enterprise IT network look like?



- Edge router
- NGN FW
- DMZ:
- Web security GW/Proxy
- Application security FW
- Web server
- Email antispam GW

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

Module: 25
What are the major components of the enterprise it network?

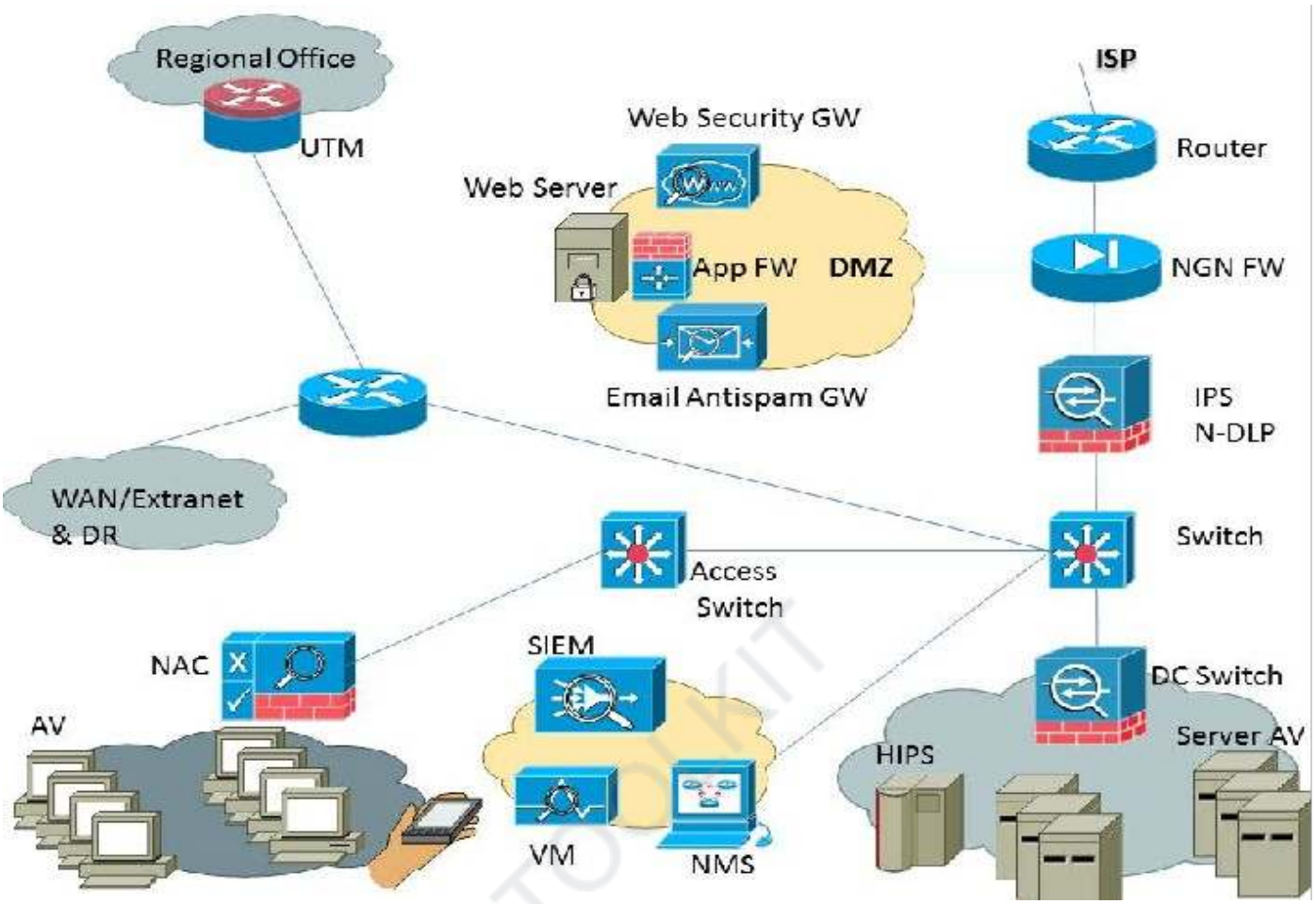
Major Components: Enterprise IT Network

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



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

Distribution switch

- Connectivity to access switches, external exit point (WAN), and DC switch

Data center switch & FW

- Data center filtering (malware & access-lists)

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

Vulnerability Manager

- Vulnerability scanning and asset tracking

System AV

- Signature based malware prevention

Server HIPS

- IPS features for servers, also file integrity checking

UTM

- Multi-featured NGN FW device

Mobile device – MDM

- Security features for mobile devices

Module: 26
What is the OSI security architecture?

OSI Security Architecture

- 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/l_01ov.pdf

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

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

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

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

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

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/l_01ov.pdf

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

Services and Mechanisms Relationship

	Mechanism							
Service	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

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

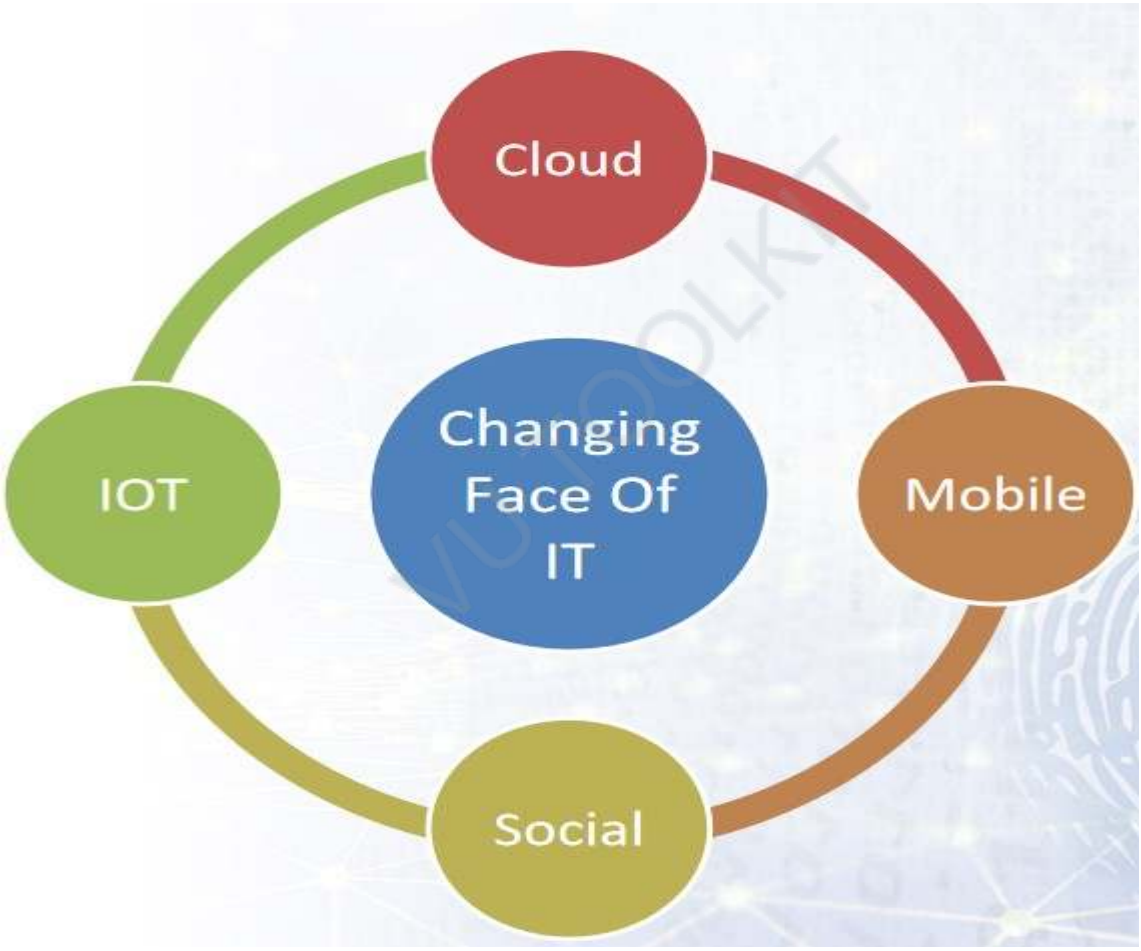
http://www.cse.wustl.edu/~jain/cse571-11/ftp/l_01ov.pdf

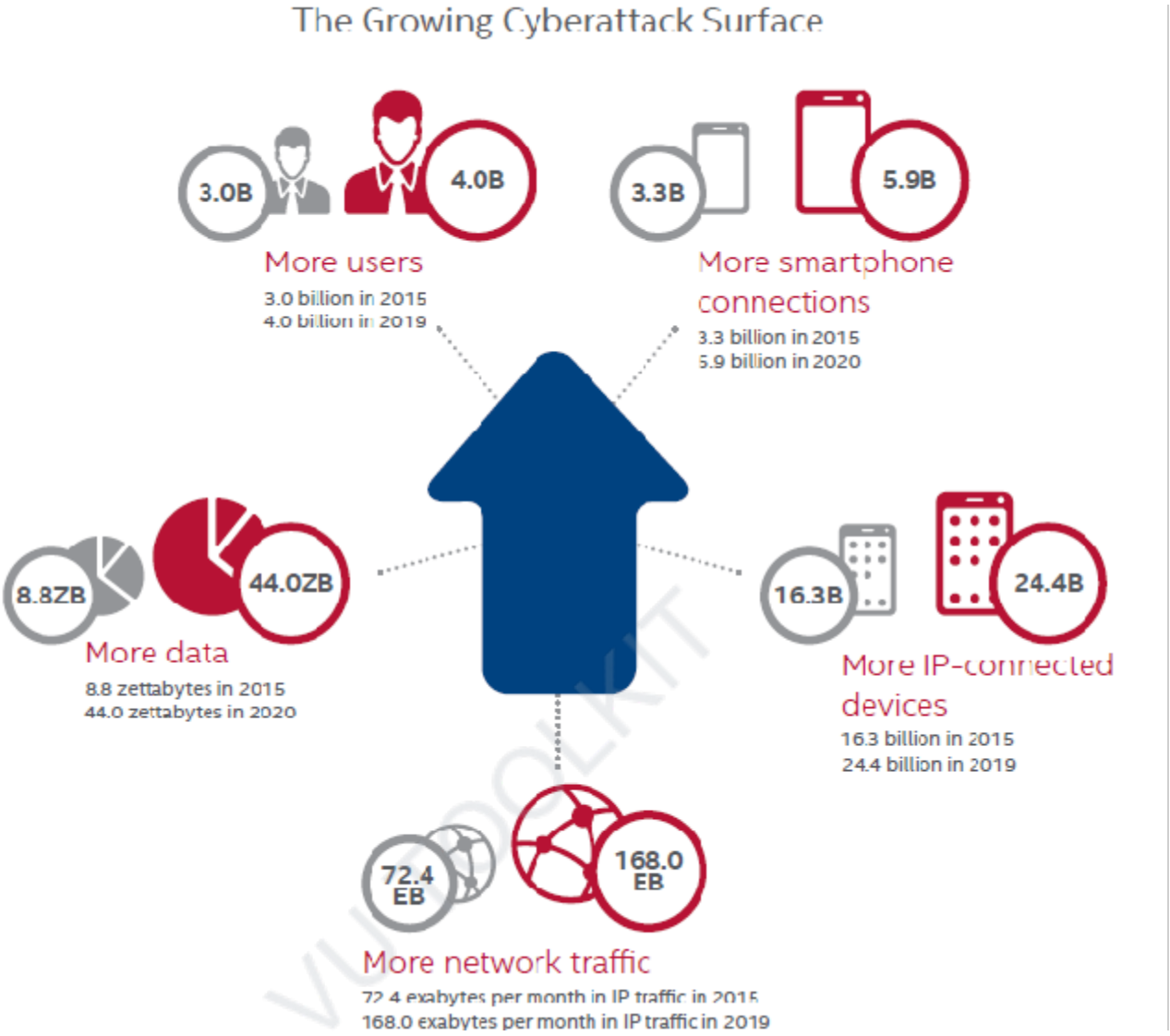
ITU-T X.800, Security Architecture for OSI is dated from 1991

Module: 27
The new frontiers of enterprise it: cloud, mobile, social, IOT

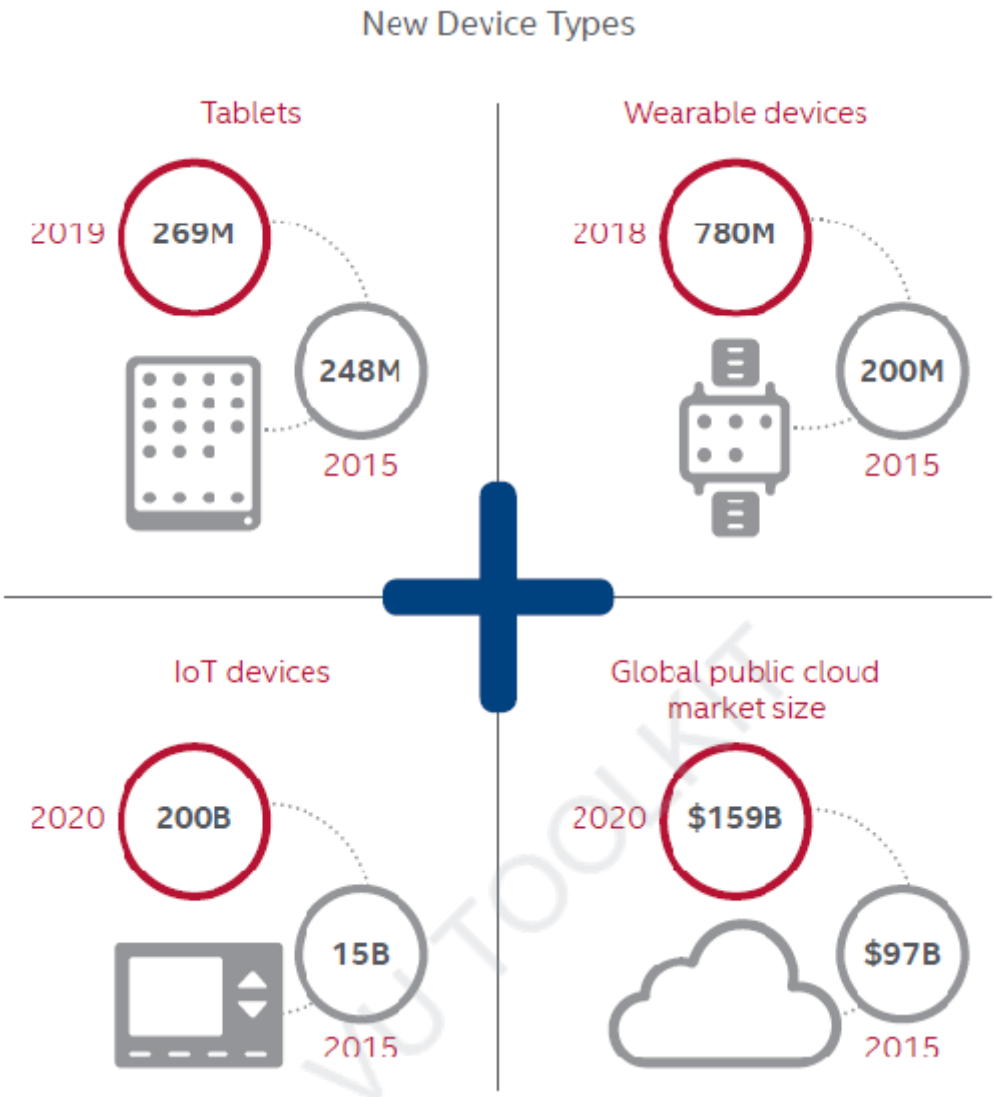
New IT Frontiers: Cloud, Mobile, Social, IOT

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

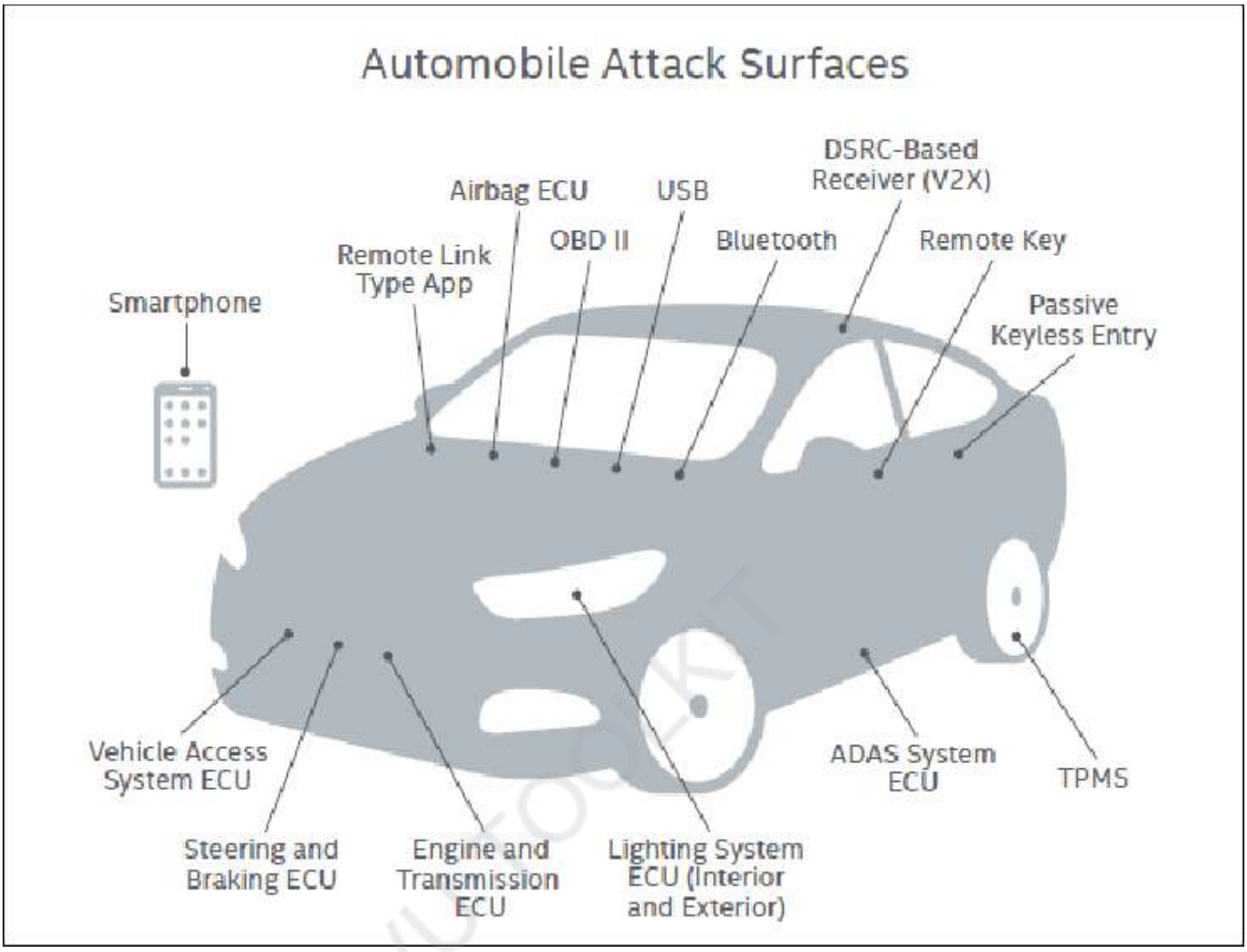




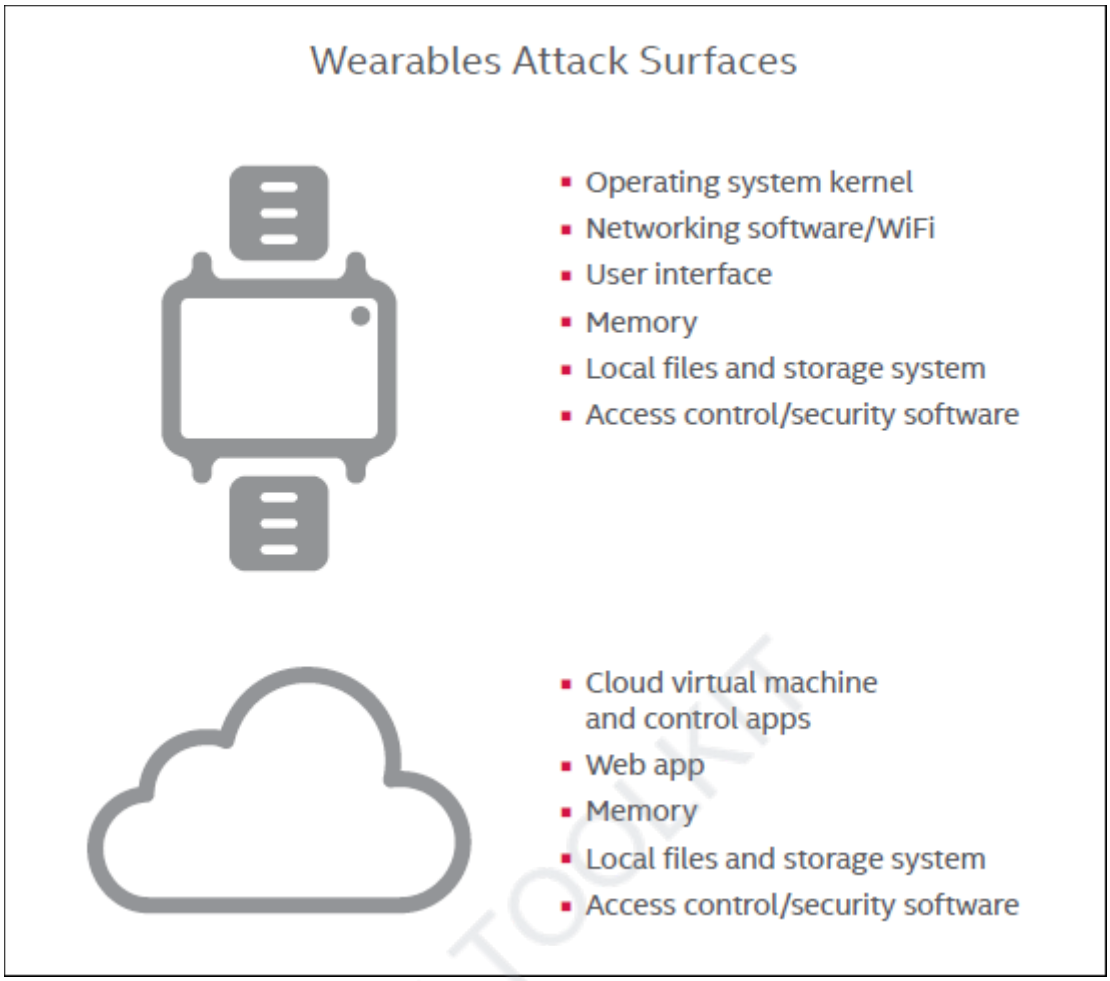
https://www.mcafee.com/us/resources/reports/rp-threats-predictions-2016.pdf



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



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



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

For cloud, mobile, and IOT security guidance, checklists, and other details visit:

- www.cloudsecurityalliance.org
- www.owasp.org

Useful URLs:

- https://www.owasp.org/index.php/OWASP_Mobile_Security_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/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/assets/research/internet-of-things/connected-vehicle-security.pdf

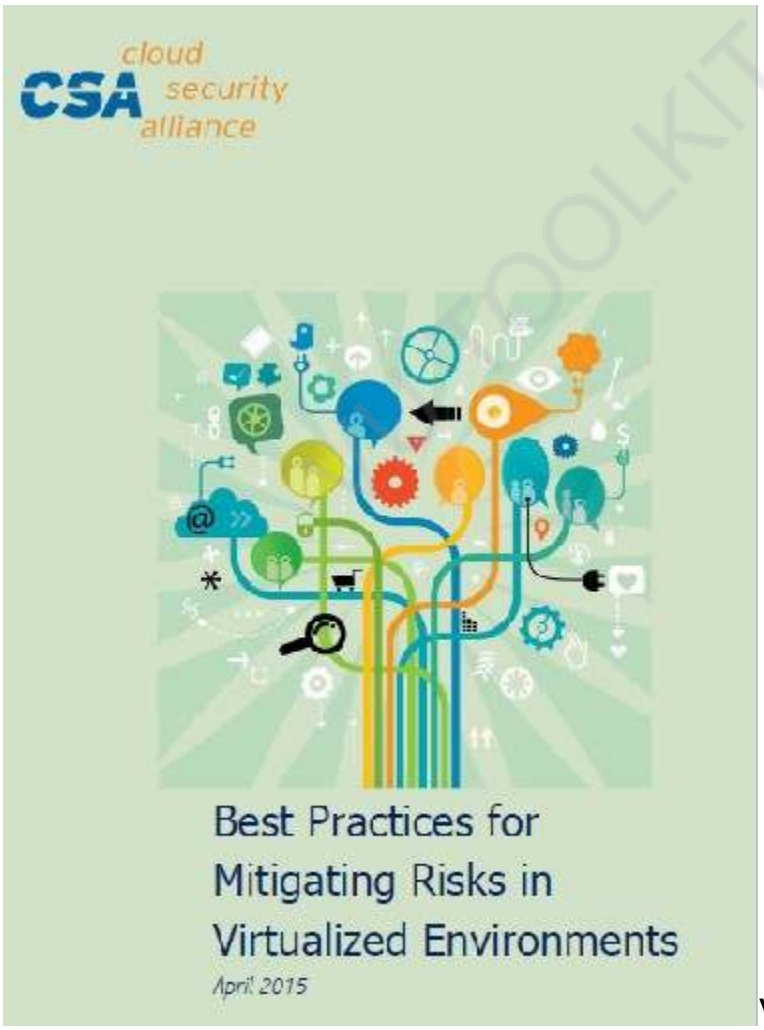
Module: 28
Virtualization and enterprise security

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

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

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
- 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
- Controls: keep a small number of identified, good and patched images of a guest operating system separately for fast recovery & restoration of systems

Risk # 2 (Sensitive Data Within a VM)

- Impact: VM images and snapshots can be copied easily via USB or console of hypervisor installed elsewhere
- 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

Module: 29
Case study of enterprise - small organization

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, Telco's, enterprises

Organizational culture:

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

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

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)

Security requirement:

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

Driving change?

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

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)

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

Module: 30
Case study of enterprise - medium sized organization

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

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

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
- 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

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)

Security requirement:

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

Driving change ?

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

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)

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

Module: 31
Case study of enterprise - large sized organization

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

Organizational culture:

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

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

Security posture:

- Superficial
- No hardening done
- Weak vulnerability management
- Poor security management/ governance
- Security team exists

- No management commitment (prior)

Security requirement:

- Security incident; servers hacked causing financial loss

Driving change?

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

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)

Conclusion:

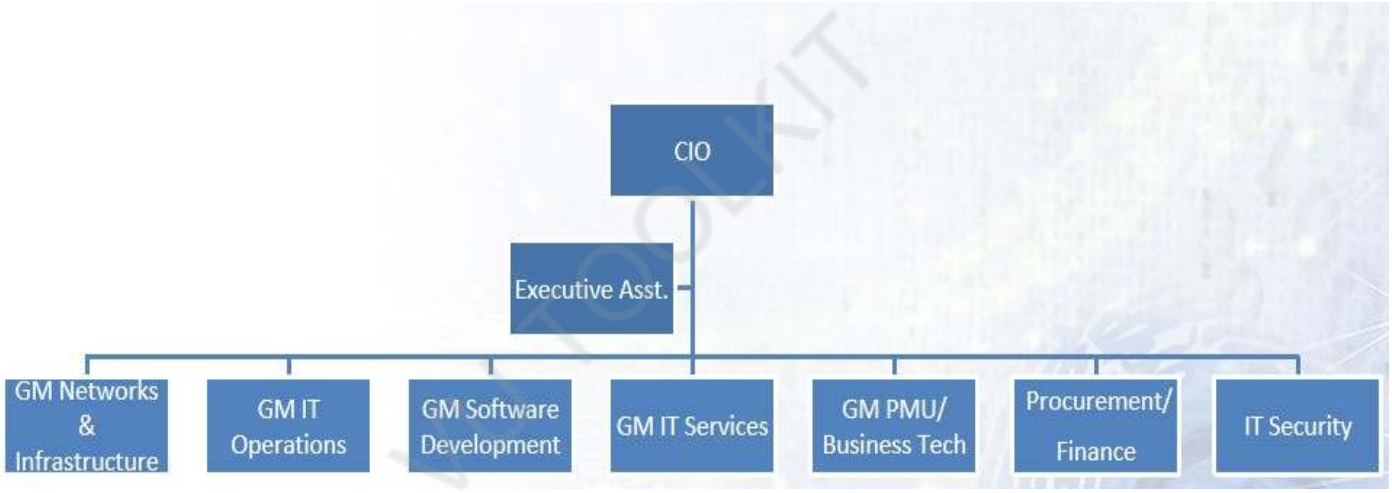
- Strong commitment of the Board & IT Director drove the implementation of the security transformation project
- ISO27001:2013 (ISMS) achieved as a security credential

Module: 32
What is the typical structure of an it team?

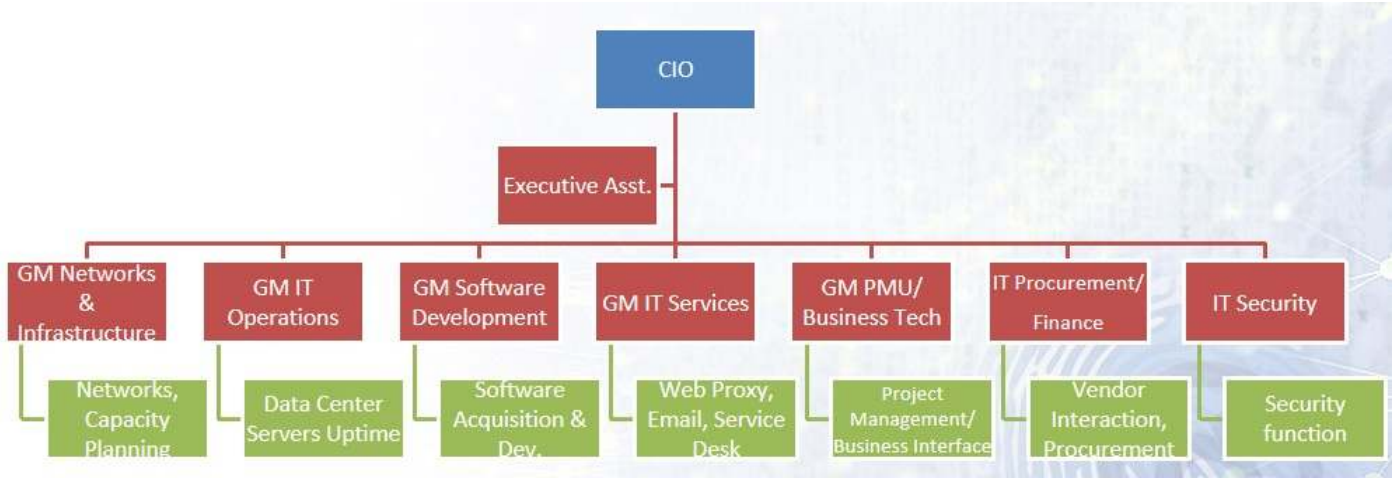
Structure of An IT Team

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

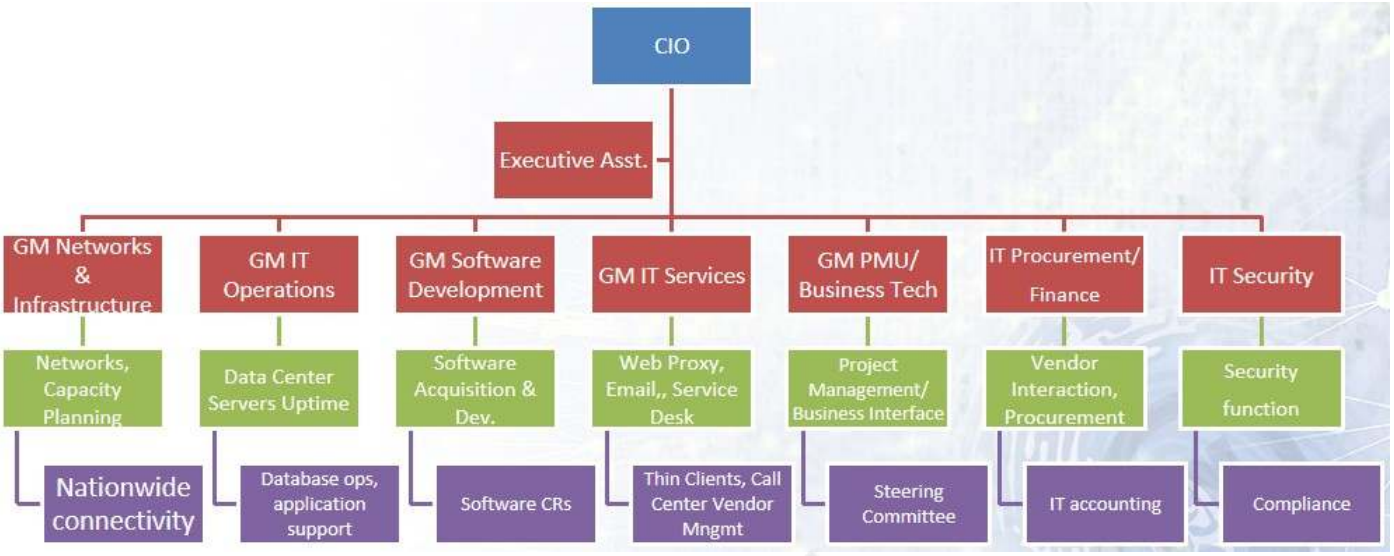
GENERAL STRUCTURE



JOB FUNCTIONS

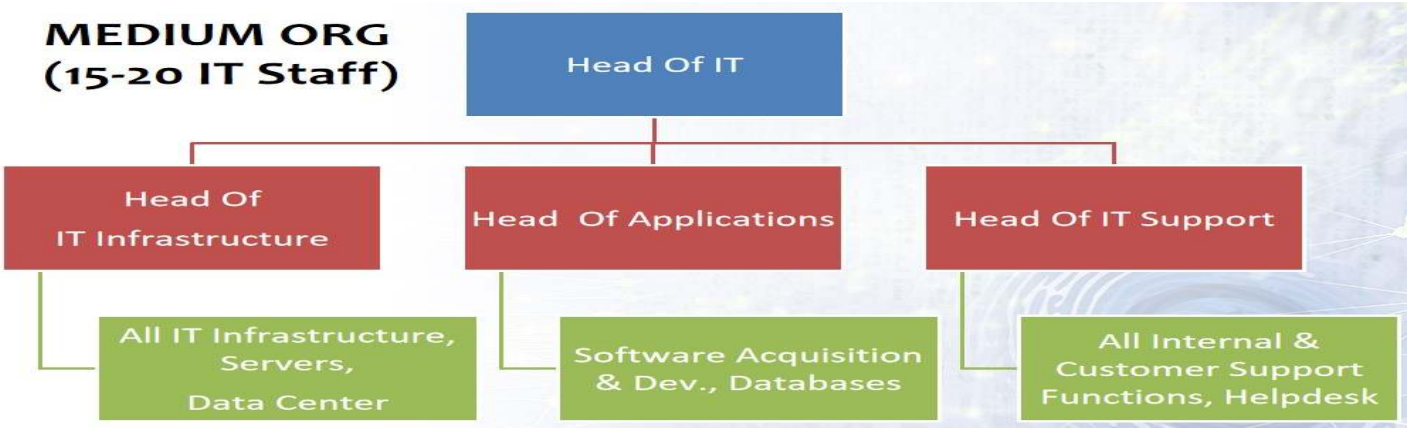


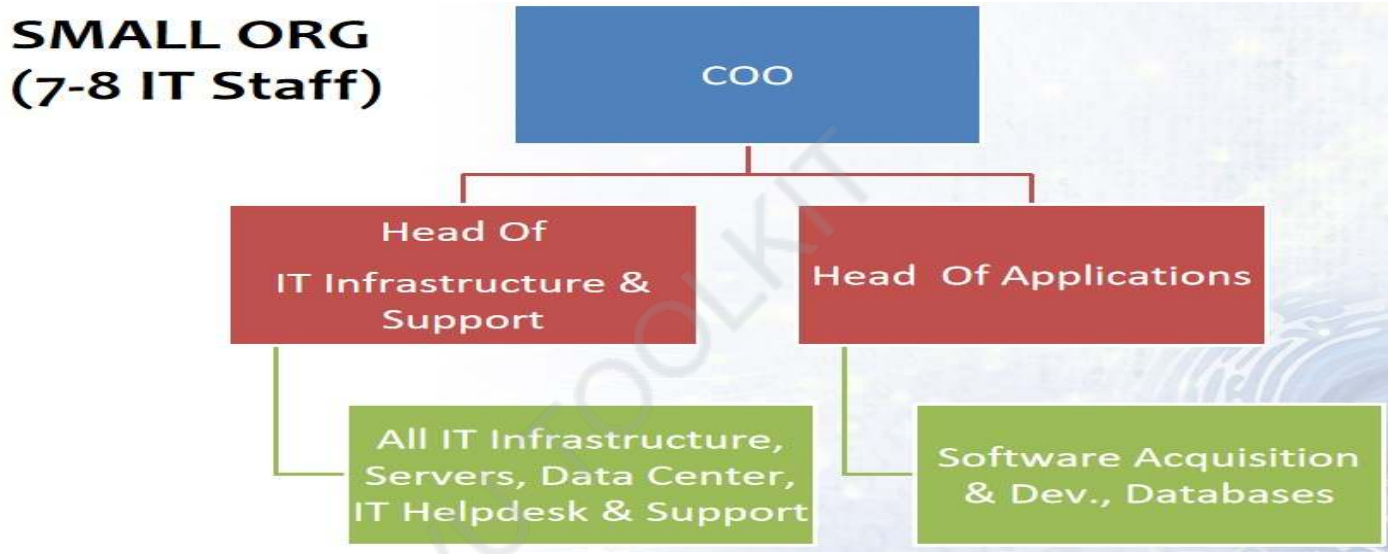
ADDITIONAL TASKS



LARGE ORG

(150 IT Staff)





- 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

Module: 33
What are the objectives and KPIs of a CIO and it team?

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

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

Performance KPIs:

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

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

General IT team's 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)

General IT team's 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

General IT team’s performance in Enterprise:

- Competence and professionalism of IT teams matches culture of organization
- IT efficiency driven by top management commitment and interest

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

Module: 34
How do the it team interact with other stakeholders in the organization?

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 budget/projects approved by IT Steering Committee (annual):

- Capex and opex layout
- Includes new projects & licensing / maintenance of operations
- New hirings

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

Audit & compliance requirements:

- External audit
- Internal audit
- Compliance
- Information security & risk depts

Expansion (branches) & maintenance:

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

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

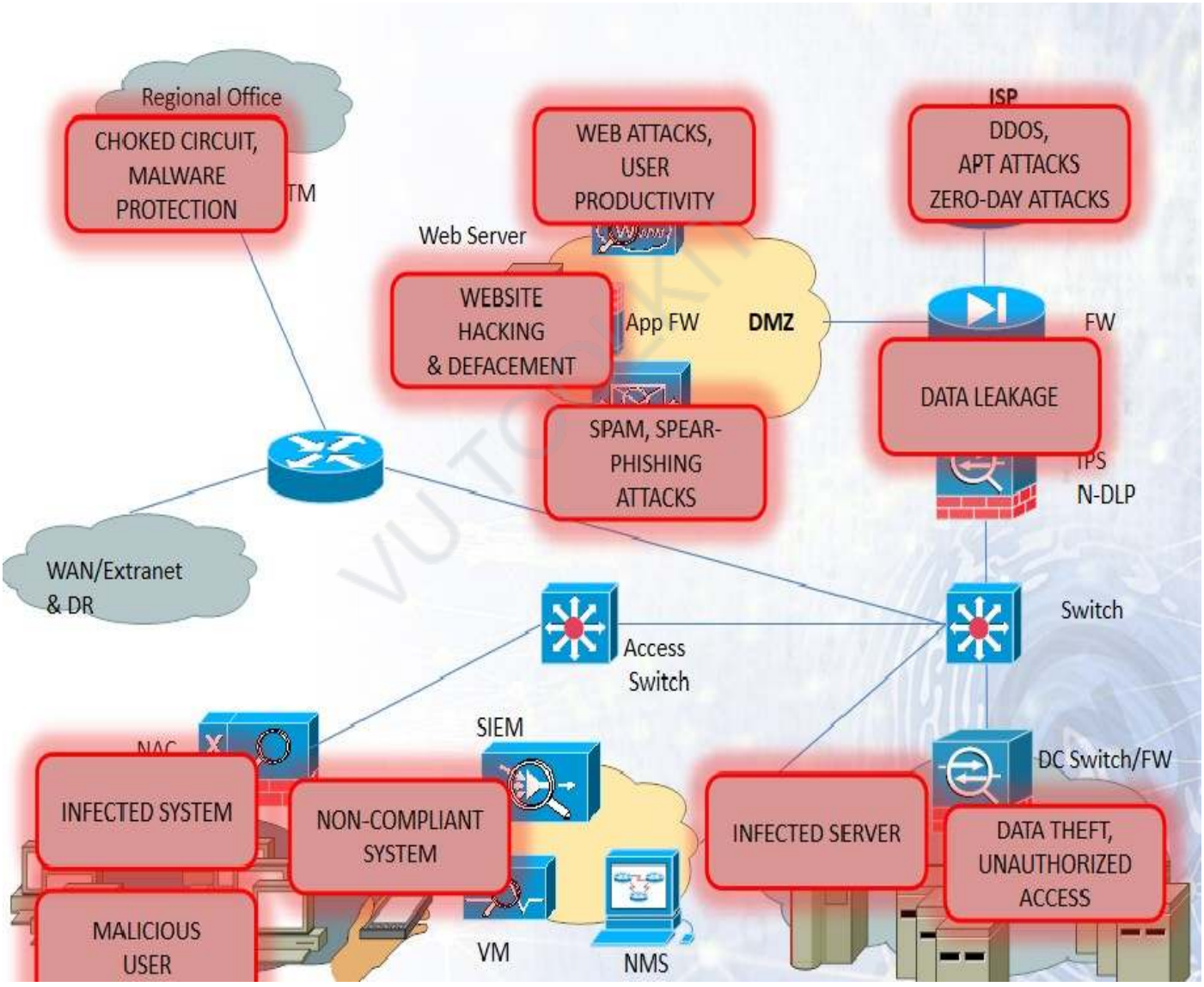
Business continuity & DR:

- 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

Module: 35
Security overlay of an enterprise architecture - i (components)

Security Overlay of Enterprise (Part 1)

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



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

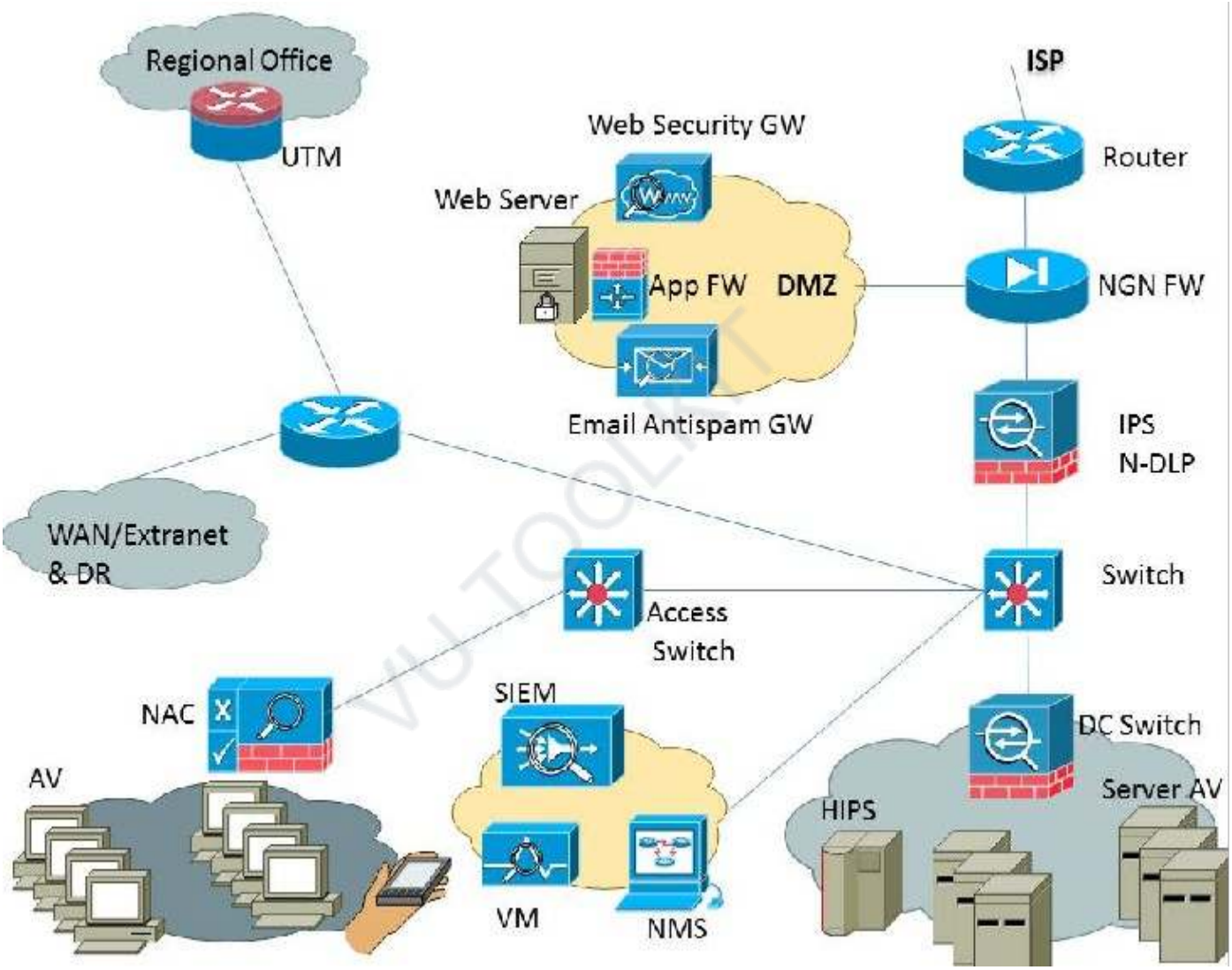
Security Challenge	Location/Device	Security Solution
Web-based User Attacks	DMZ / Web Security GW	Web Filtering & Malware Protection
System Malware	System	AV
User Network Access Control	At Aggregation Point Of User Access	Network Admission Control (NAC)
User Controls For USB/Media, HDD Encrypt	System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

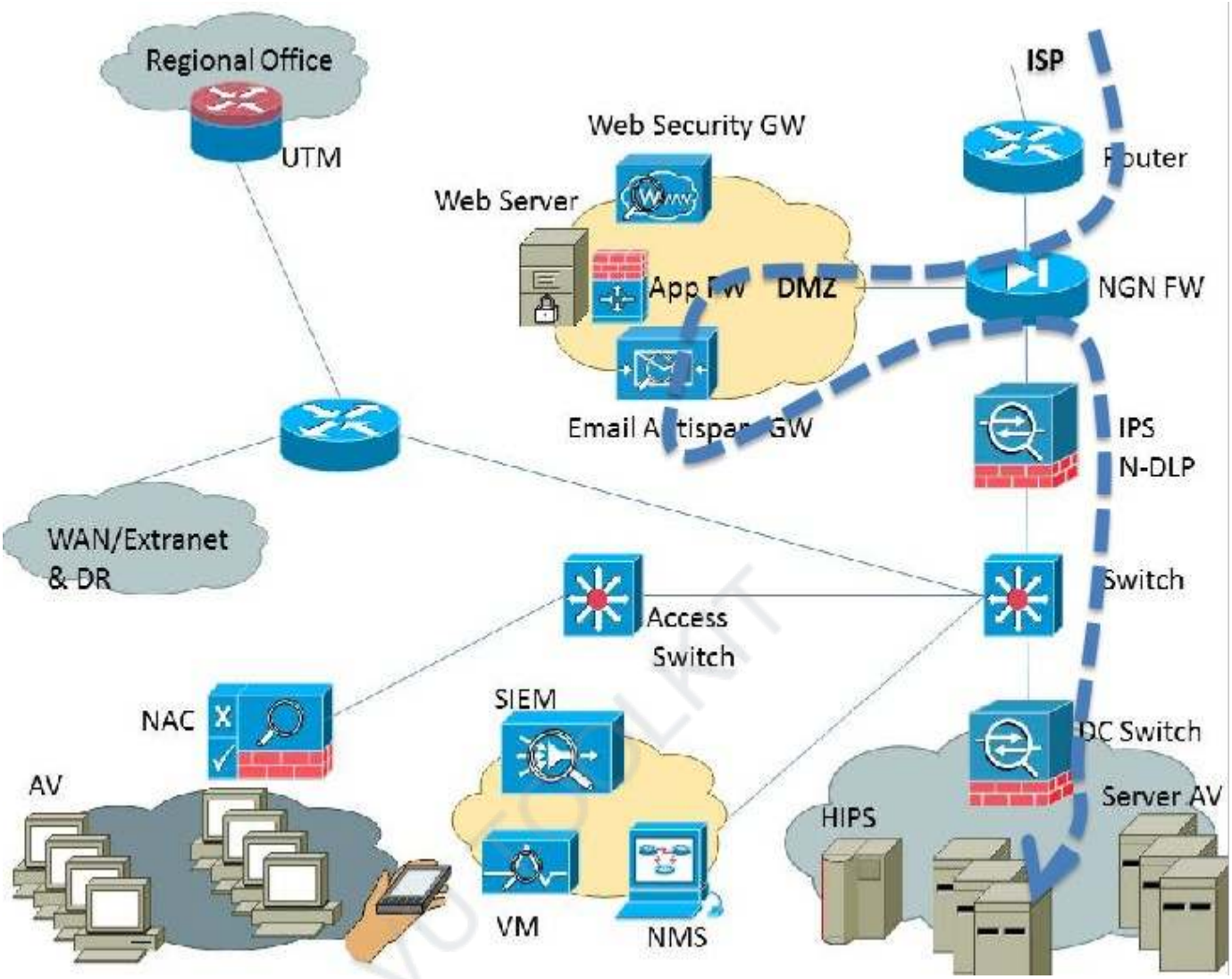
Security Challenge	Location/Device	Security Solution
Data Center Unauthorized Access / Malware	Data Center FW	Data Center FW Filtering & Malware Protection
Data Exfiltration	Edge / Network DLP	Network DLP Solution
Event Monitoring & Detection	Data Center / SIEM	Security Info. & Event Management
Unpatched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

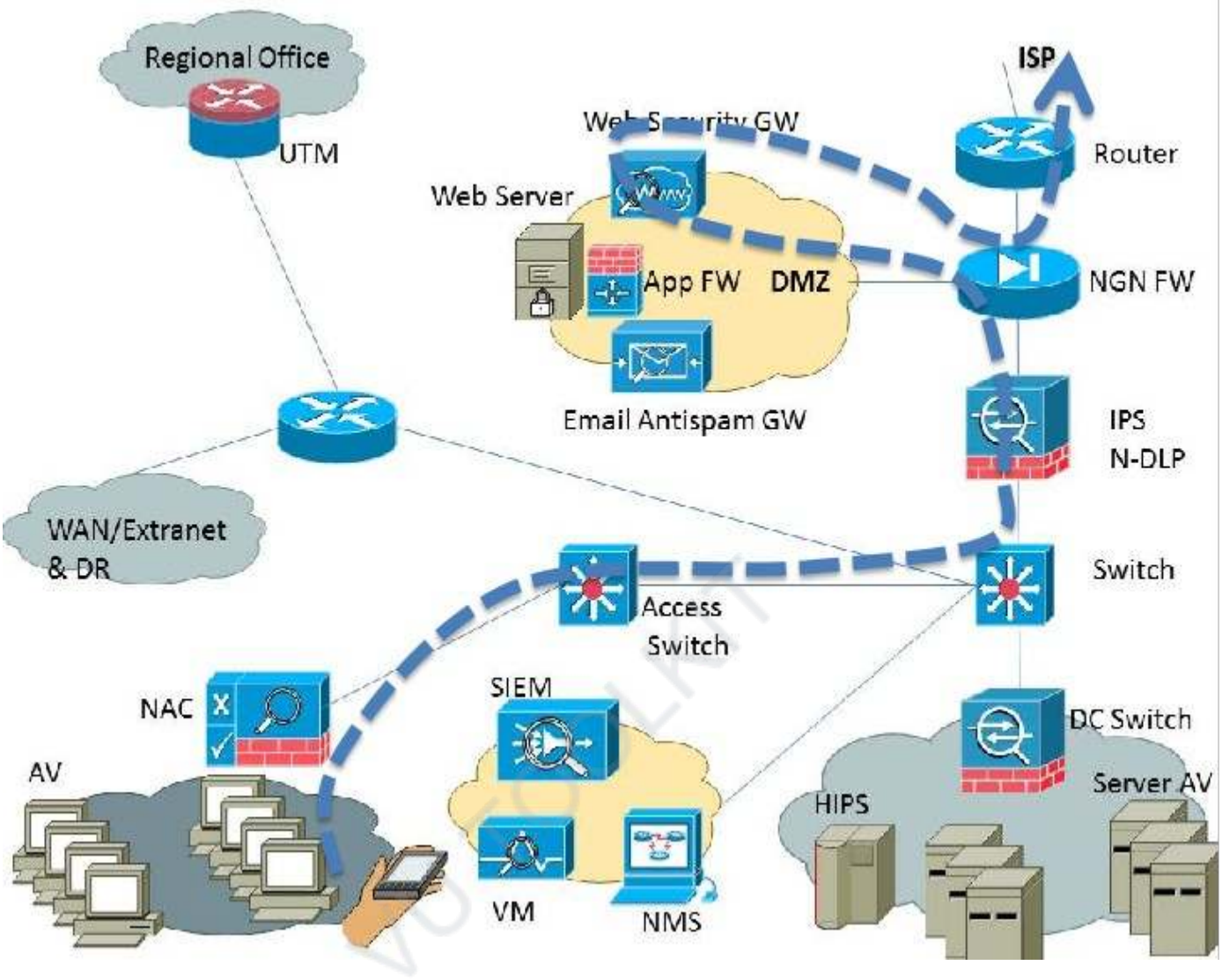
How is the enterprise secured with the help of various components and security design?

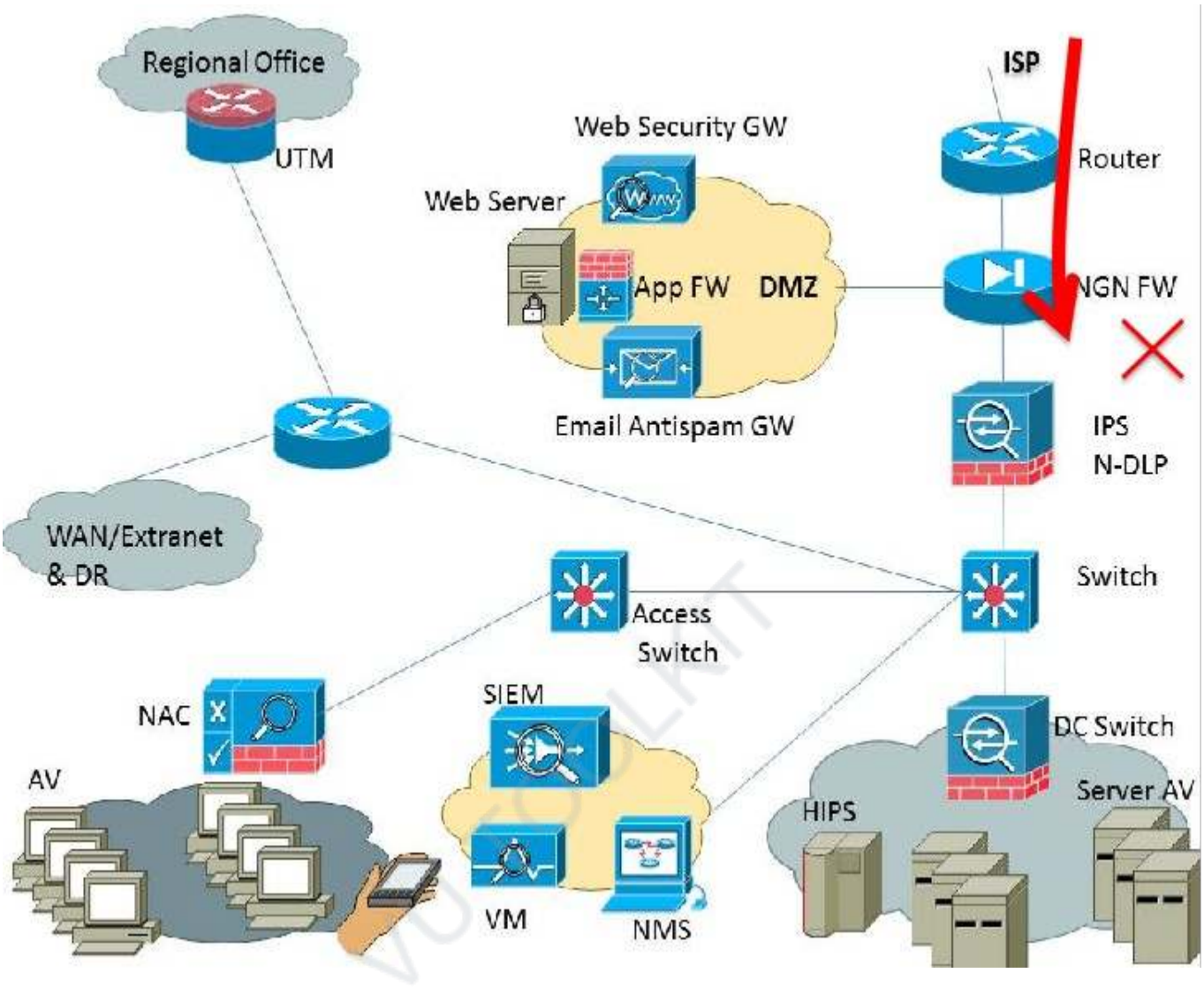
Module: 36
Security overlay of an enterprise architecture - ii (Traffic Flow)

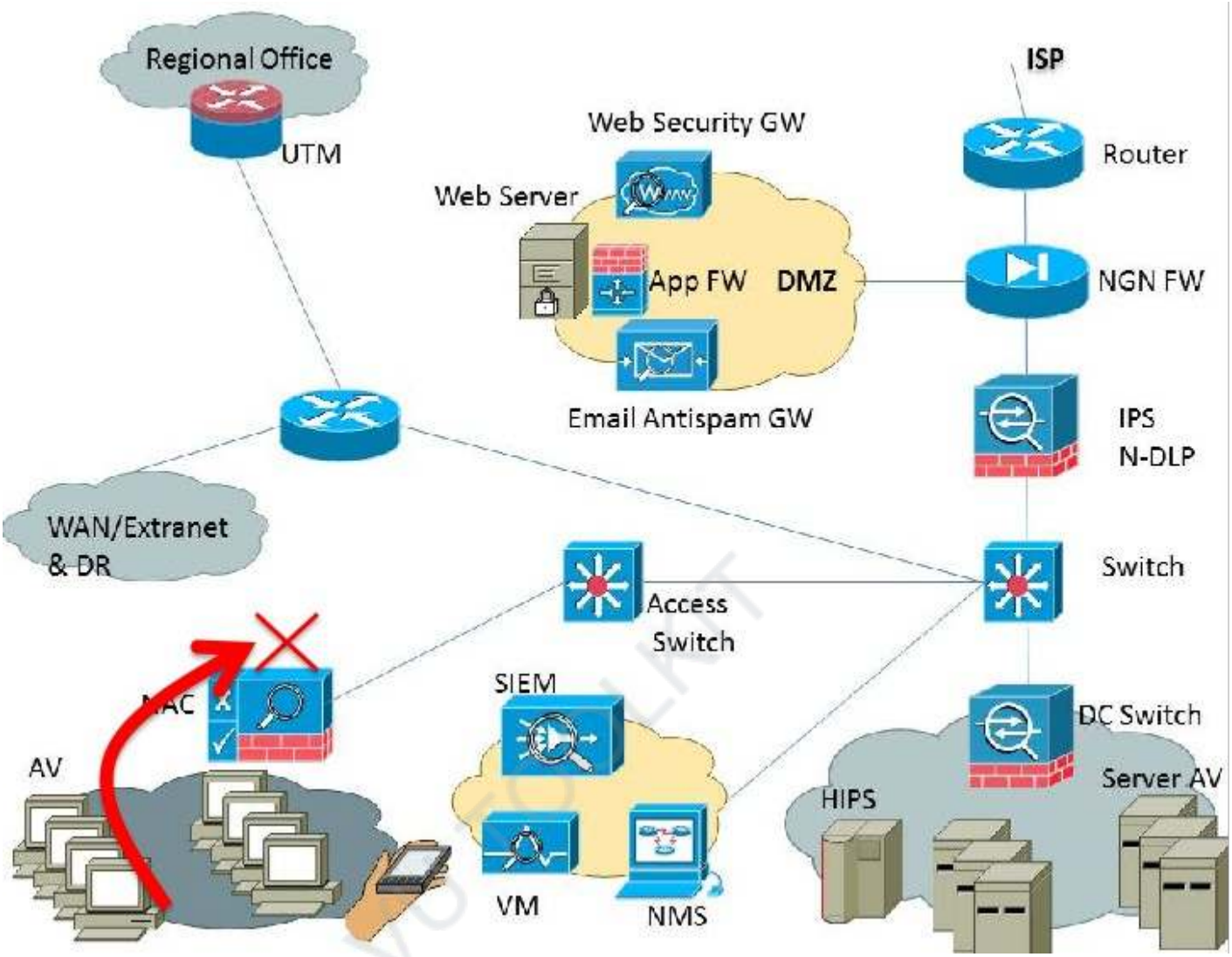
What is the traffic flows specific to good security design?

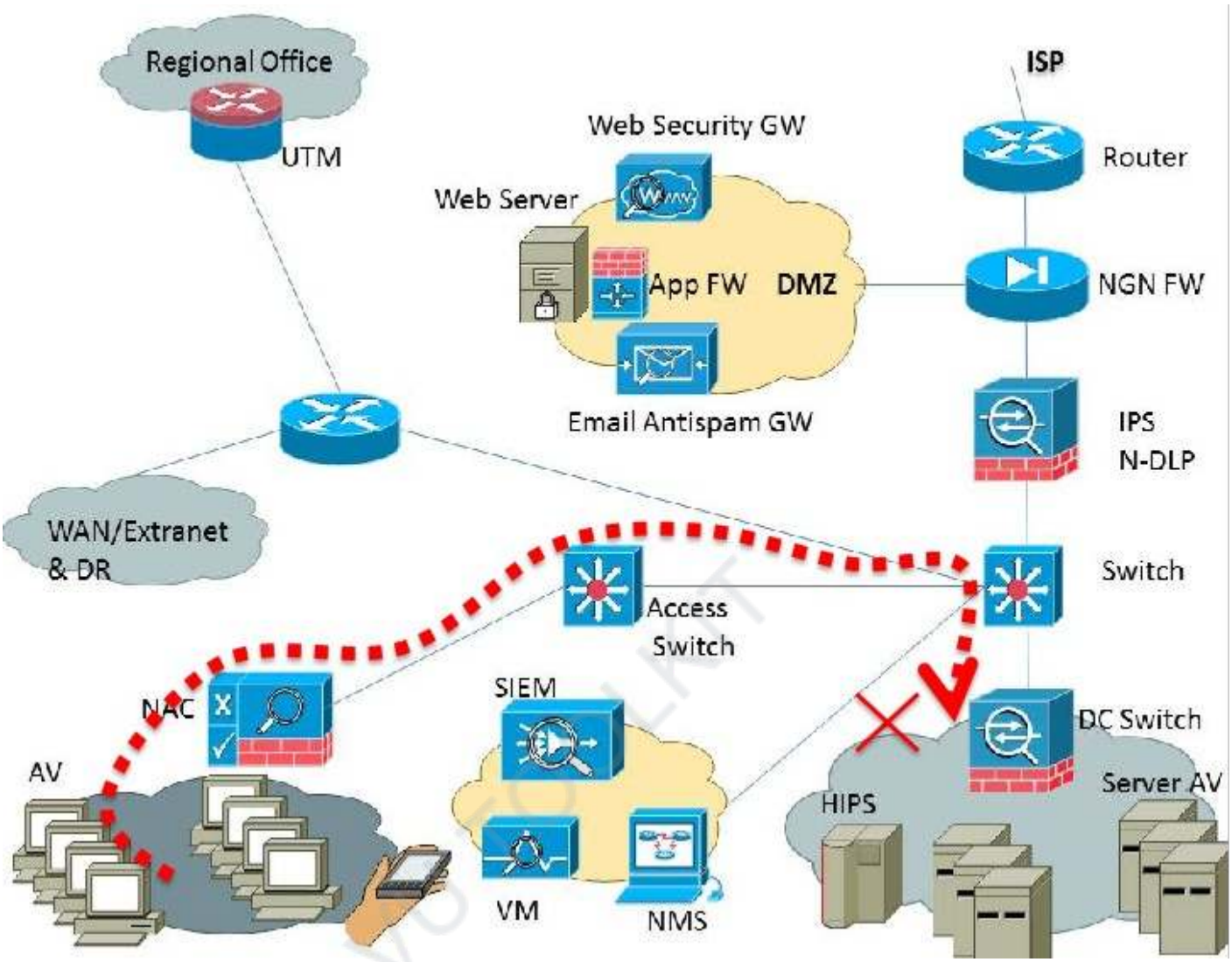


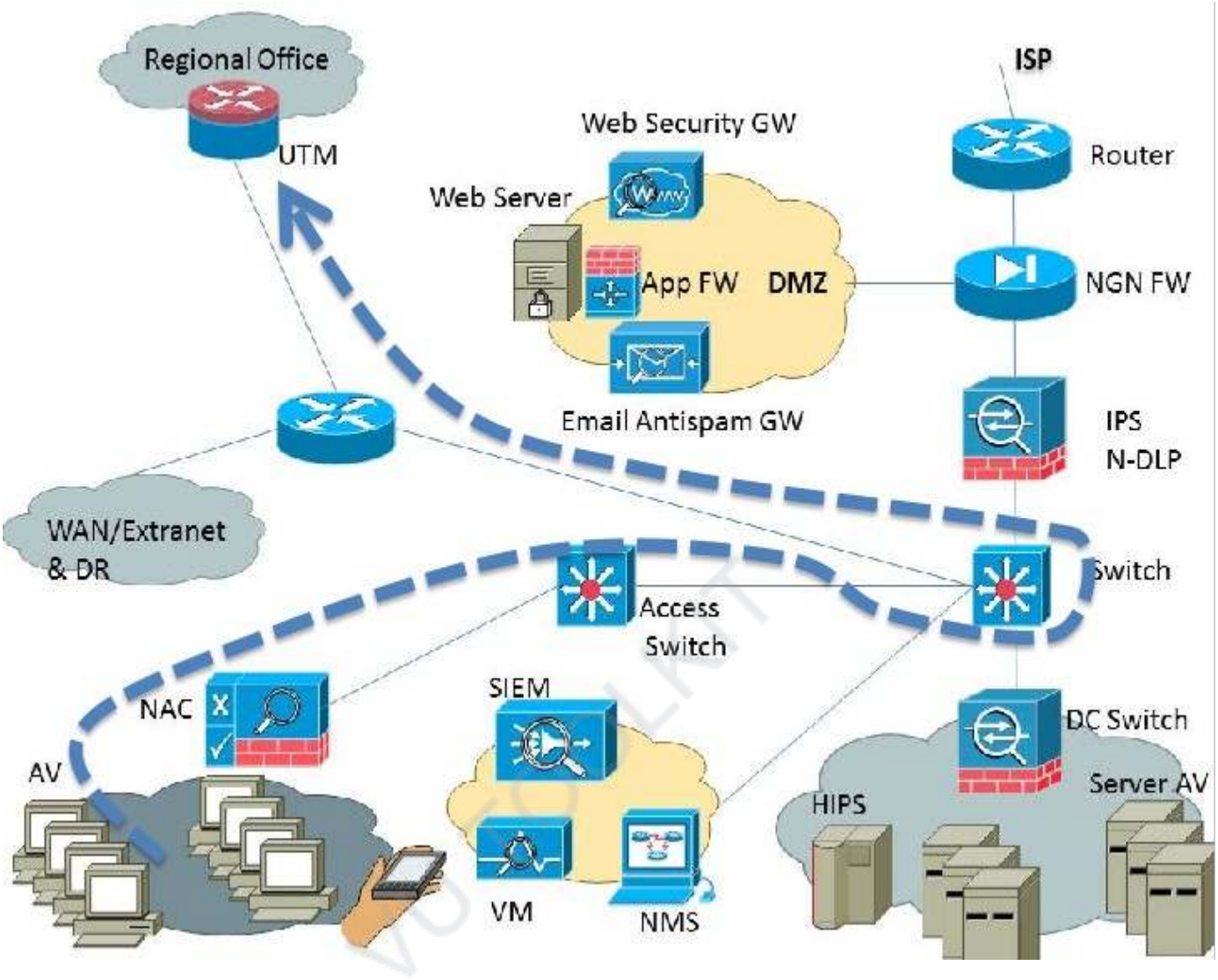


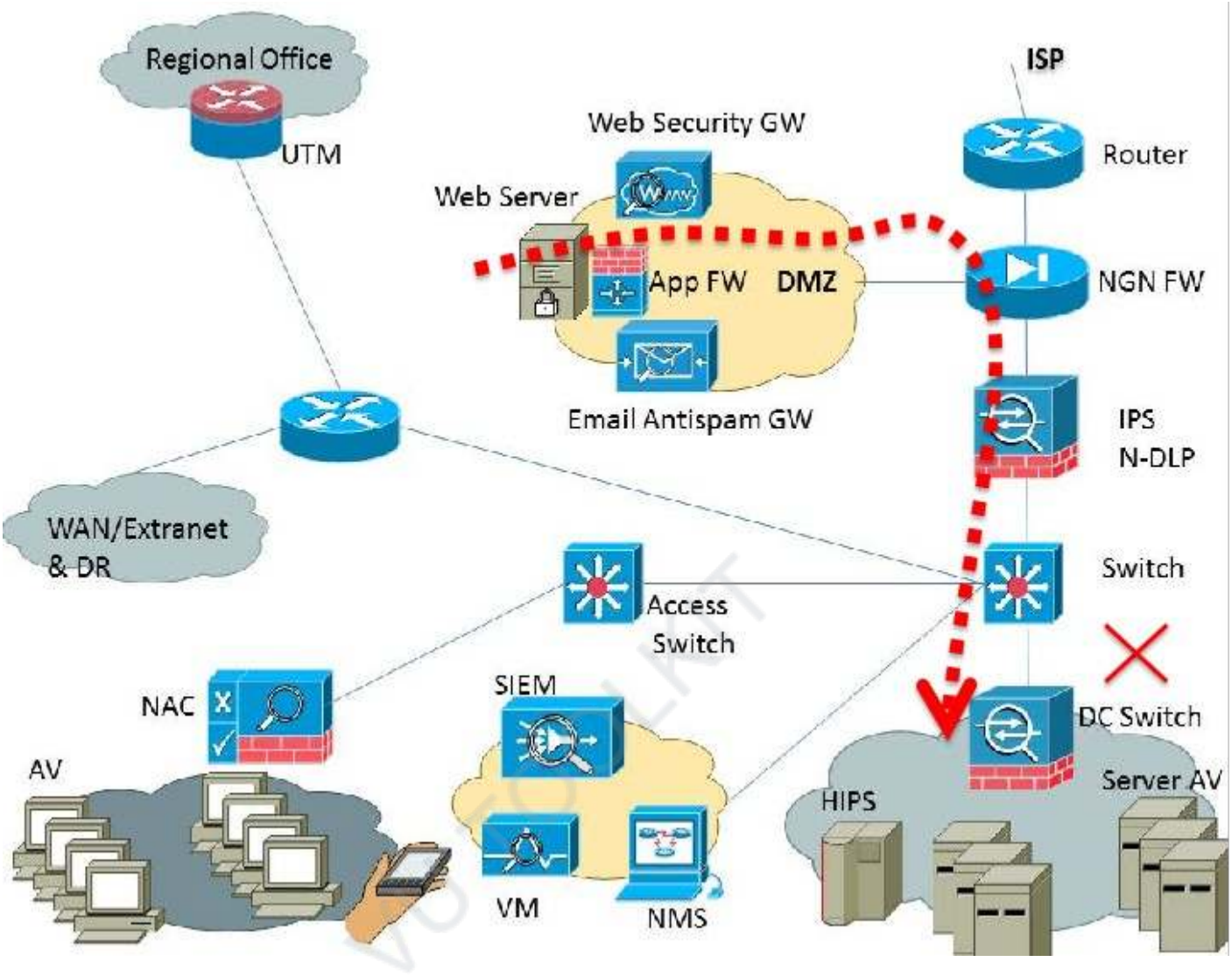








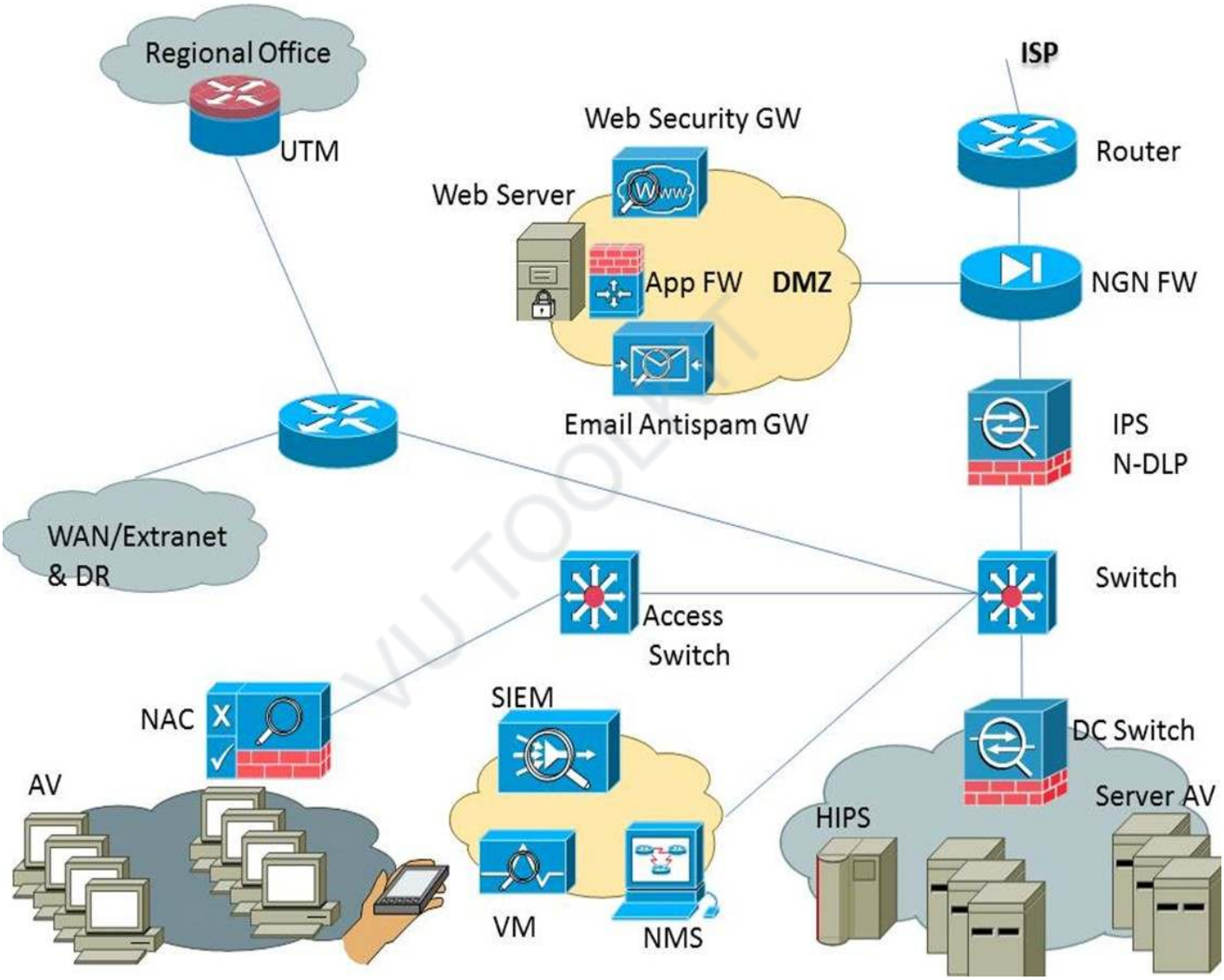




Granular access list filtering and a well-planned and tested security design are keys to success.

Module: 37
Security overlay of an enterprise architecture - iii (General security design)

General security design principles



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)

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

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)

Even More Advanced Security:

•Network forensics

•Host-based APT / IoC solution

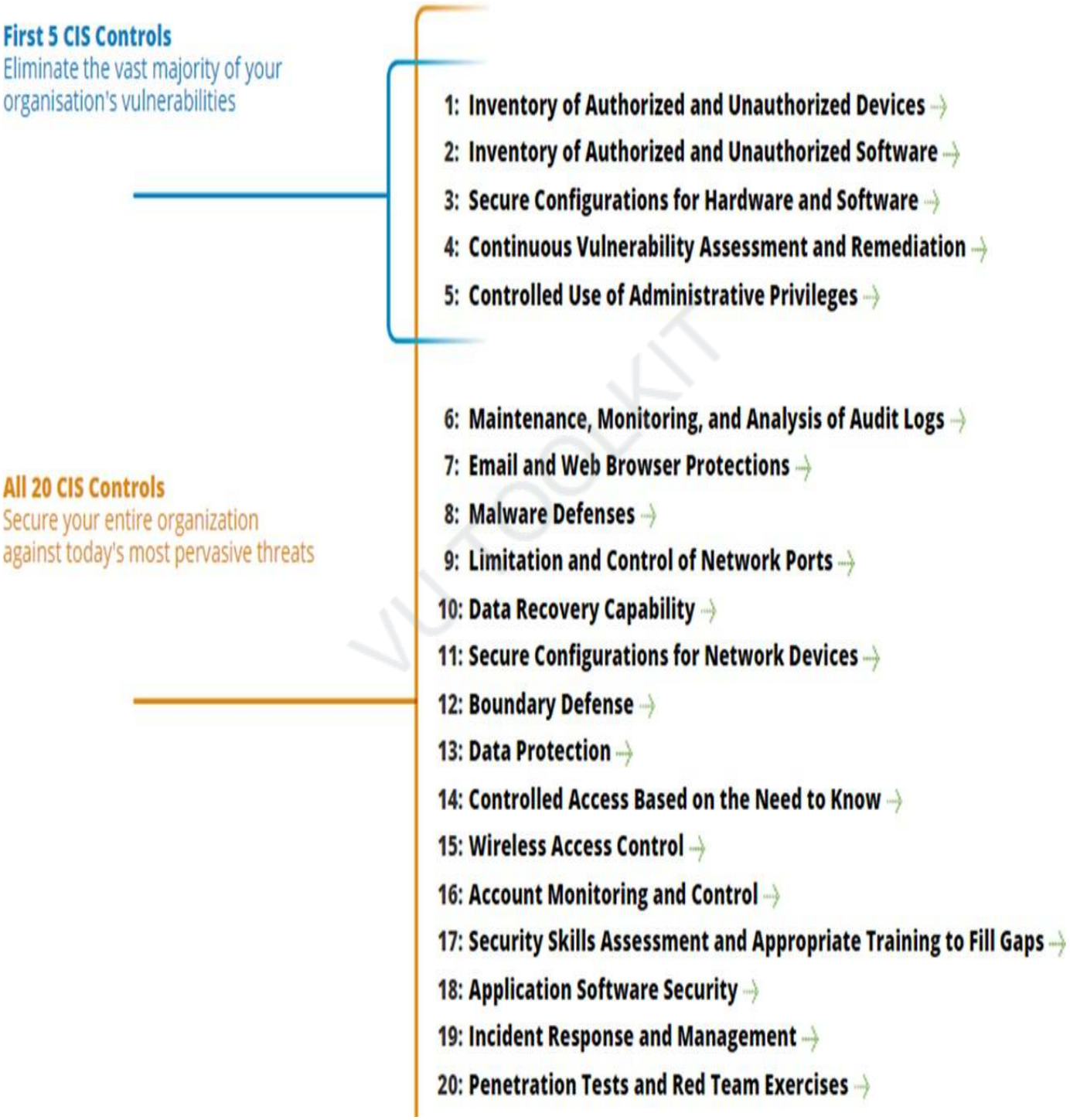
•Identity & access management (IAM)

•Privileged identity management (PIM)

•Database security solution

•Further guidelines for strong security controls:

–CIS 20 critical security controls



Further guidelines for strong security controls:

–CIS 20 critical security controls

Module: 38
What is high availability

–High availability of a system or component assures a high level of operational performance (uptime) for a given period of time

•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

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

•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 and fault tolerance:

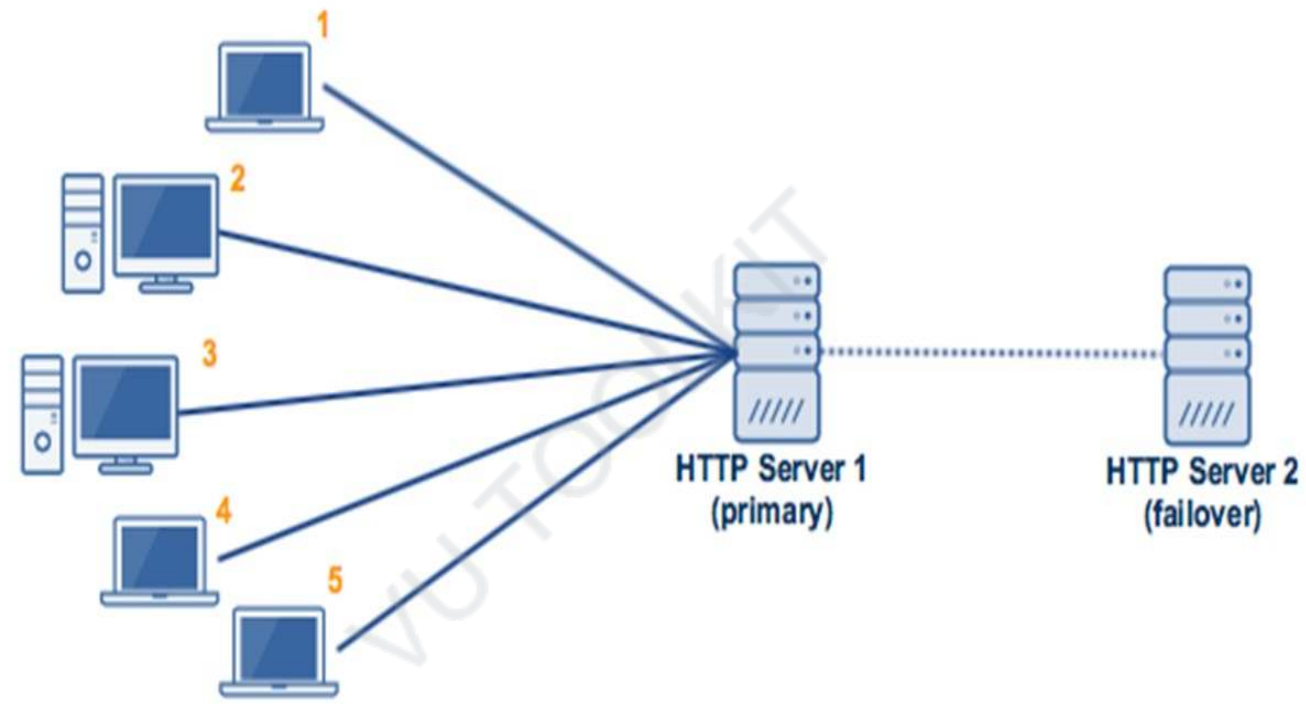
–Designed to minimize downtime with the help of redundant components

•Disaster Recovery:

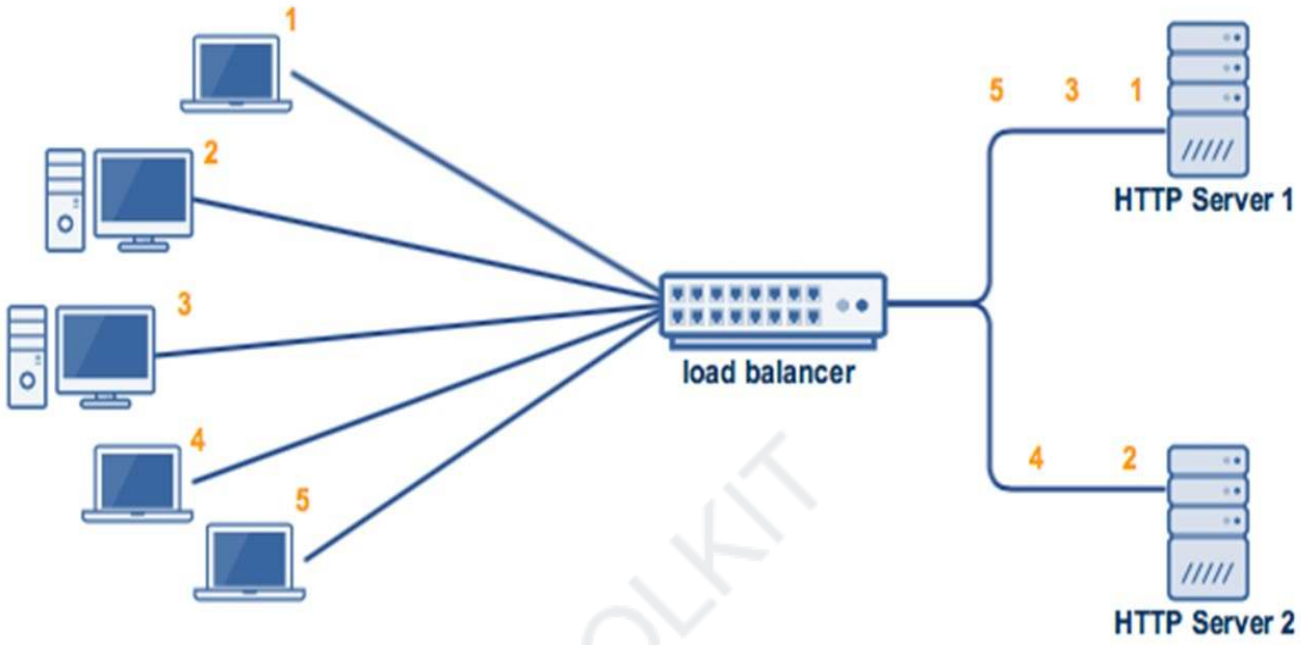
– A pre-planned approach for re-establishing IT functions at an alternate site

Module: 39
High availability design.

Let's look at various HA designs



ACTIVE-ACTIVE SERVER CONFIGURATION



Module: 40
How is site redundancy incorporated into enterprise network design?

•Three types of redundant site models:

•Hot site

•Cold site

•Warm site

•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

•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

•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

•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)

•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)

•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.

Module: 41
High availability and 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

•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

•Primary DC:

–Fully redundant (HA) design for network, systems, and storage

–Cisco HA (active-standby)

–Oracle cluster technology for servers and DBs (active-active)

•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

•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)

•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

•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

Module: 42
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 ?

•What to backup ?

–Network configuration files

–OS backups

–Database & application data

–Other critical data

•Backup location ?

–Onsite for faster recovery

–Offsite for DR purposes

–Intermediate site (secondary site) as a middle-ground

•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 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 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 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

Module: 43
What is the role of security tools in securing the enterprise

Typical security tools used in an enterprise:

–Enterprise antivirus

–MS Active Directory (AD)

–Vulnerability manager

–Logs management

–Network & performance monitoring

–Automated backups

•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

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

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

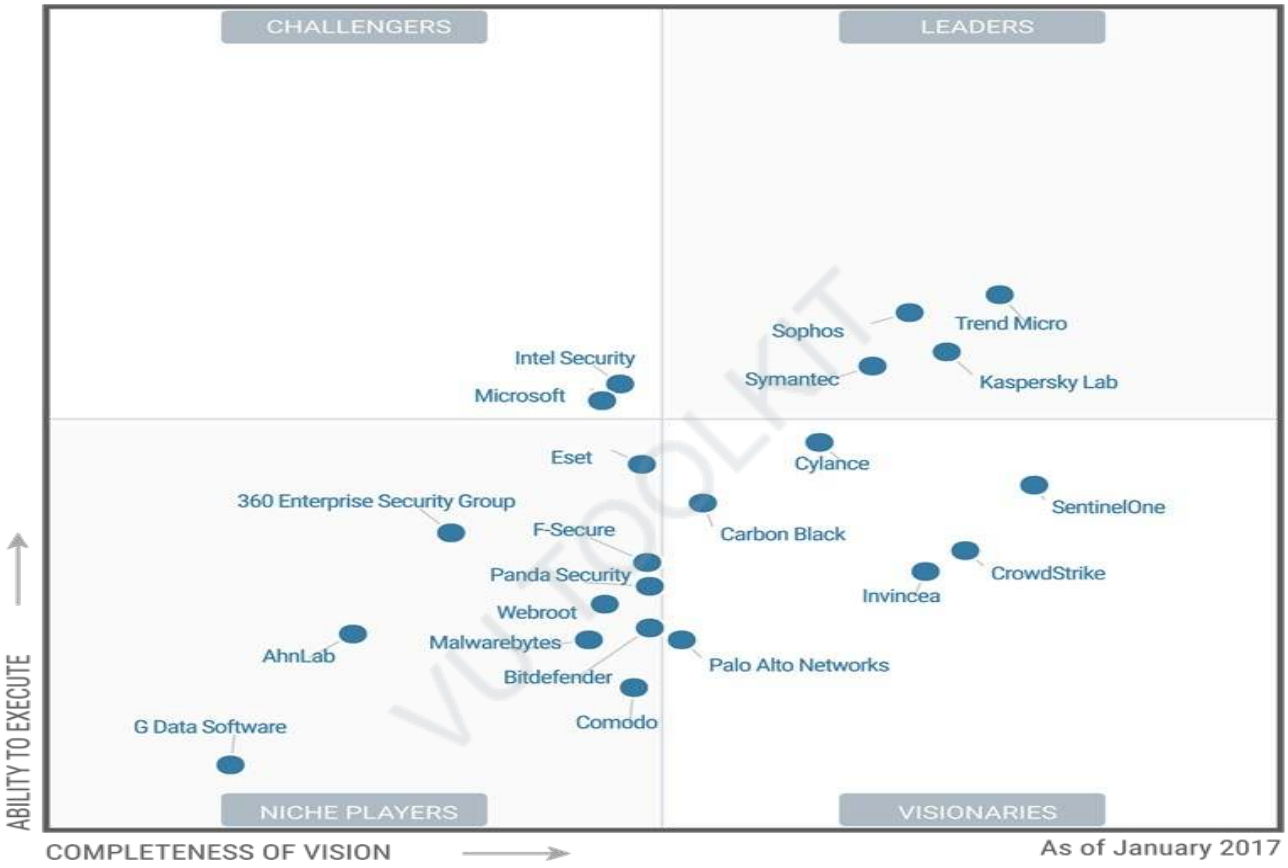
Tool	Function	Complexity level	Examples
Asset Management	Dtect, Track, Manage Assets	Medium	Asset Explorer, PulseWay
Trouble Ticket System	TT Workflow	Medium	BMC Track-IT, SysAid
SIEM	Event Management	High	OSSEC, Splunk, Q-Radar
DLP	Data Loss Prevention	High	Symantec,
Encryption Software	Encryption	High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

- Lots of tools available
- People, process, technology

Module: 44
Typical security tools used in an enterprise IT network – Part 1

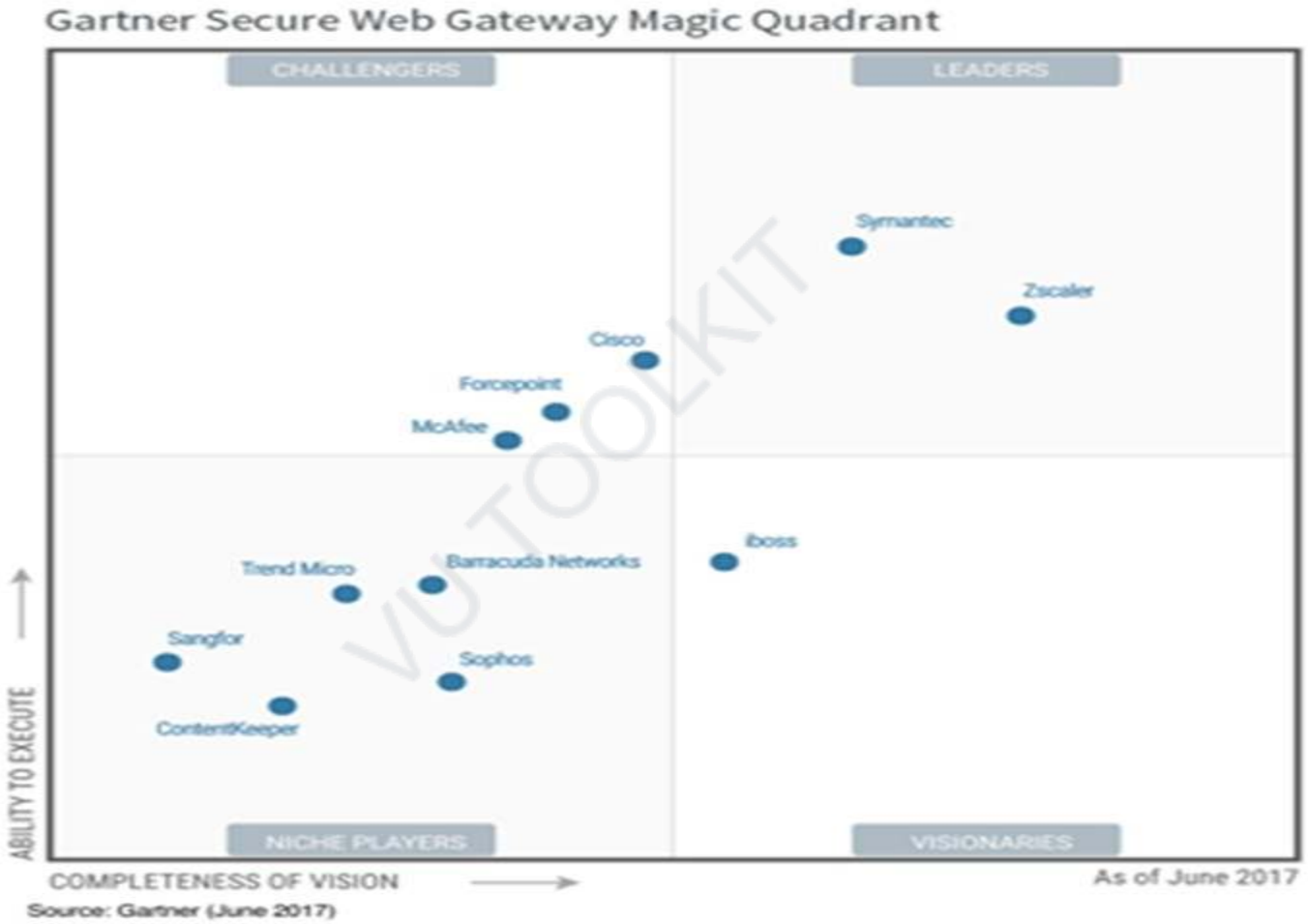
Gartner Magic Quadrant reports

•List of some other industry reports



Endpoint Protection Jan, 2017 Gartner

Trend Micro Sophos Kaspersky Symantec



Secure Web GW June, 2017 Gartner

Symantec Zscaler

UTM
(SMB Multi-function FW)
June, 2017
Gartner

Fortinet
Checkpoint

View and read various industry reports for security tools comparisons:

–Gartner

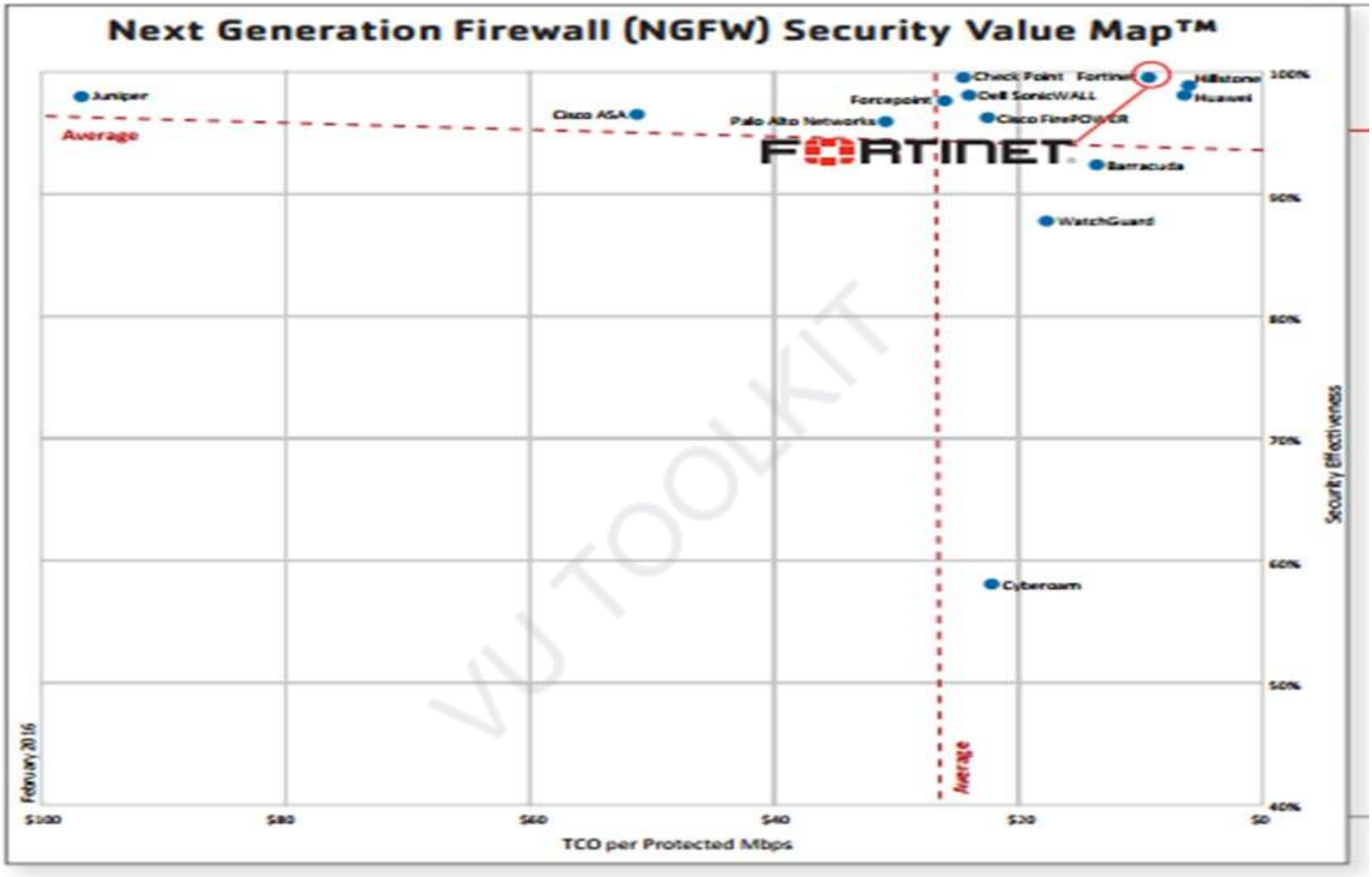
–Forrestor

–Security Awards

–Lab reports: ICSA, NSS

Module: 45
Typical security tools used in an enterprise IT network – Part 2

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



NGFW
NSS Labs
2016

Hillstone
Huawei
Fortinet

Enterprise Mobility Management (EMM) June 2017

VMWARE MobileIron IBM Blackberry

Gartner

- Forrestor
- NSS labs
- ICSA Labs

Module: 46
What does the term “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

•Box for :

–Email security

–Web security

–FW

–IPS

–APT attack prevention

–DDOS prevention

–Network DLP

–Network Forensics

–Others

•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

•“Box security” is not the silver bullet

•Although many devices and boxes are required, they do not ensure a good security posture

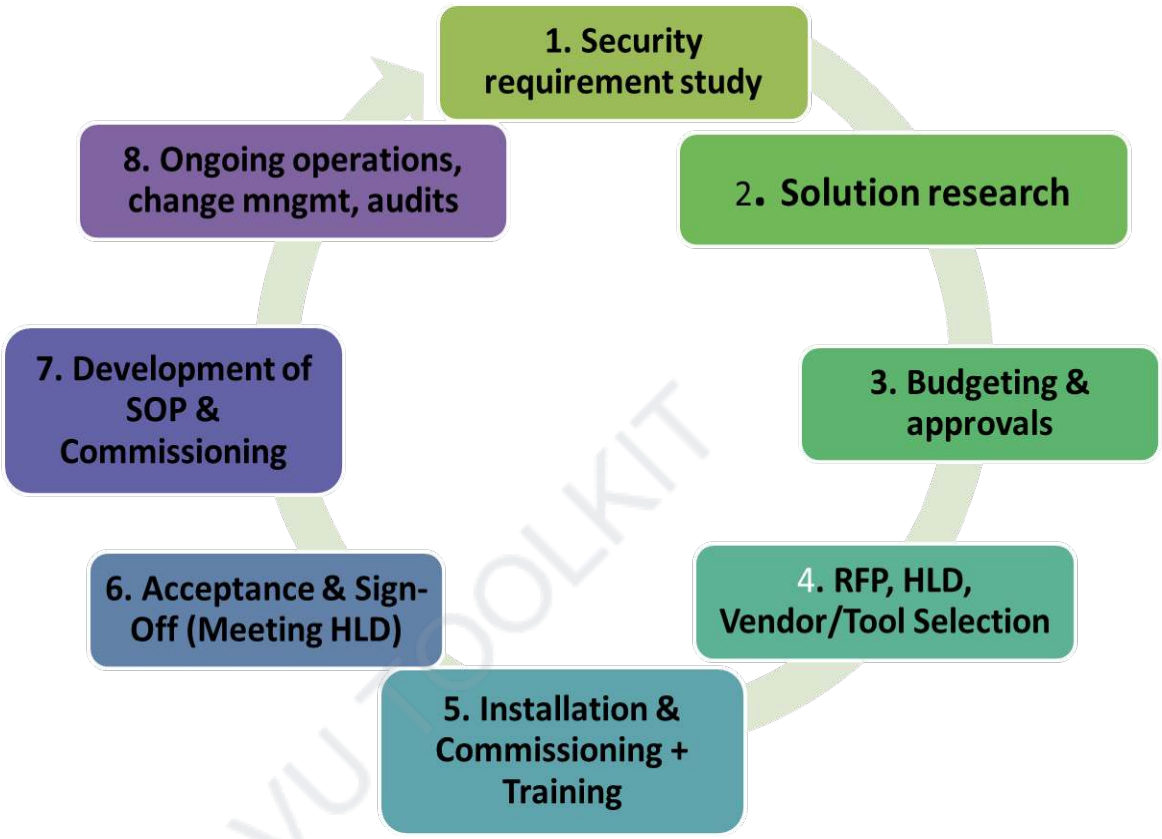
•This approach is unfortunately promoted by many vendors who have equipment to sell

•Consider organizational maturity & readiness

•Other challenges with “box security” approach:

–Shortage of staff (IT & security)

–Training and skill required to operate the sophisticated devices and features



•Device objectives, and high-level-design (HLD) should be planned prior to commissioning

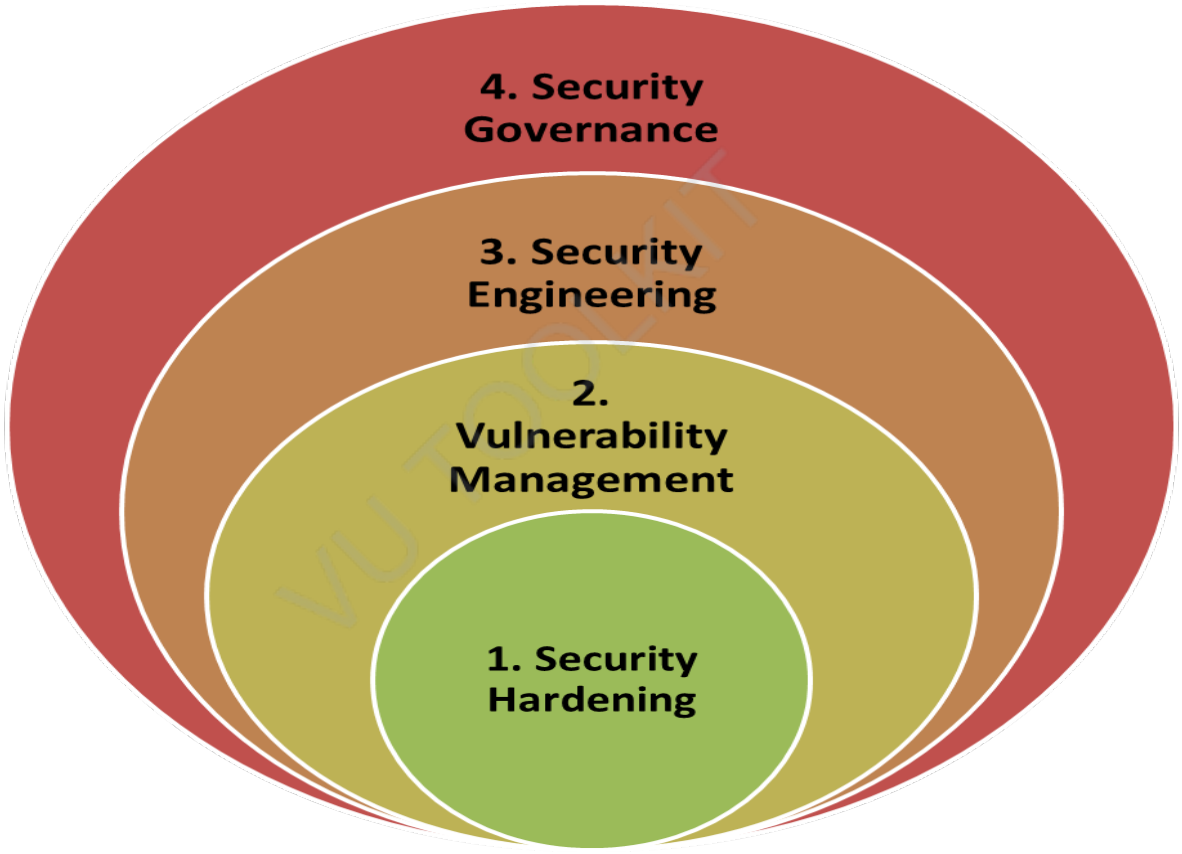
•Min operational baseline and configuration should be documented in SOP

•Device feature set and configuration audits should be conducted on a periodic basis (annual)

Module: 47
What is the best approach to secure the IT enterprise architecture?

•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



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

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

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.

Module: 48
What is disaster recovery?

•What is a disaster?

–Any significant event that causes disruption of information technology processing facilities, thus affecting the operations of the business

•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

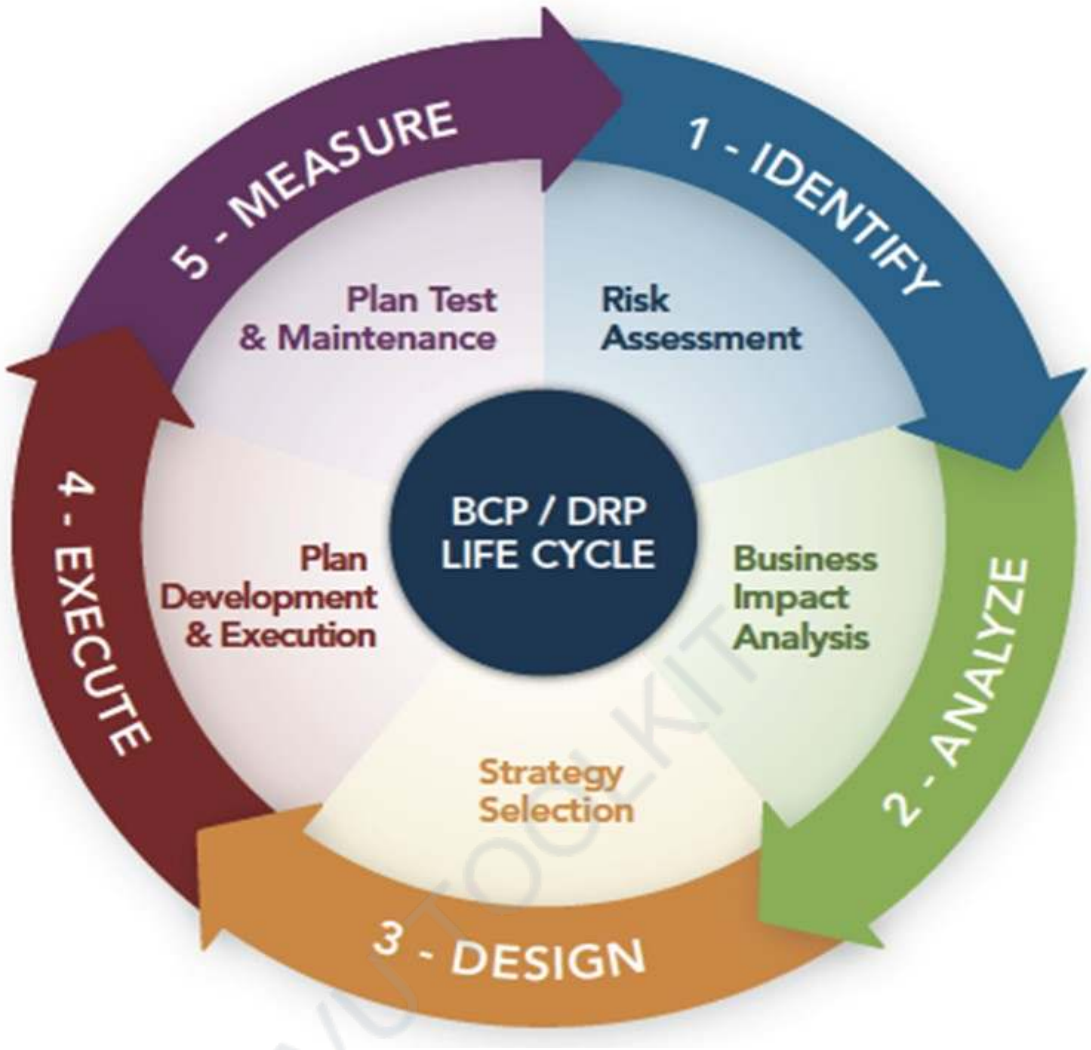
•What could cause the invocation of a DR failover to DR site ?

–Natural disasters such as flood, earthquake, lightning, storm

–Disaster caused by human actions such as riot, fire, terrorist act, etc

•What is 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)



•Three step process:

–Failover to the DR site (DR invocation)

–Restoration of the services/facilities on primary site

–Recovery (switchover back to primary site)

•What is a DR plan?

–A documented, structured approach to dealing with unplanned incidents

•DR plan checklist:

–Scope of the activity

–Gathering relevant network infrastructure documents

–Identifying the most serious threats and vulnerabilities, and the most critical assets

–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

•Sample DR plan template:

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

Module: 49
What is business continuity?

•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)*

•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 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)*

•What is a BC plan ?

–A document that consists of critical information an organization needs to continue operating during an unplanned event

•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.

Module: 50
How is DR accommodated into the enterprise architecture – part 1

•DR considerations:

–DR plan

–RTO & RPO

•DR plan:

–A disaster recovery policy statement, plan overview and main goals of the plan

–Key personnel and DR team contact information

•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.

•DR plan (contd)…:

–A list of software and systems that will be used in the recovery.

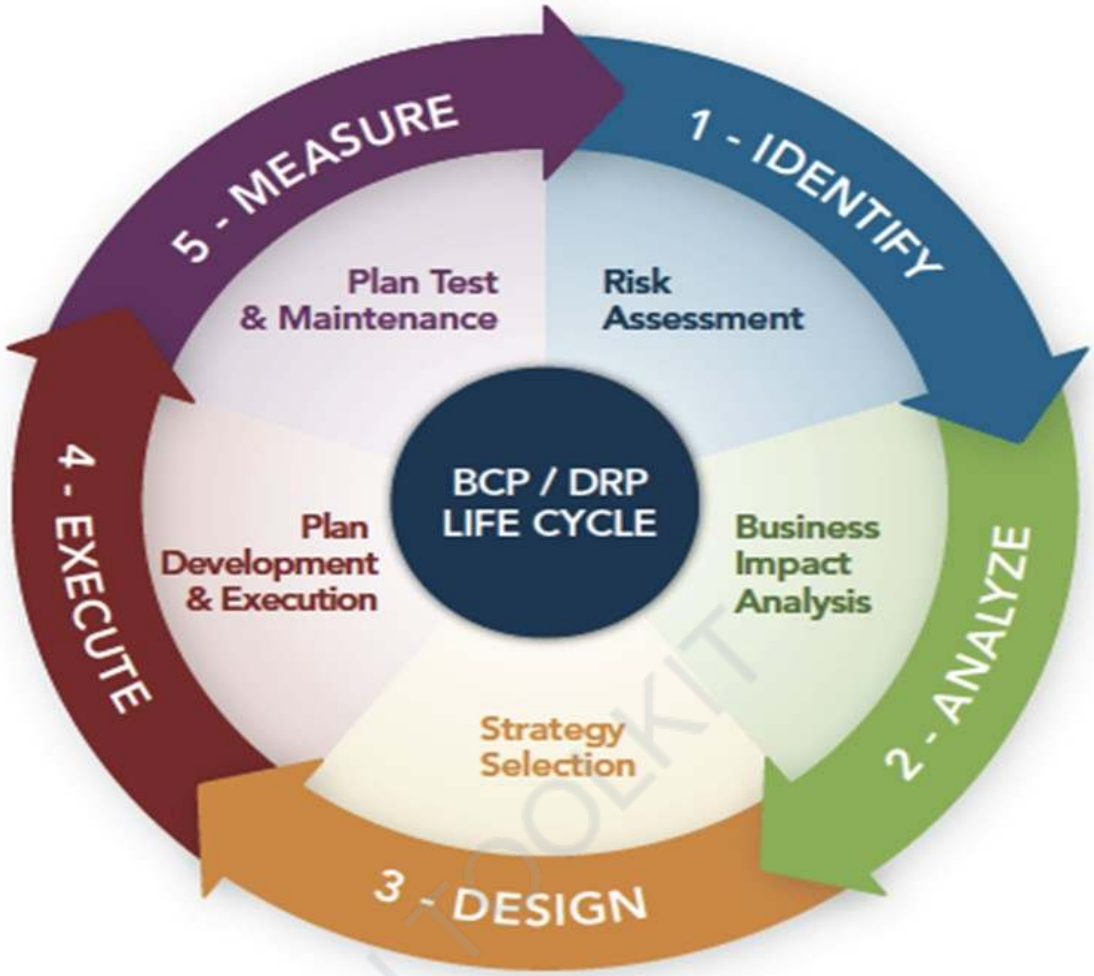
–Sample templates for a variety of technology recoveries, including technical documentation from vendors.

•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.



•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.

•RTO:

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

•RPO:

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

•RPO:

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

Module: 51
How is DR accommodated into the enterprise architecture – part 2

•DR considerations:

–DR facility

–DR drills & testing

–DR testing checklist

–BC plan alignment

•DR facility:

–Location

–Media circuits and backup circuits

–Power and environment

–IT data center design

–Based on DR plan

–Operations & maintenance

•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 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.

•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.

•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

•BC plan alignment:

–DR is under IT ownership, whereas BC is under business operations ownership

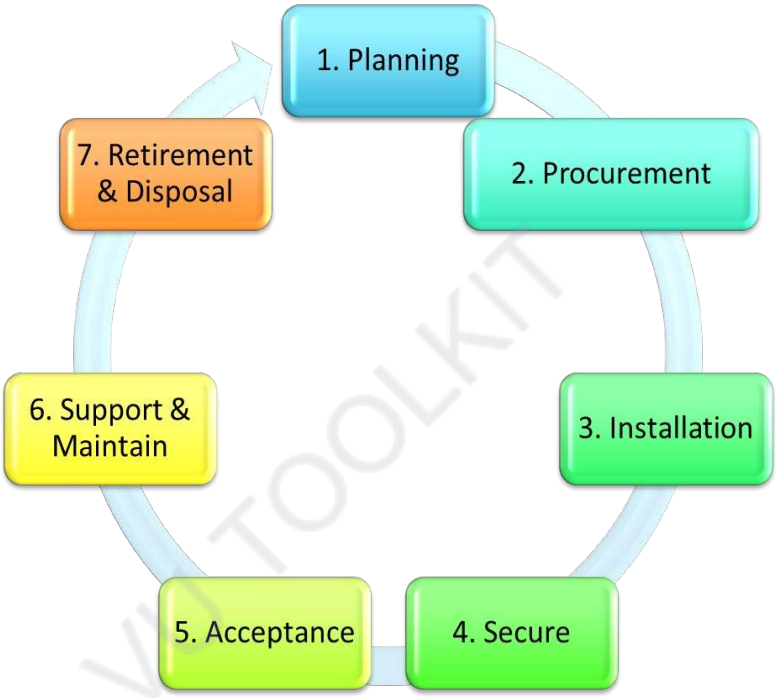
–DR is part of overall BC

–Both plans must integrate and align seamlessly

Module: 52
What is the role of an IT set in securing the organization?

•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.



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

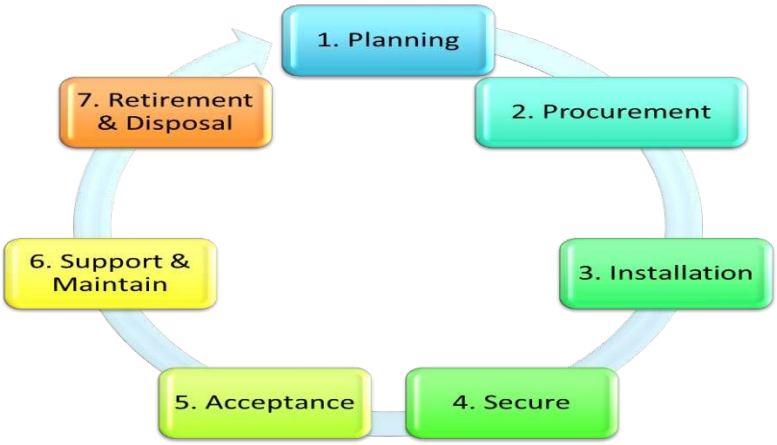
- Test Scripts
- UAT
- Security Accreditation
- Commissioning Sign-off
- Change Management

6. SUPPORT/MAINTAIN

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

7. RETIRE/DISPOSE

- Decommission
- Dispose/Salvage
- Update Inventory



•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

•Acceptable Use (Of IT Assets):

–Laptops

–Mobiles

–Web browsing

–Email usage

–Servers

–Company data

Module: 53
How to determine security posture of an organization

•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 ?

–Security hardening done on IT assets ?

–Which standard used for hardening ?

–Internal VM program ?

–Frequency of VM scanning ?

–Licensed software for OS/DB/Programs ?

–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 ?

–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 ?

–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 ?

–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 ?

–Security standard or framework followed for governance ?

–Internal security awareness program ?

–Maturity of change management and incident management

–Board Steering Committee (Information Security)

•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 ?

Module: 54
How do you drive a successful information security transformation?

•Critical factors for successful security transformation projects:

–Board-level buy-in and sponsorship

–Regular Board or Executive management project reviews and decisions

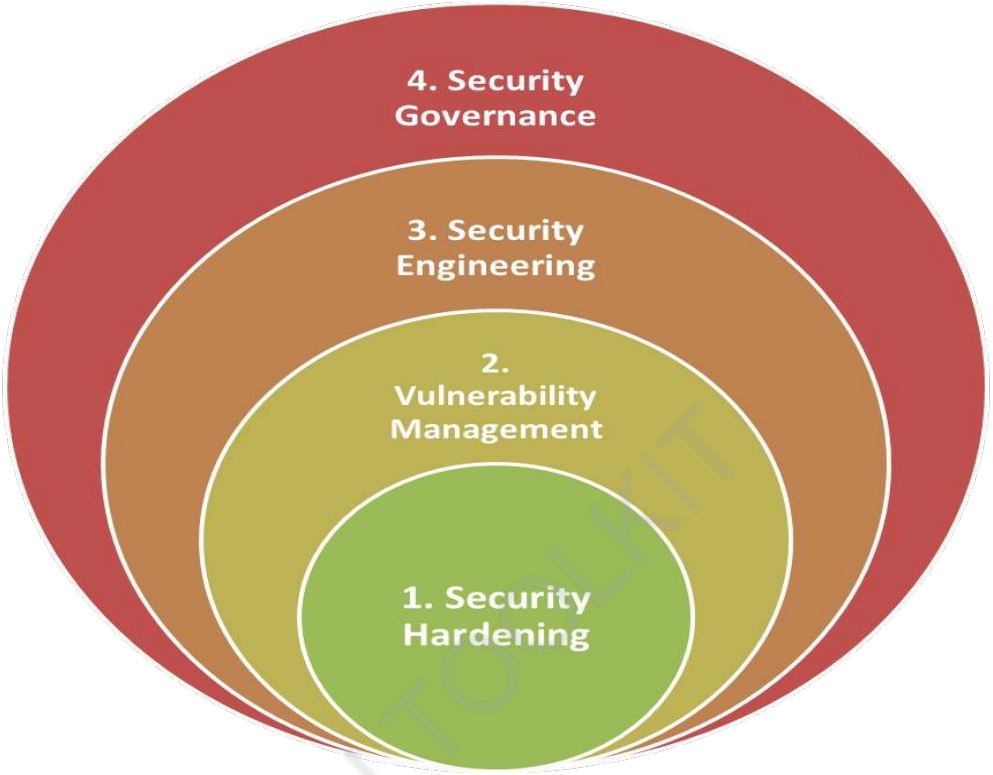
–Allocation of sufficient priority & resources

•Projects either fail or succeed before they begin !

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

Module: 55
Difference between security hardening and Patching

–Security Transformation Stage 1: Security Hardening Of IT Assets



•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”

•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)

•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

•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 required for customized instances•

•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

•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

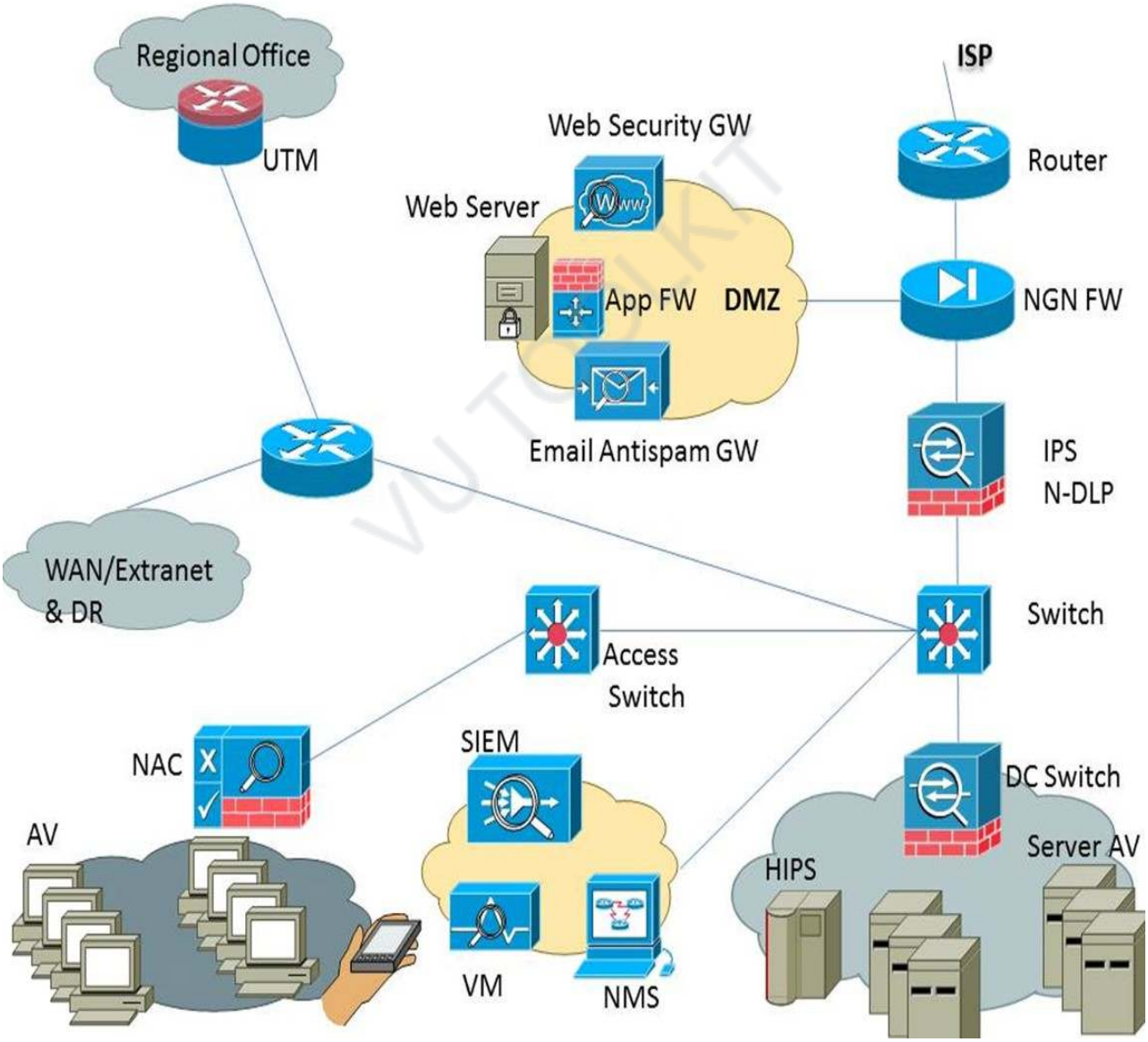
Module: 56
Security hardening strategies

•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

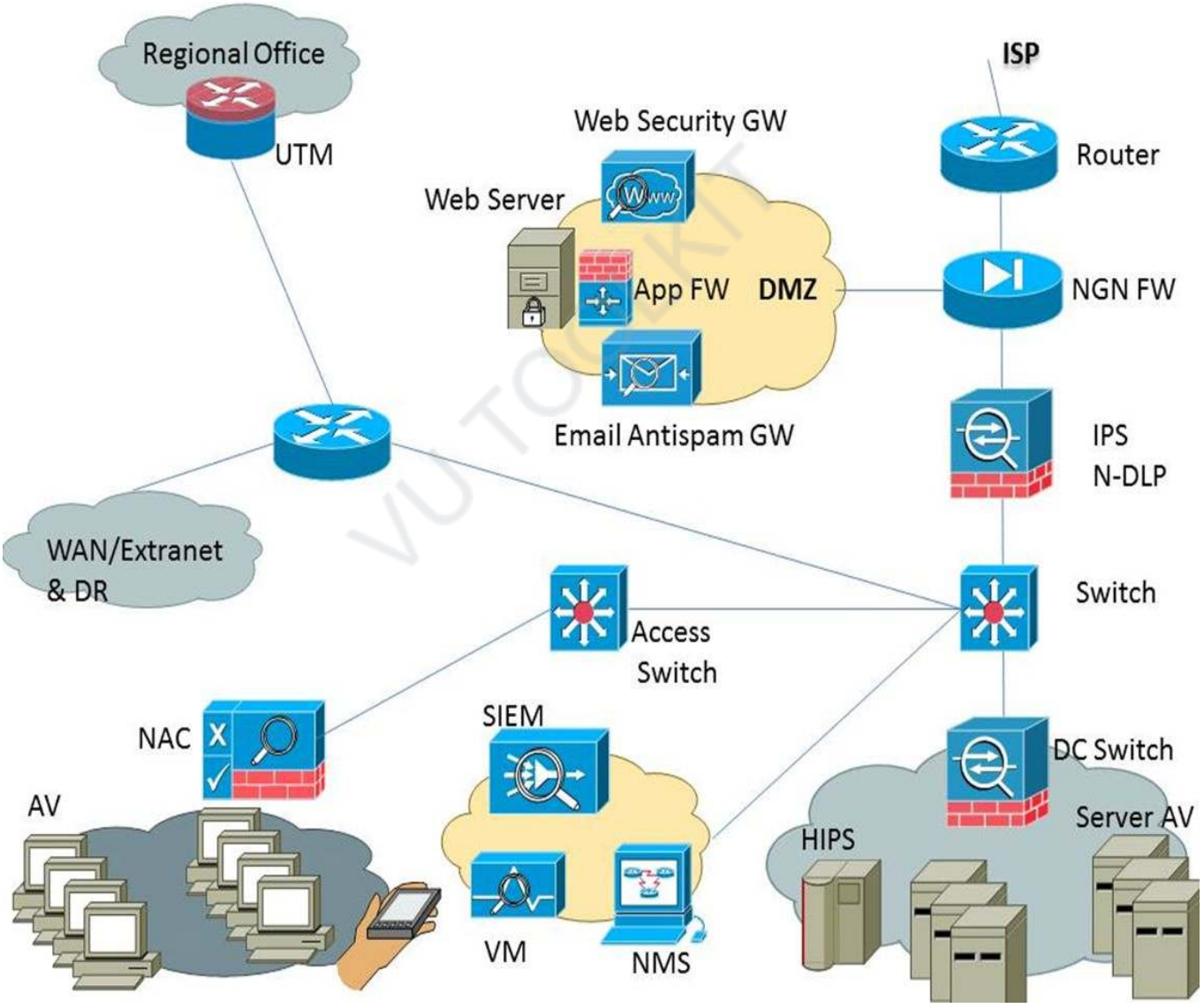


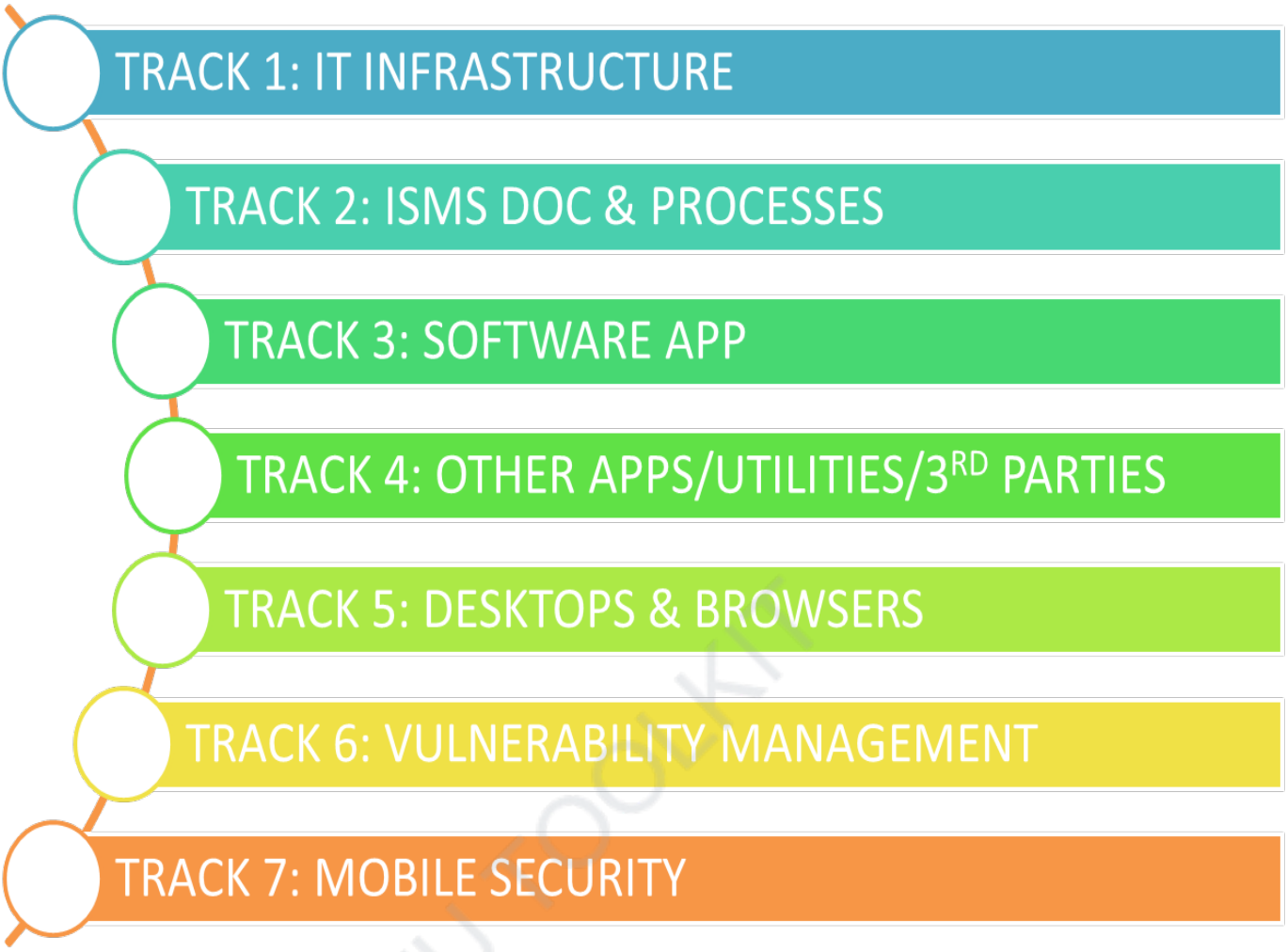
•Separate security engineering (Step 3) from security hardening (step 1)

•Security engineering requires more thorough working so will slow down the security implementation

•Do the low hanging fruit first (security hardening).

•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





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

Module: 57
Pre-requisites for the security hardening program

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

1.Security program approved

–Project director

–Timeline

–General project sequence and strategy

–Understanding of main players and roles

–Understanding of project structure

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

3.Project kick-off meeting held

–Project goals & mission

–All key stakeholders made aware of their roles

–Responsibilities & authority

–Success criteria & reporting mechanism

4.ISMC team identified and their loading for this project communicated

–ISMC plays a critical role

–Cooperation & teamwork

–Security leadership culture

–Clarity on goals

5.Appraisal linkage of core resources announced by CIO

–Broader team

–Announcement by CIO

Clarity on evaluation mechanism

Module: 58
Who will conduct security hardening?

•Involvement of various stakeholders for security hardening

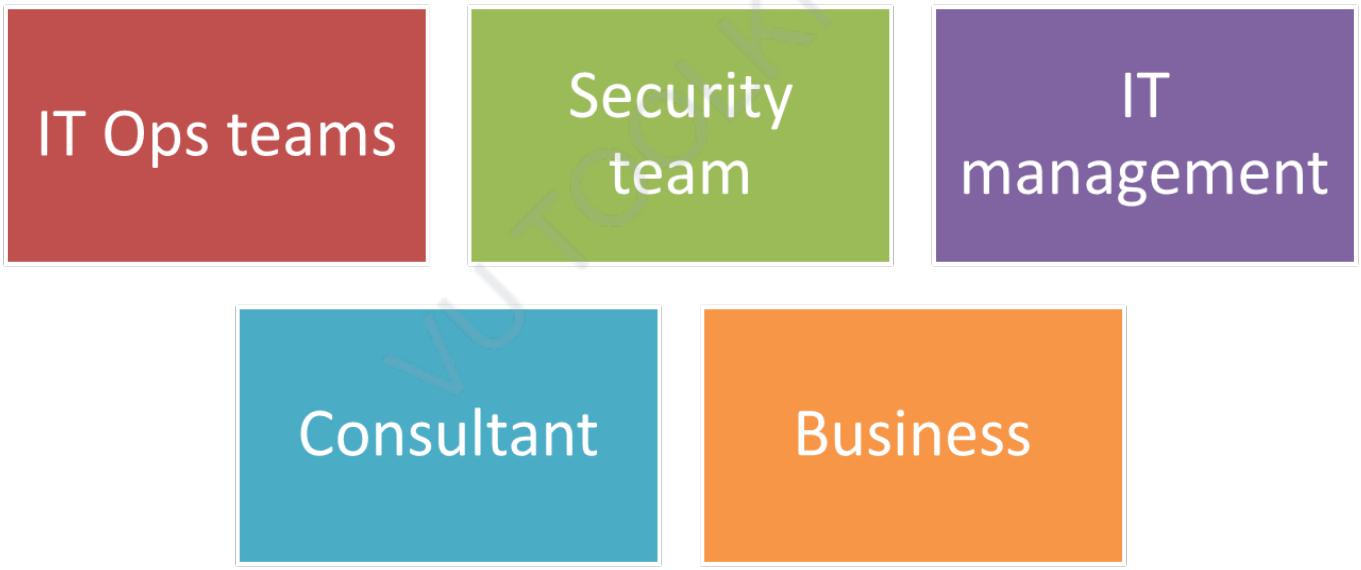
–Operations teams

–Security team

–IT management

–Consultant

Business



•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

•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

•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

•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

•Consultant or project director:

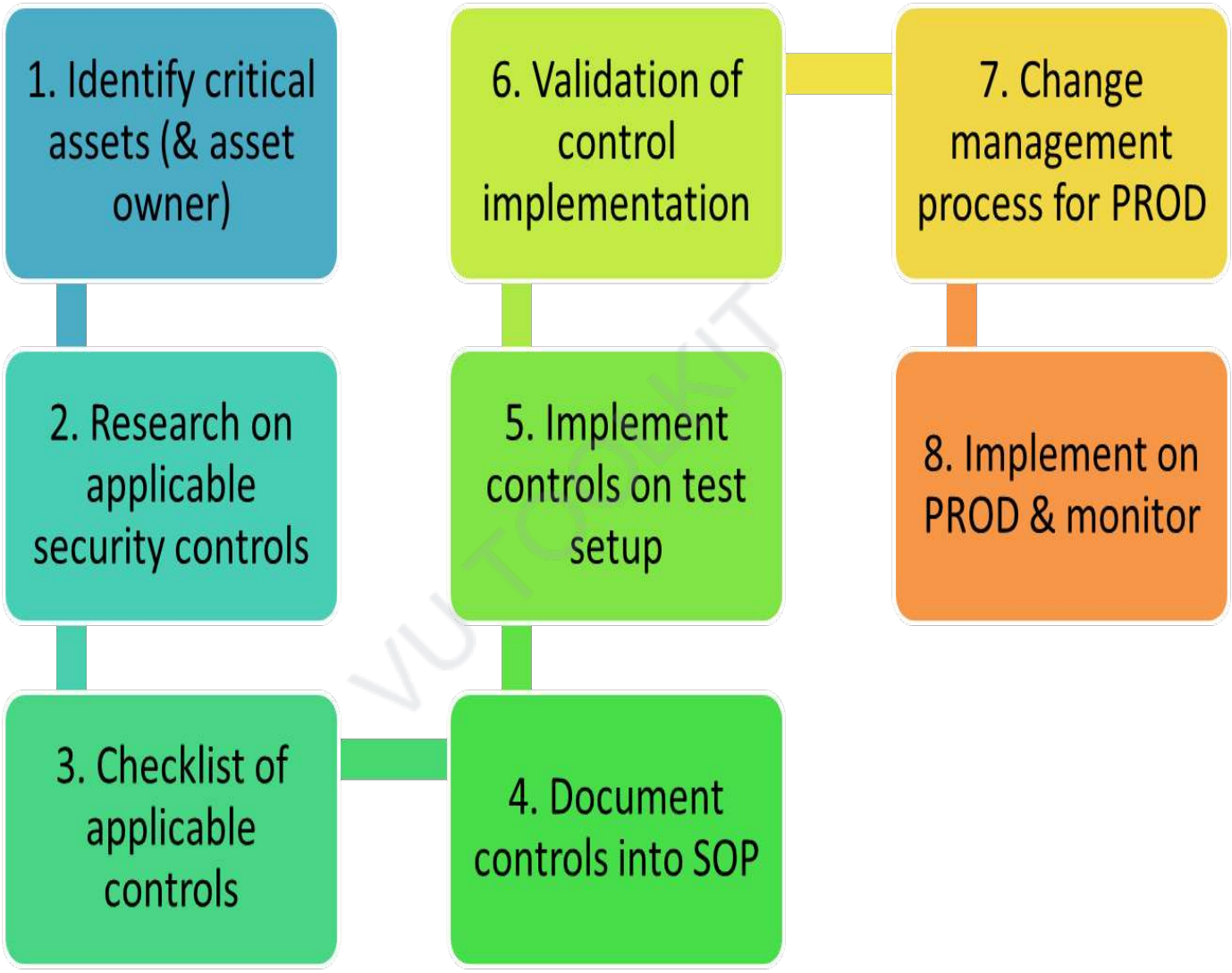
–Drives the security program

–Ensures that strategy is aligned with project objectives

–Ensures process and activities are moving at good momentum as per timeline

Module: 59
What is the 8-step methodology for security hardening?
Part- 1

•What is the 8 step security hardening methodology?



•Purpose:

–Many assets need to be hardened at various times, by various teams, for various requirements and projects

–Standardize and follow a consistent approach

•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

•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

ISMC	TEAM LEAD	IT OPS TEAM	INFOSEC TEAM
• DRIVES THE PROGRAM • DECISION MAKING • INCLUDES ALL 3-4 DOMAIN TEAM LEADS	• MEMBER OF ISMC • REPORTS TO HEAD OF THE DEPT	• TEAM THAT WILL IMPLEMENT THE SECURITY CONTROLS	• REPORTS TO CISO OR INFOSEC HEAD • OR LED BY CONSULTANT

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

•Let’s look at the steps in detail in the next module

Module: 60
What is the 8-step methodology for security hardening?
Part- 2

•Step 1: Identify Critical Assets & Asset Owner:

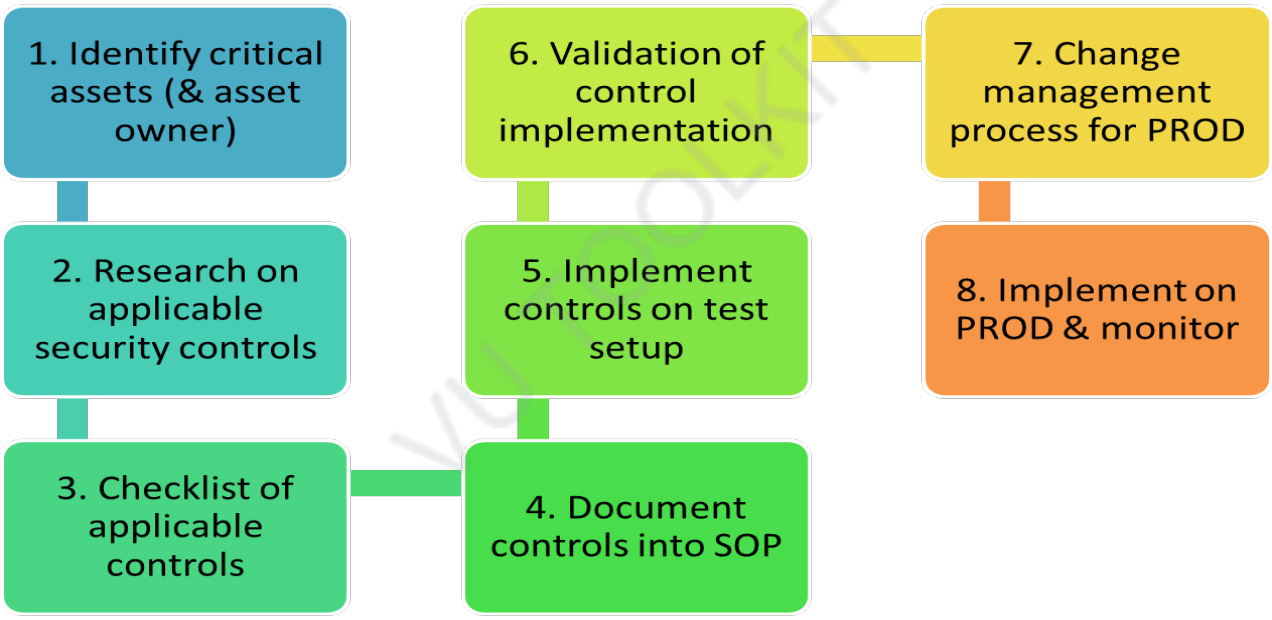
–Asset inventory & infrastructure diagram

–Examine risks

–Analyze assets at a high level and prioritize

–Minimum security baseline (MSB)

–Break into phases



•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

•Step 3: Checklist of applicable security controls

–Checklist for progress tracking

–Share with appropriate IT team

–Forms record for controls trail

•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

Module: 61
What is the 8-step methodology for security hardening?
Part-3

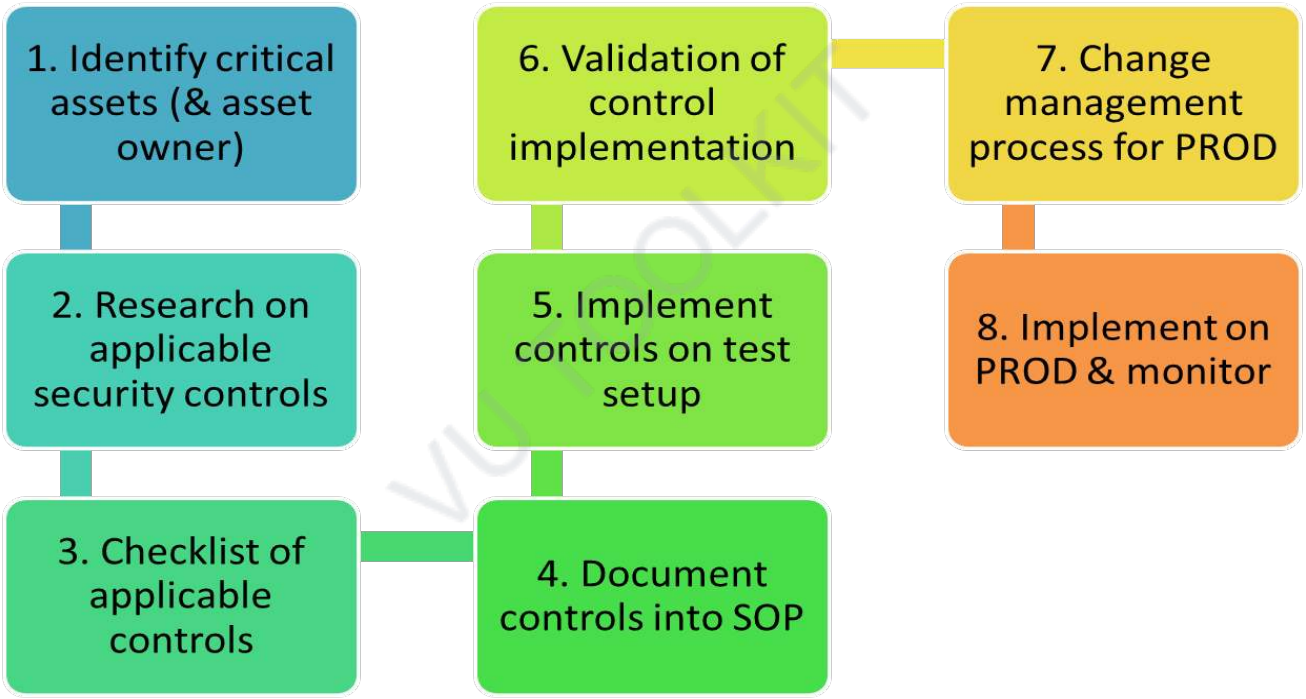
Step 5: Implement controls on test setup

–Relevant IT team to implement controls on test setup

–Update checklist

–Update SOP (if necessary)

–Send checklist back to InfoSec team



•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

•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

•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

Module: 62
A look at CIS security benchmark part - 1

Center for Internet Security (CIS)

–https://www.cisecurity.org/cis-benchmarks/

–Fill out your details and will receive an email with link

#	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**

#	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

#	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**

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

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

#	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

#	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**

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

Module: 63
A look at CIS security benchmark part - 2

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

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

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

#	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**

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

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

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

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

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

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

Module: 64
A look at CIS security benchmark part - 3

CIS Benchmarks example (Network Devices)

#	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**

CIS Cisco Firewall Benchmark

•Control content:

–Profile applicability (ASA 8.X, ASA 9.X)

–Description

–Rationale

–Audit

–Remediation

–Default value

References

•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.

•1.8 (page 88); Session Timeout

–Rationale: Limiting session timeout prevents unauthorized users from using abandoned sessions to perform malicious activities.

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.

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
```

•1.8 (page 88); Session Timeout

–Default Value: The default timeout is 0, which means the console session will not time out

•1.8 (page 88); Session Timeout

–Reference: CLI Book 1: Cisco ASA Series General Operations CLI Configuration Guide, 9.1

Module: 65
A look at CIS security benchmark part - 4

CIS Benchmarks example (Operating Systems)

–MS Windows Server 2012-R2

#	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**

CIS Microsoft Windows Server 2012 R2 Benchmark

•Profile applicability:

–Level 1 domain controller

–Level 1 member server

–**Level 2 domain controller**

–**Level 2 member server**

•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

•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

•Control content:

–Profile applicability (ASA 8.X, ASA 9.X)

–Description

–Rationale

–Audit

–Remediation

–**Impact**

–Default value

–References

•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*

•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.

•1.1.2 [L1] Audit:

–Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed.

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
```

•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)

Module: 66
A look at DISA security technical implement guides (STIGs) – part - 1

•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

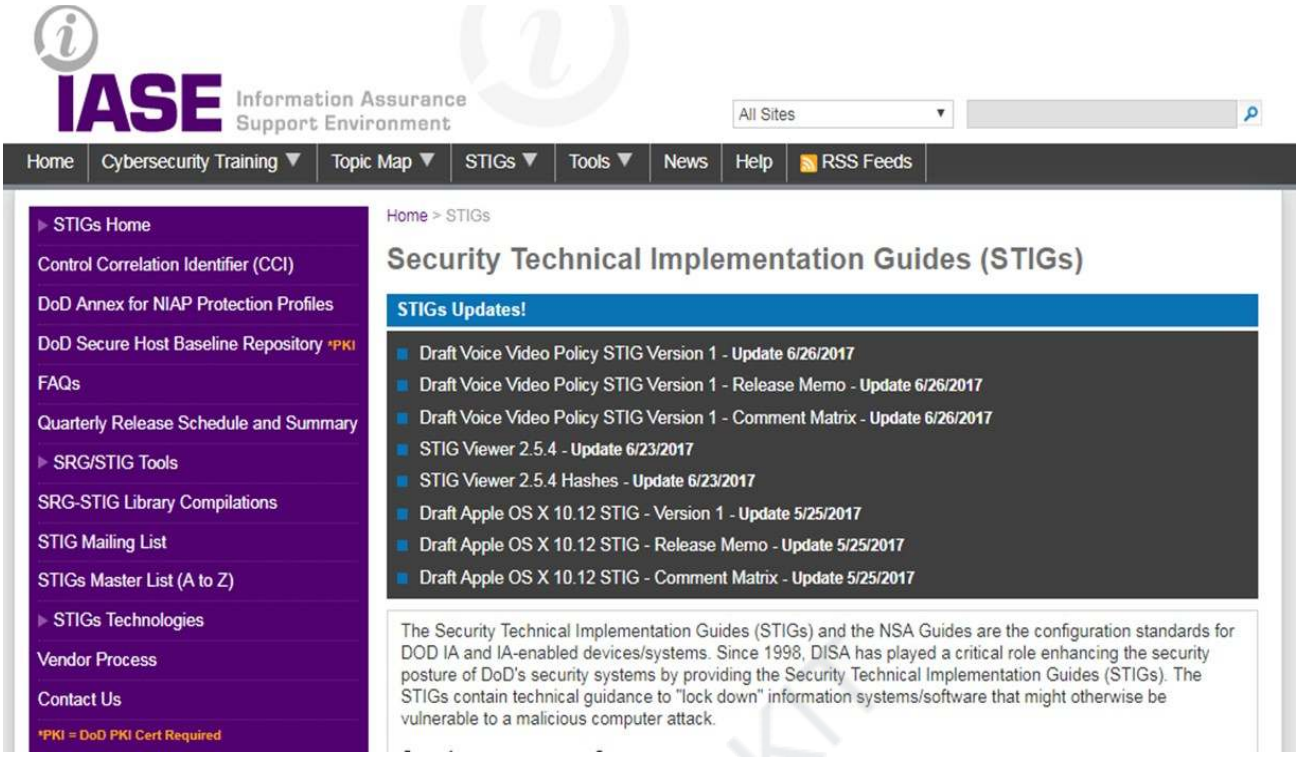
425 STIGs available

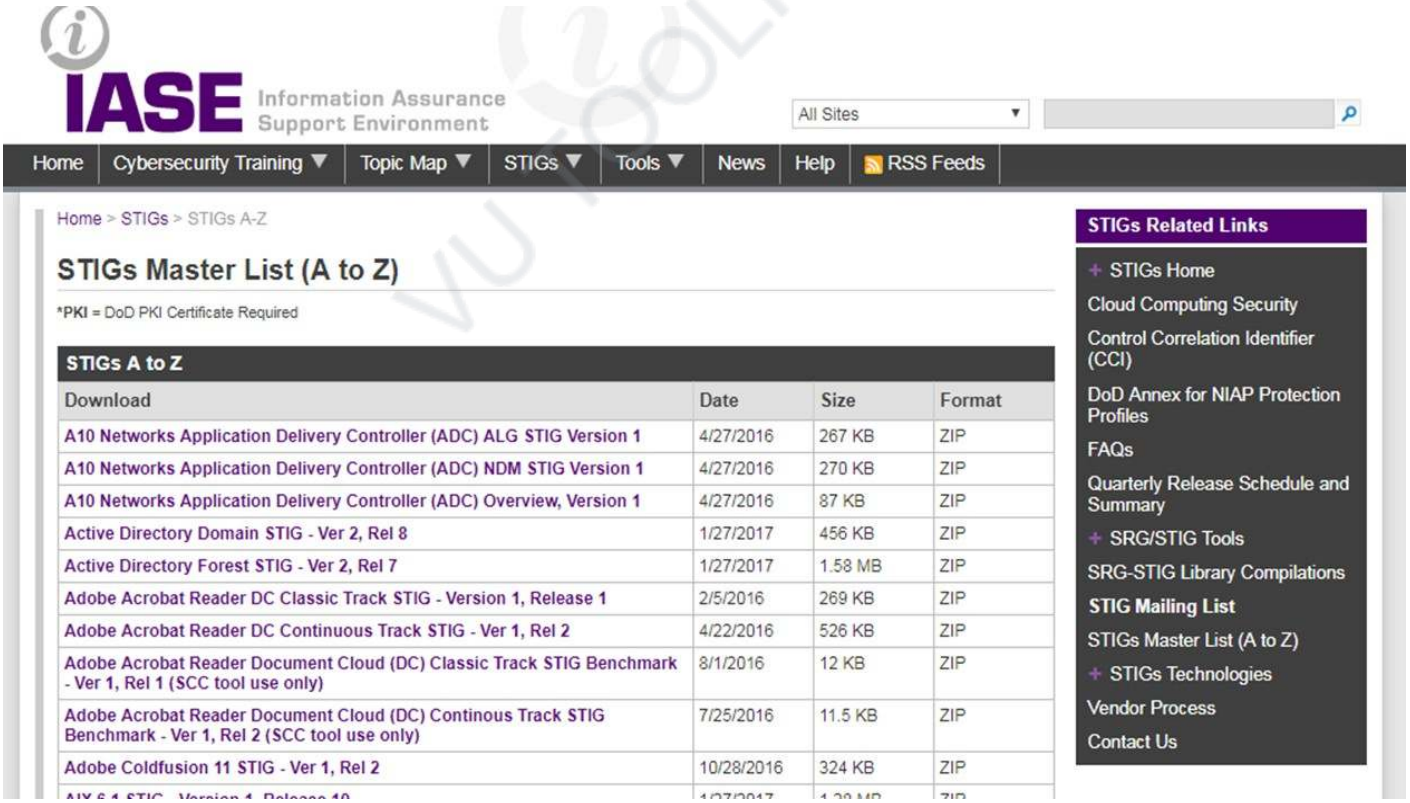
•STIGs master list (A-Z):

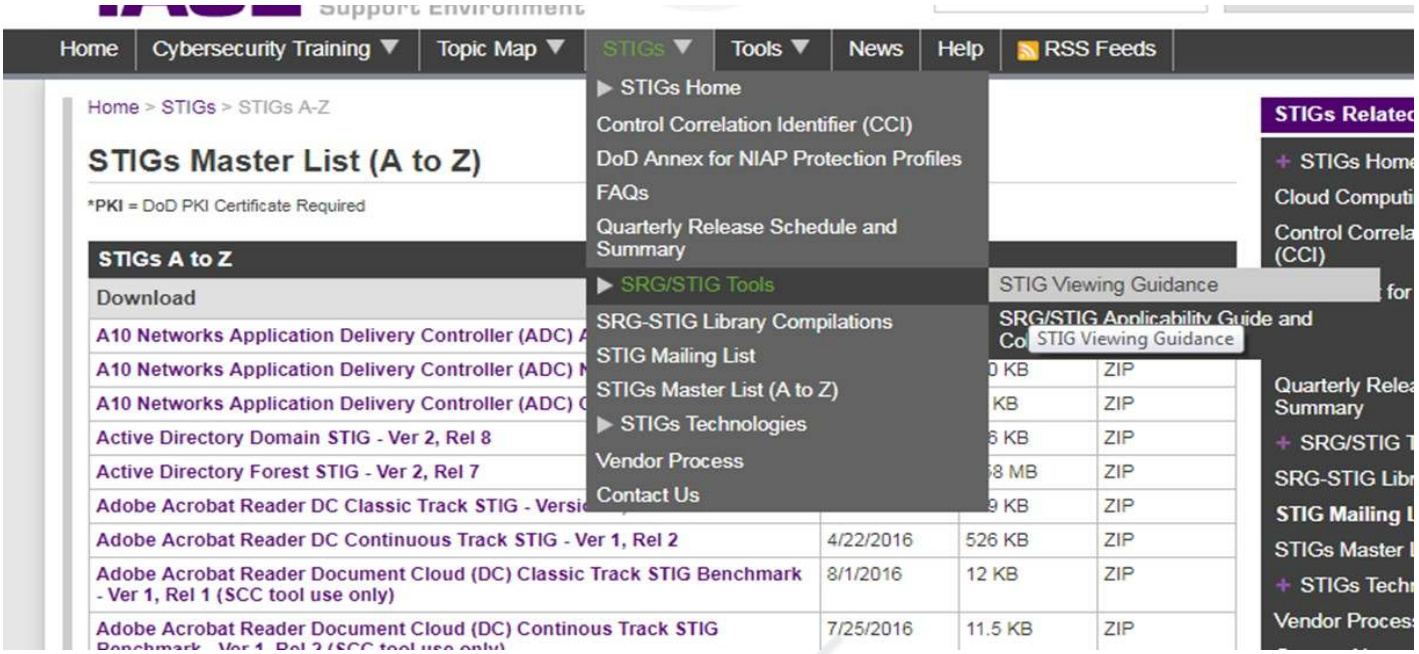
–http://iase.disa.mil/stigs/Pages/a-z.aspx

•STIG viewer:

–http://iase.disa.mil/stigs/Pages/stig-viewing-guidance.aspx







STIG Viewing Guidance

*PKI = DoD PKI Certificate Required

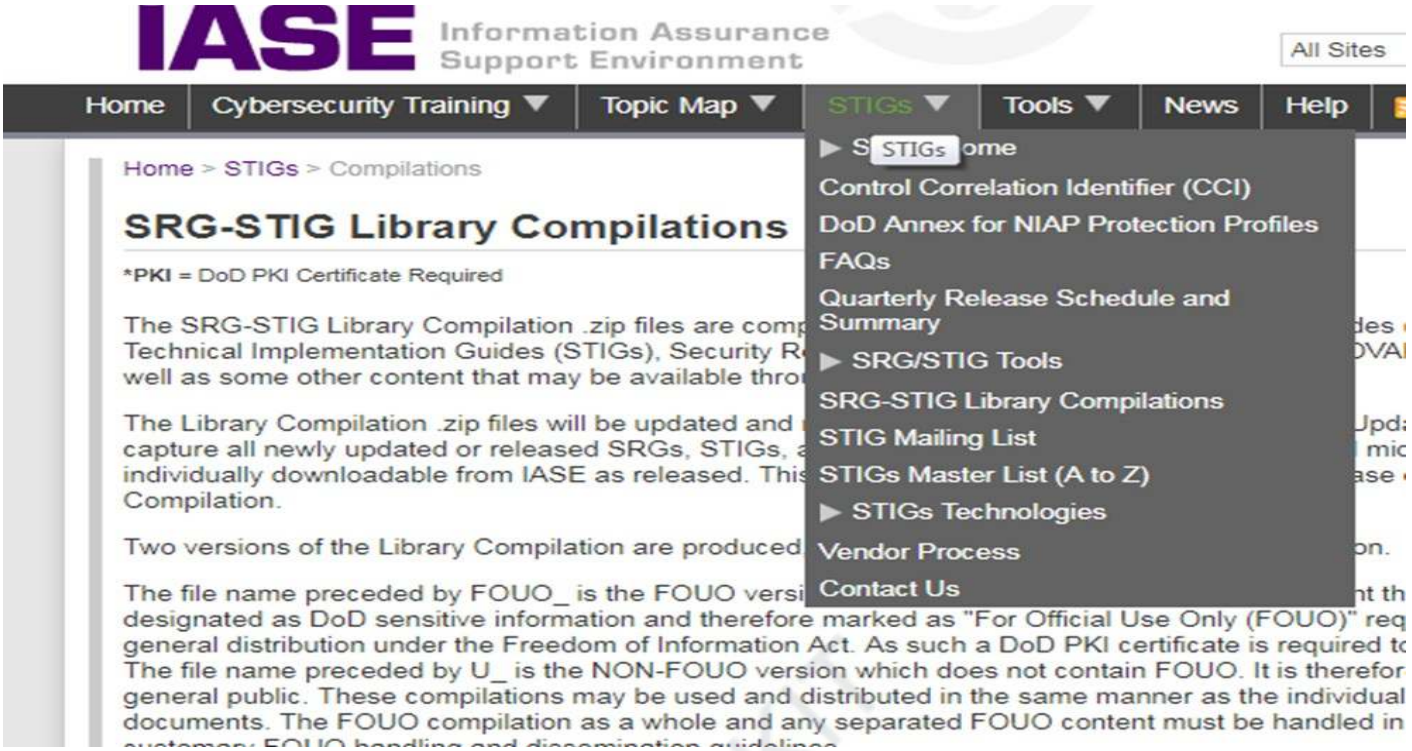
XCCDF formatted SRGs and STIGs are intended be ingested into an SCAP validated tool for use in validating compli of a Target of Evaluation (TOE). As such, getting to the content of a XCCDF formatted STIG to read and understand t content is not as easy as opening a .doc or .pdf file and reading it. The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

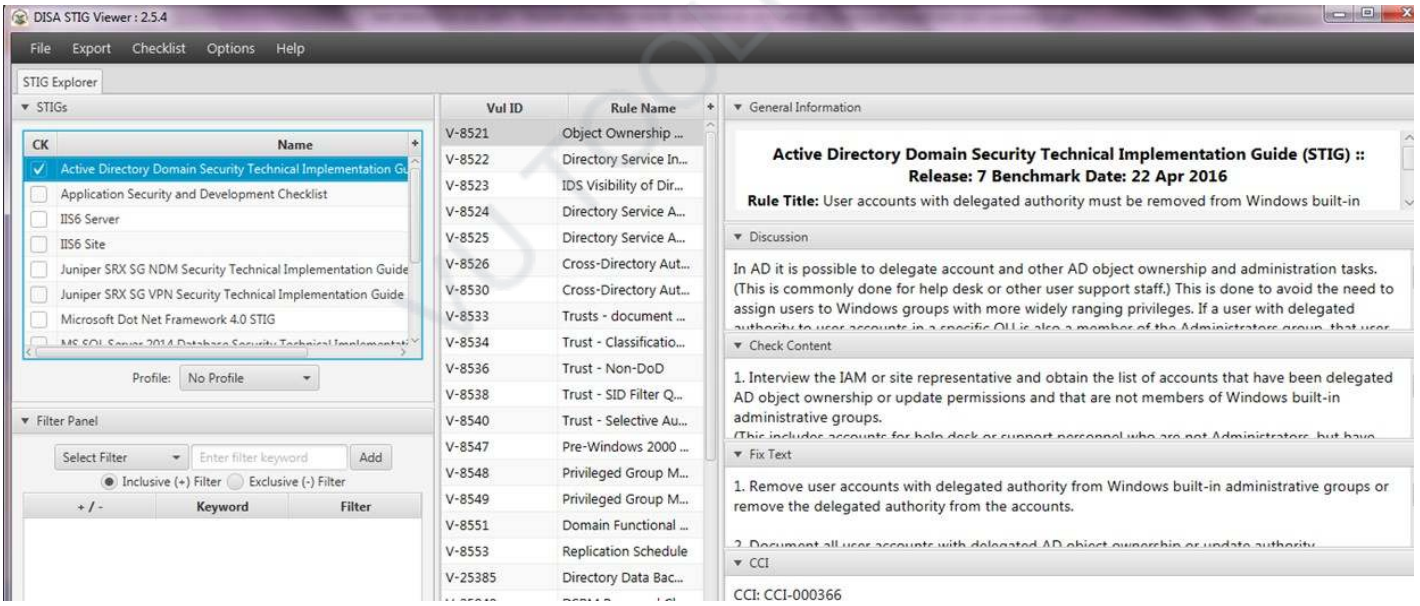
How to View SRGs and STIGs

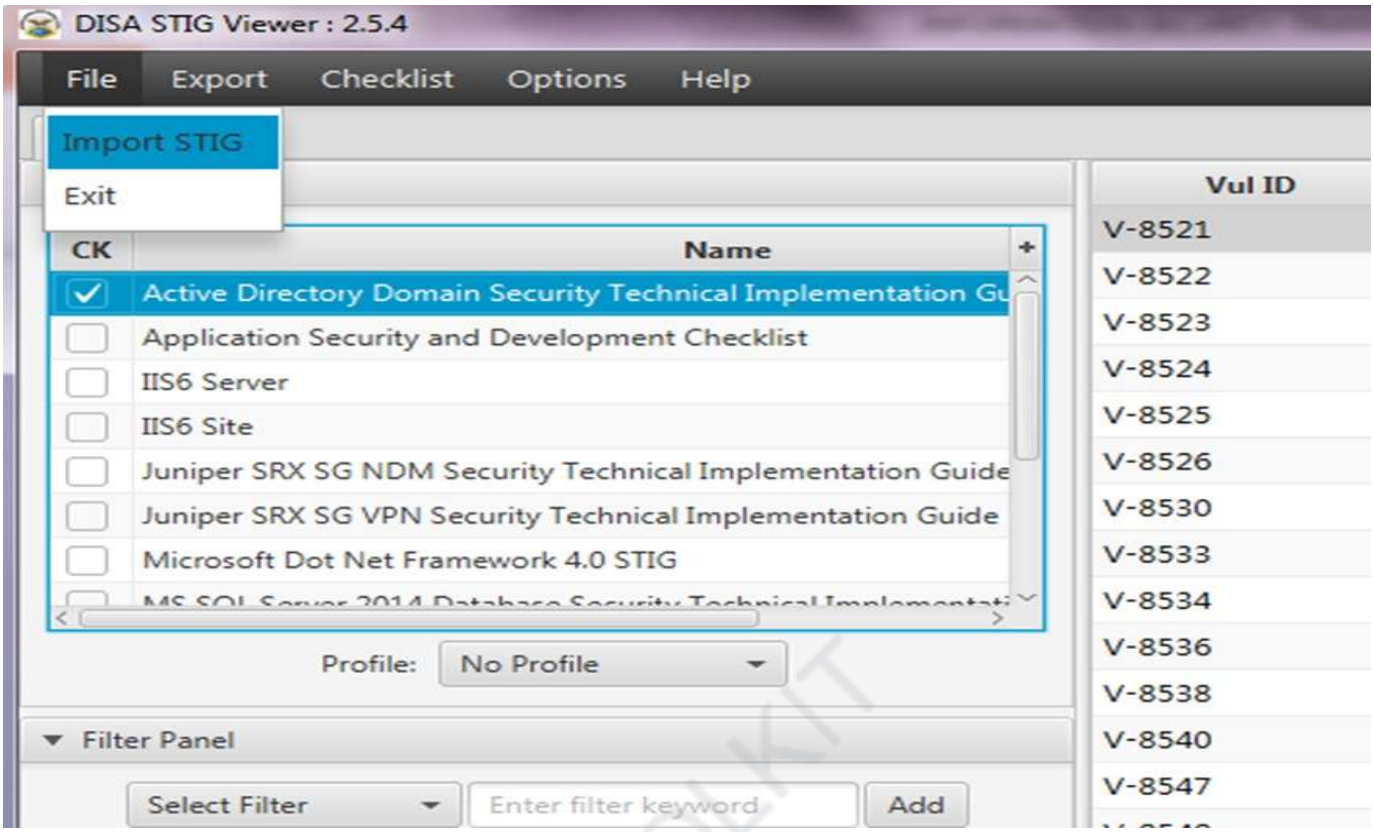
Download	Date	Size	Format
How to View SRGs and STIGs	8/29/2016	80 KB	DOCX

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







- Completely different mechanism for DISA STIGs

Module: 67
A look at DISA security technical implement guides (STIGs) – part – 2

•STIG content:

–General information (title)

–Discussion

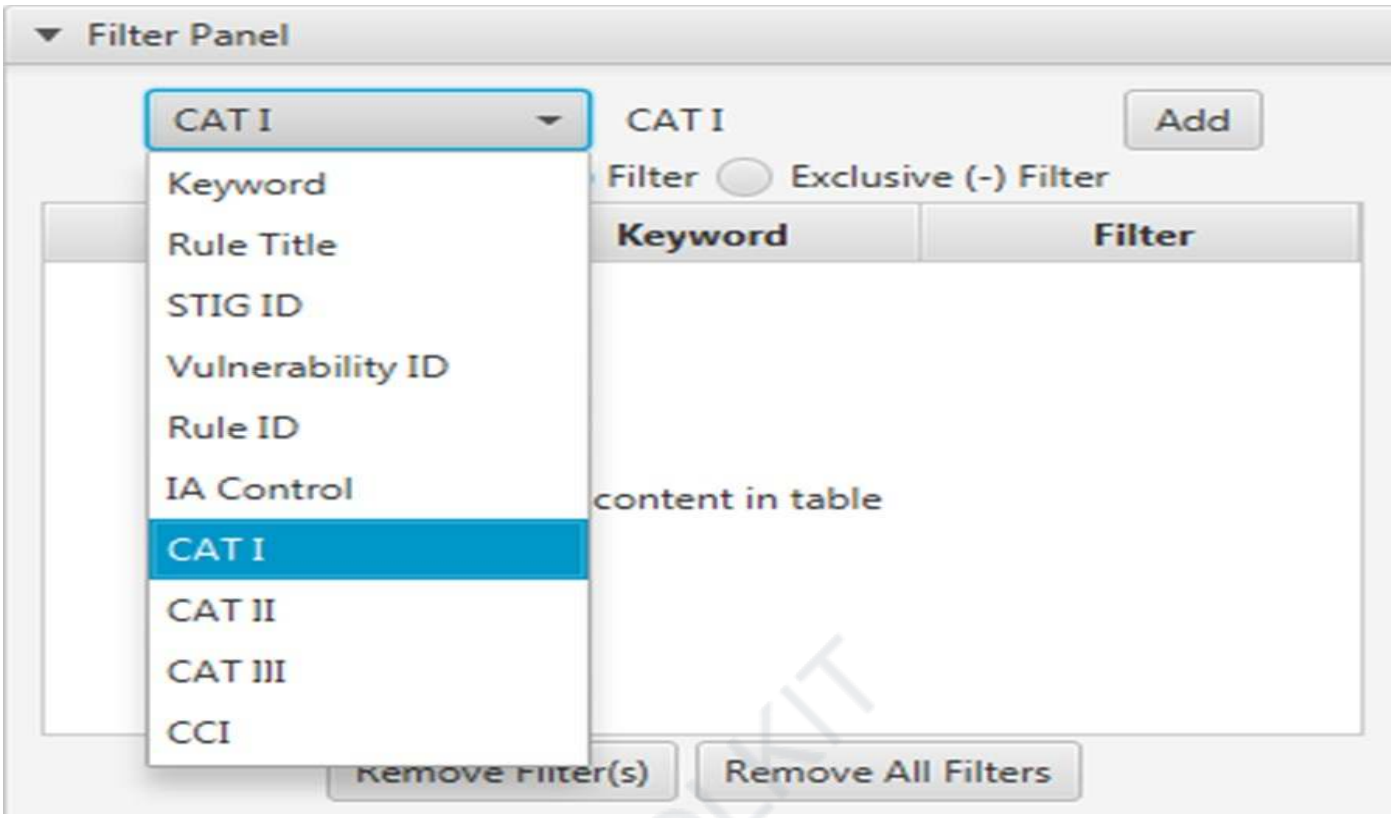
–Check content

–Fix text

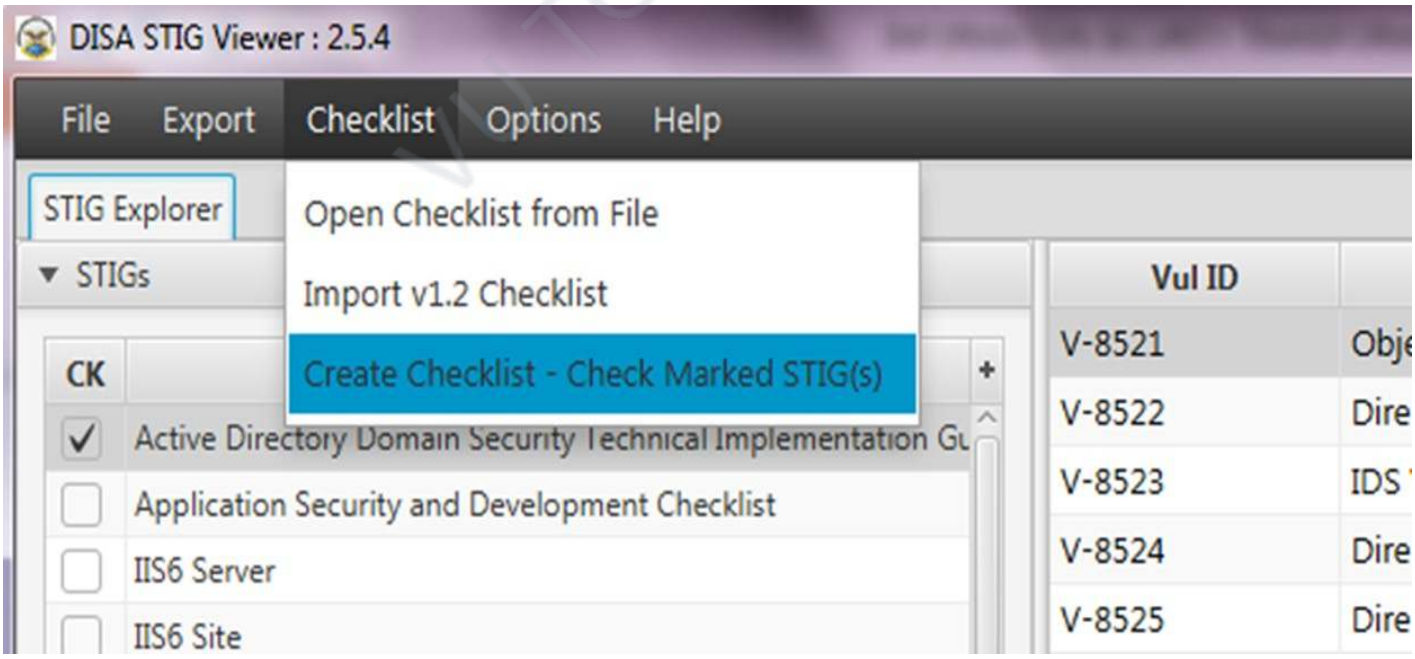
–CCI (References)

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

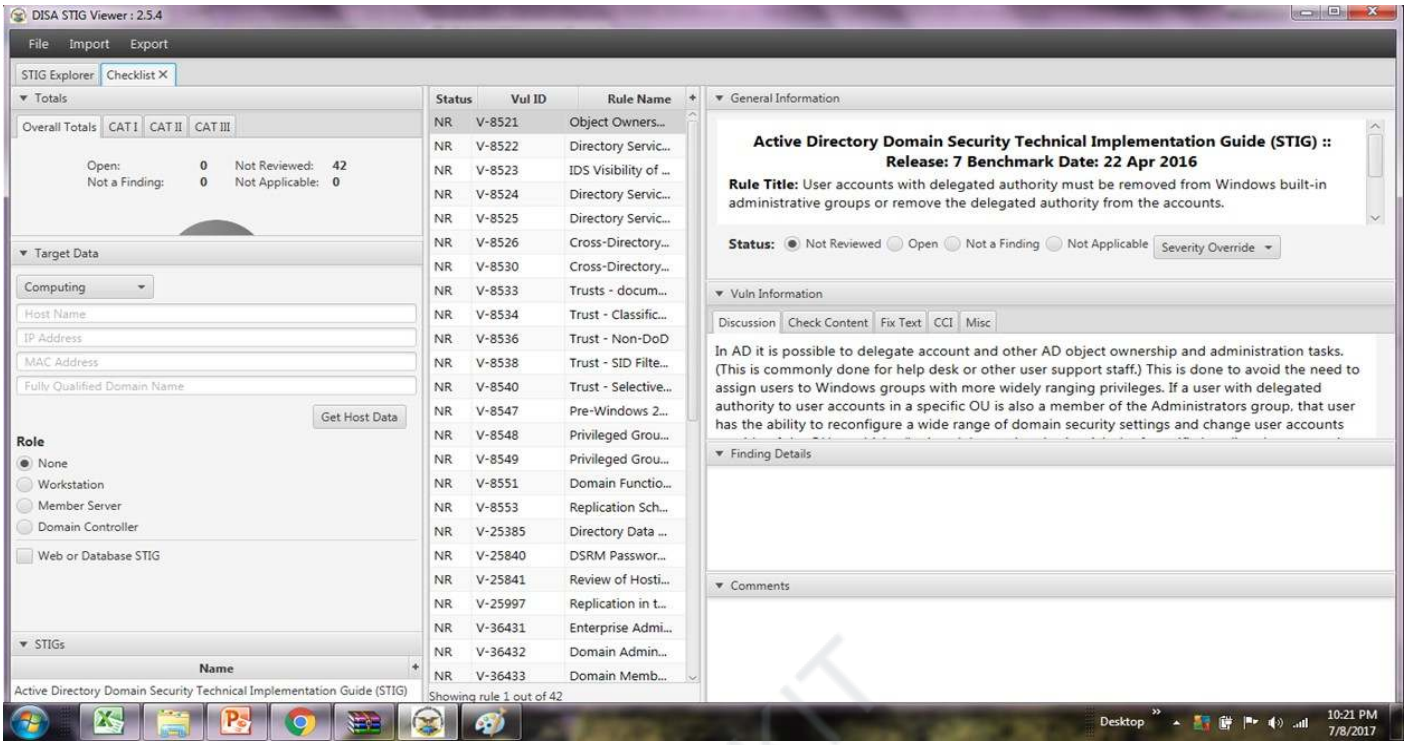
FILTER PANEL



CREATE CHECKLIST



CHECKLIST



•Checklist screens:

–Overall totals

–Target data

–Role

–Finding details

–Comments

•Checklist screens (STATUS):

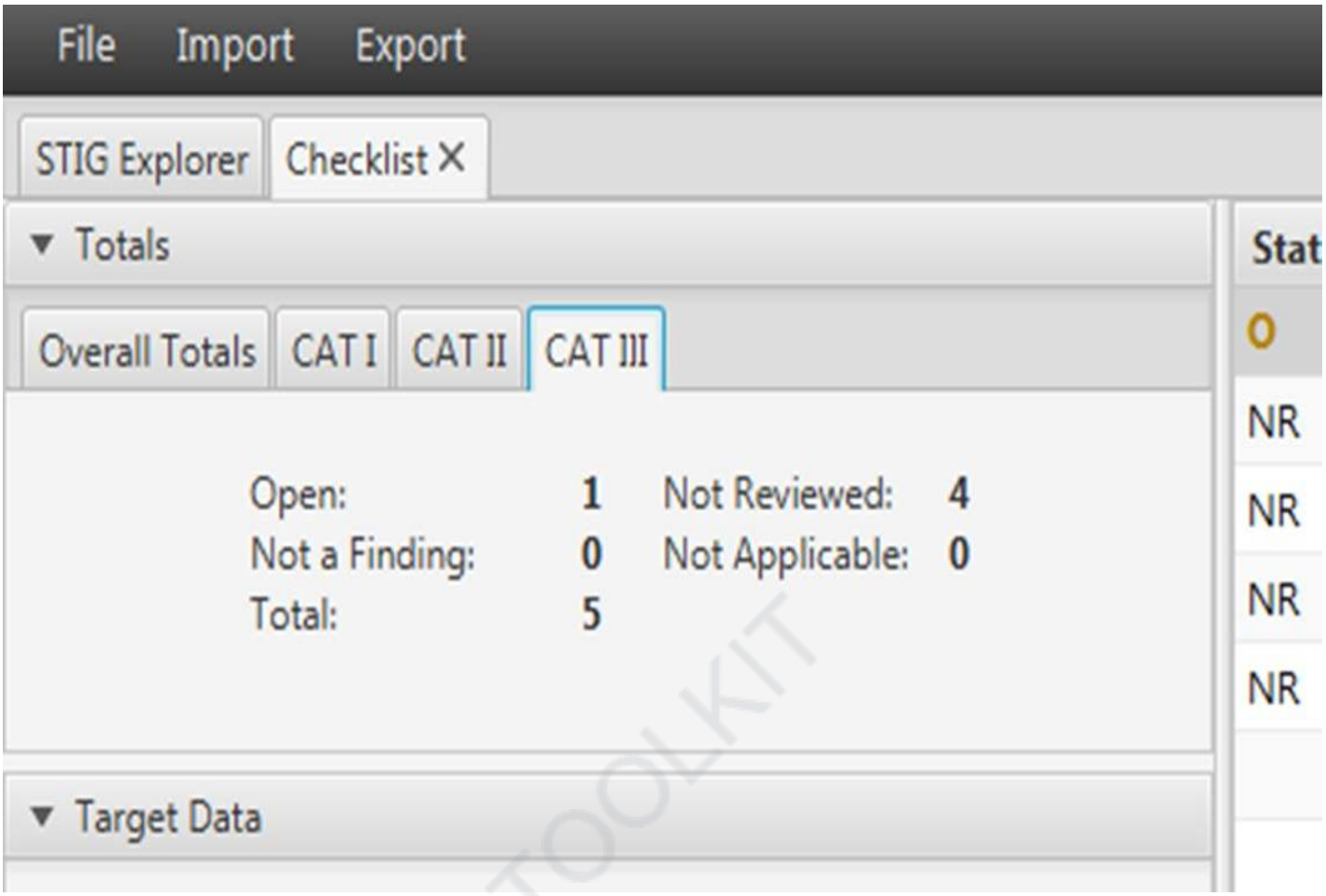
–Not reviewed

–Open

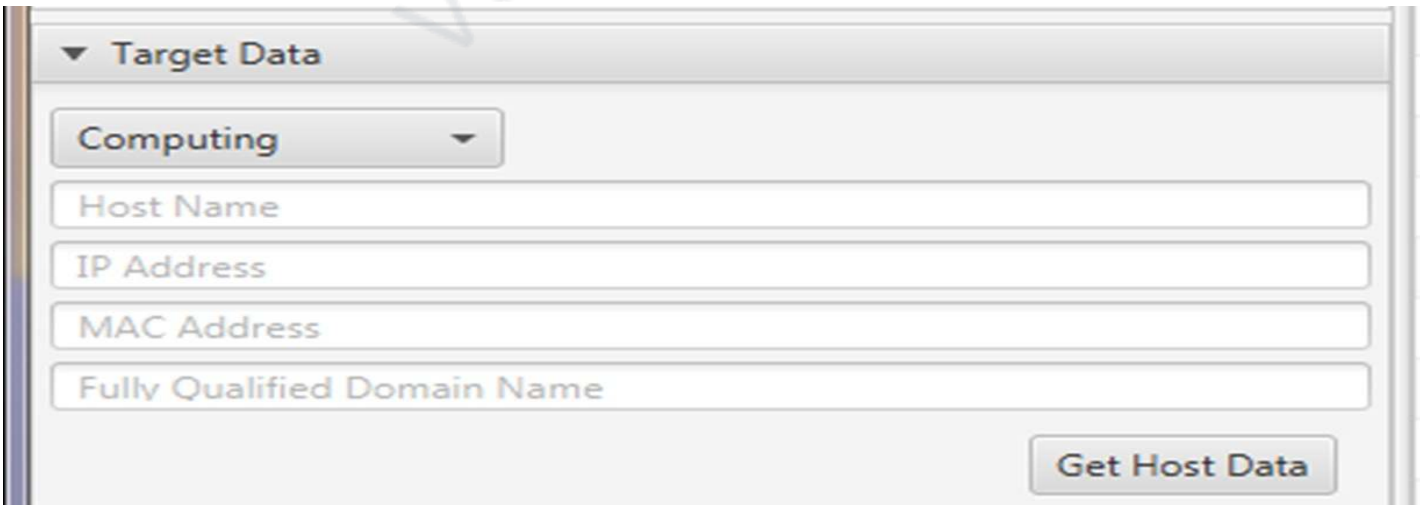
–Not a finding

–Not applicable

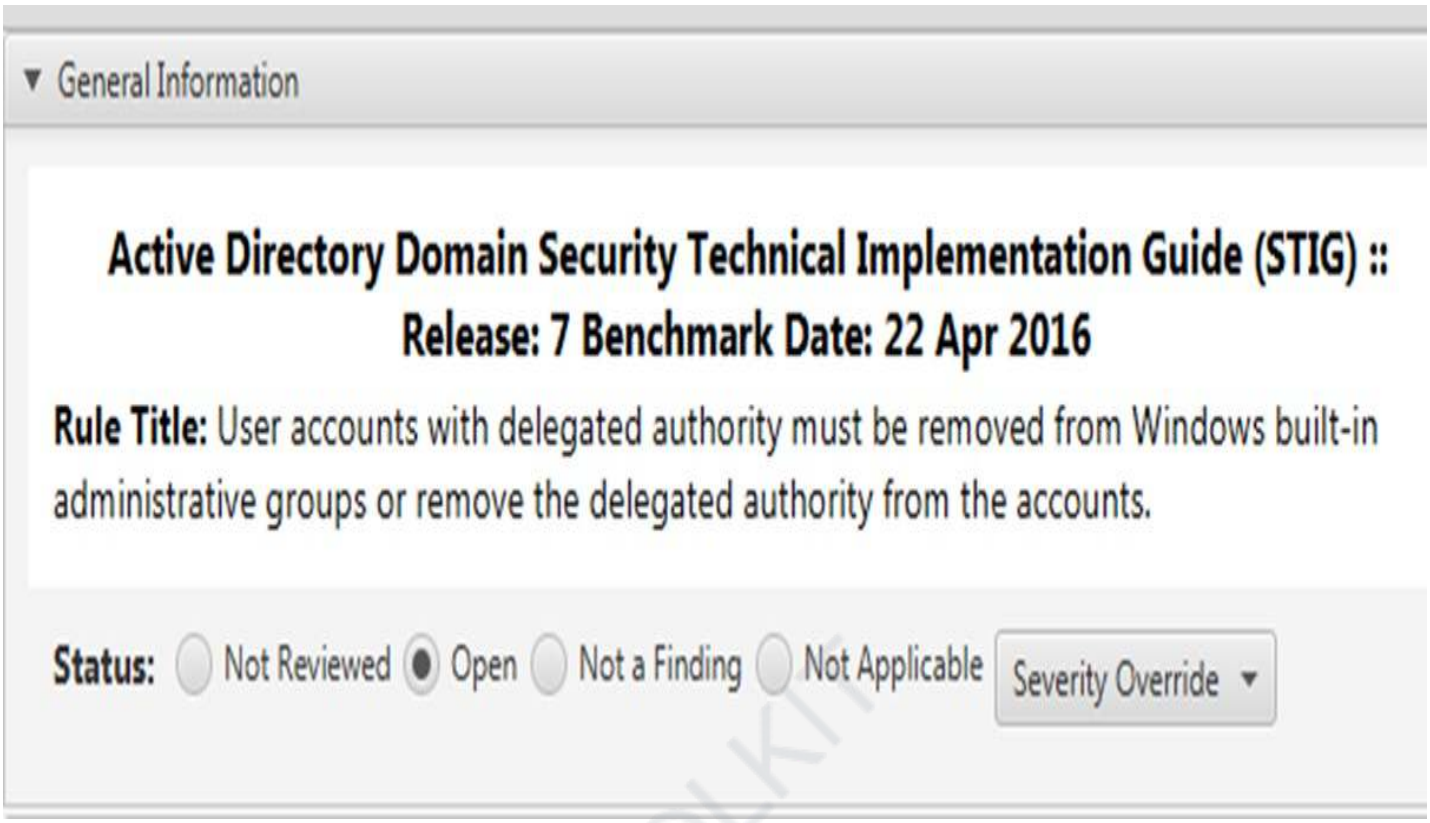
Totals



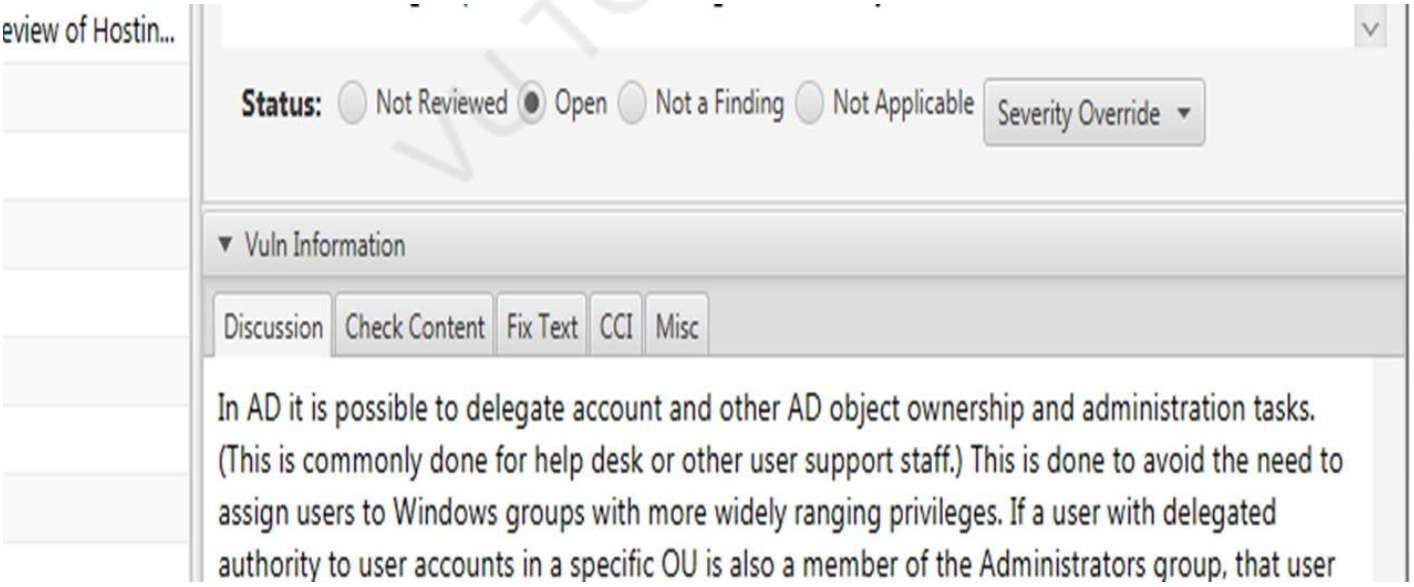
Target Data



Status



Vuln Information

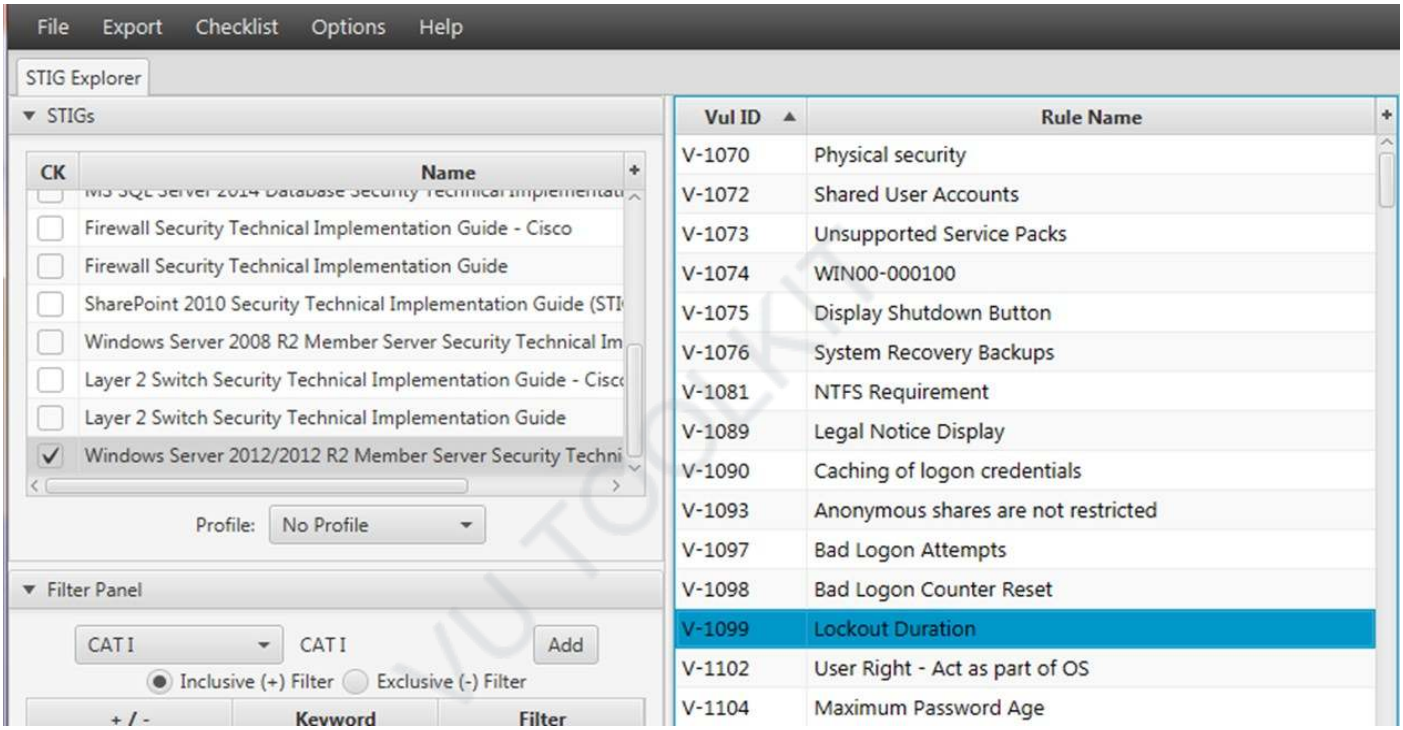


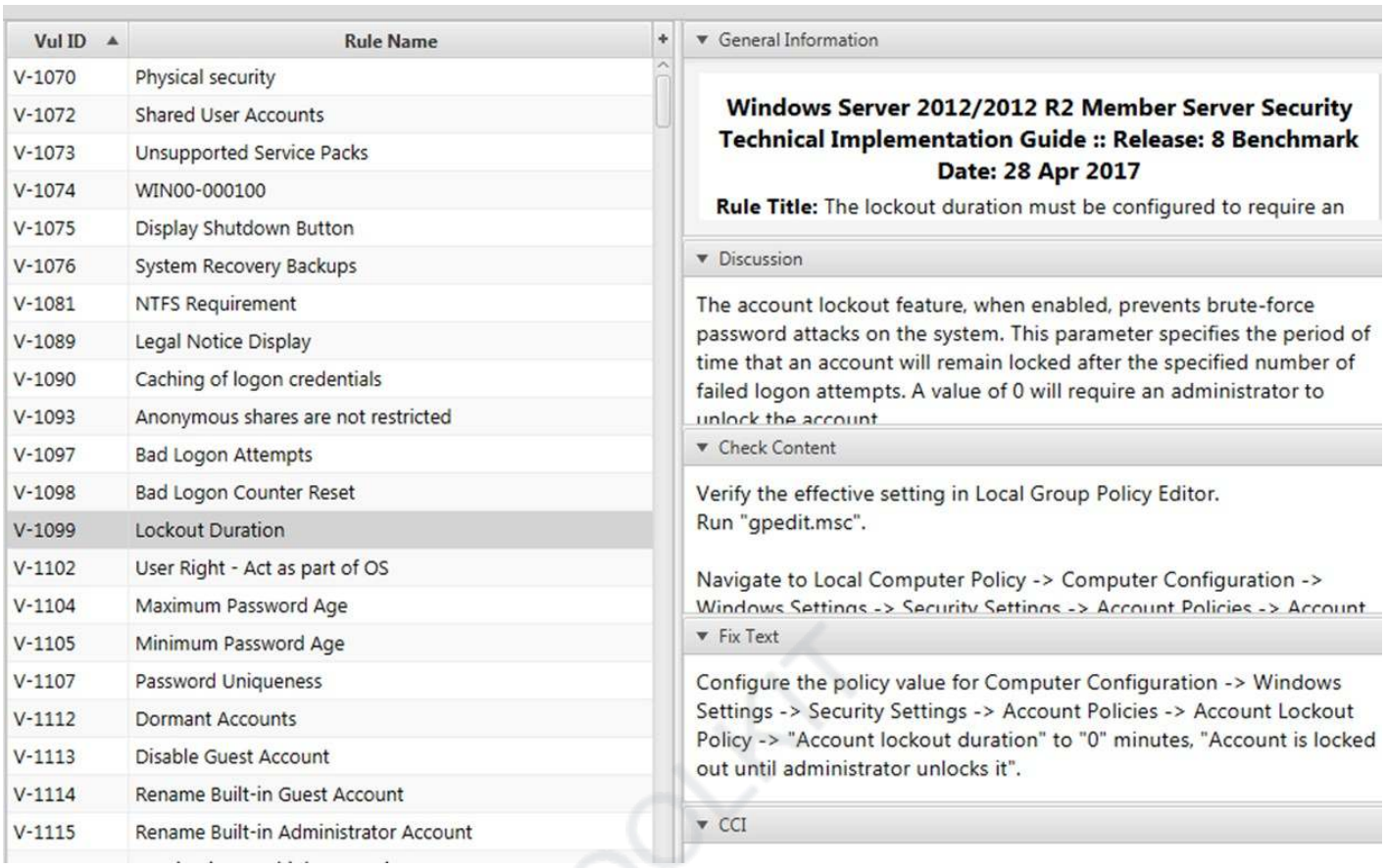
Module: 68
A look at DISA security technical implement guides (STIGs) – part - 3

•Windows Server 2012 R2 Member Server

–Import STIG

–V1099 (Lockout duration)





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
V-1105	Minimum Password Age
V-1107	Password Uniqueness
V-1112	Dormant Accounts
V-1113	Disable Guest Account
V-1114	Rename Built-in Guest Account
V-1115	Rename Built-in Administrator Account

- **Rule Title:**

–The lockout duration must be configured to require an administrator to unlock an account

–Severity: CAT II

- **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

- **Discussion…:**

–of failed login attempts. A value of 0 will require an administrator to unlock the account.

•**Check Content:**

–Verify the effective setting in Local Group Policy Editor.

Run "gpedit.msc".

•**Check Content:**

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

•**Check Content…:**

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

•**Fix Text:**

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

•Fix Text….:

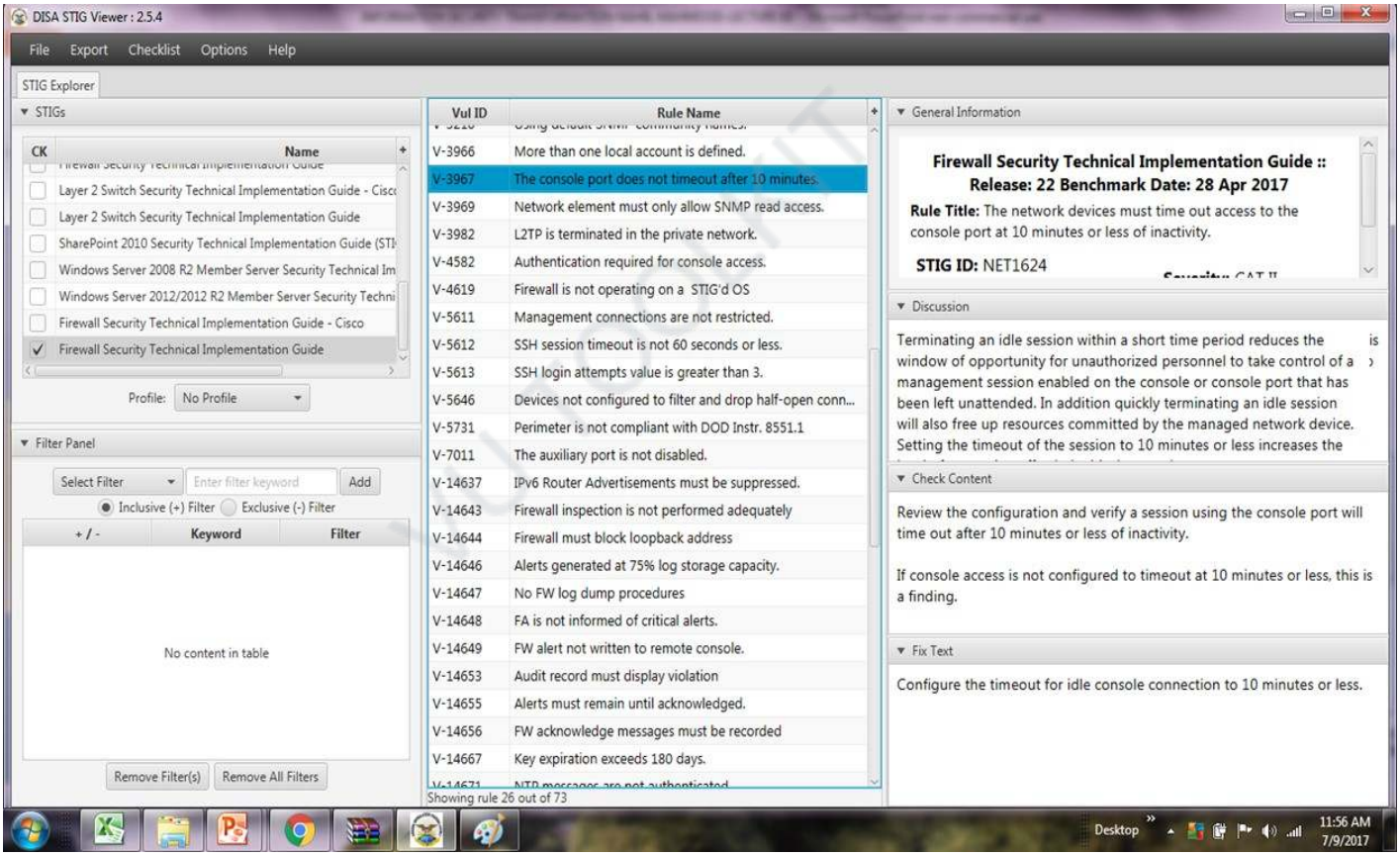
–"Account is locked out until administrator unlocks it".

•CCI: NIST SP 800-53 Revision 4 :: AC-7 b

Module: 69
A look at DISA security technical implement guides (STIGs) – part - 4

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

STIGVIEWER WINDOW



- **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

- **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…

- **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

- **Discussion…:**

–or less increases the level of protection afforded critical network components

- **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.

- Fix Text:

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

Module: 70
Comparison of CIS security benchmarks versus DISA STIGs

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

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)

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

- How to select CIS/DISA:

–Size of organization

–IT infrastructure extent

–Nature of business

–Security program goals

–Maturity of IT & security staff

- **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

Module: 71
Case study – Security hardening – Windows server 2012 R2

Security Hardening – Windows Server 2012 R2

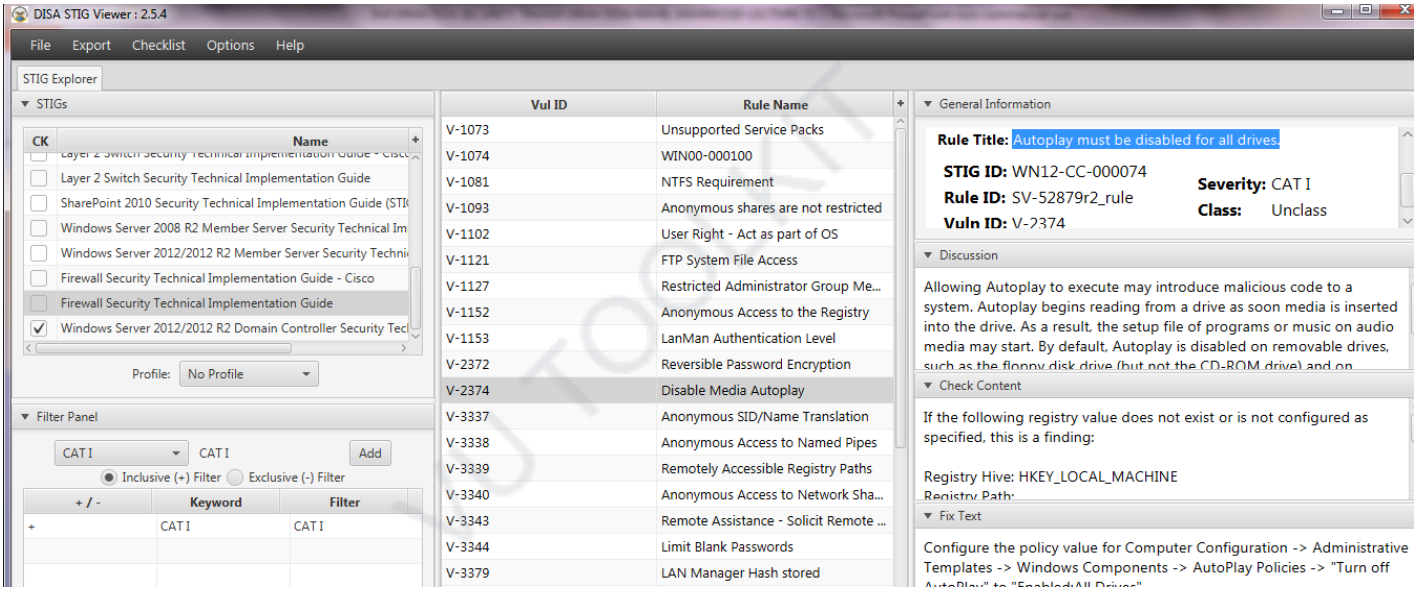
Windows Server 2012 – R2

DISA, Release 8

28 April 2017

Domain Controller

STIGVIEWER WINDOW



General Information:

Rule Title: Autoplay must be disabled for all drives

STIG ID: WN12-CC-000074

Severity: CAT I

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 network drives. Enabling this policy disables Autoplay on all drives....

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\Microsoft\Windows\CurrentVersion\policies\Explorer\

Value Name: NoDriveTypeAutoRun

Type: REG_DWORD
Value: 0x000000ff (255)

Fix Text:

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

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

Module: 72
case study – security hardening – Linux server

Case Study Security Hardening – Linux

- January 31, 2017
- 347 pages PDF doc

5.2.2 (page 258); Ensure SSH Protocol is set to 2 (Scored)

Profile applicability:

Level 1, Server

Level 1, Workstation

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.

Rationale: SSH v1 suffers from insecurities that do not affect SSH v2.

Audit: Run the following command and verify that output matches:

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

Remediation: Edit the /etc/ssh/sshd_config file to set the parameter as follows:

Protocol 2

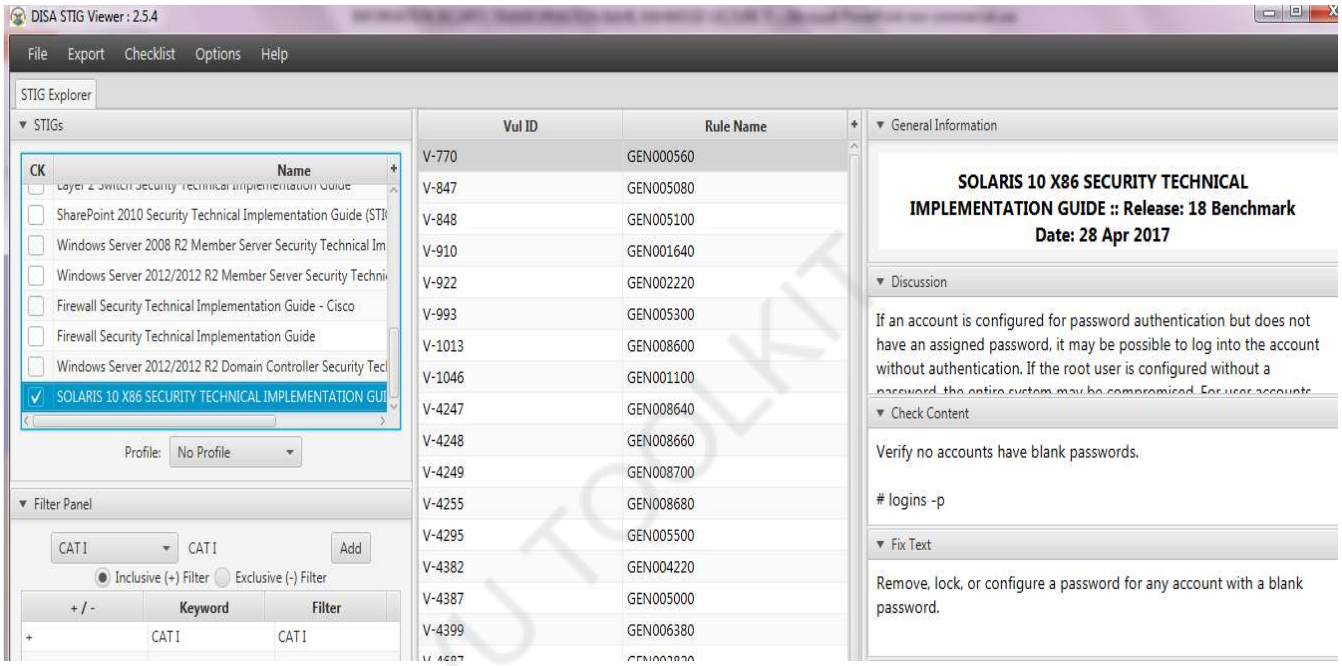
Critical Controls: 3.4

- Use Only Secure Channels For Remote System Administration
- 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
- should only be used if they are performed over a secondary encryption channel, such as SSL, TLS or IPSEC.

Module: 73
case study – security hardening – Solaris server

Security Hardening – Case Study – Solaris

STIGVIEWER WINDOW



General Information:

Rule Title: All shell files must have mode 0755 or less permissive

STIG ID: GEN002220

Severity: CAT I

Discussion:

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

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

If a shell has a mode more permissive than 0755, this is a finding
Fix Text:

Change the mode of the shell
chmod 0755 <shell>

CCI (Control Correlation Identifier):

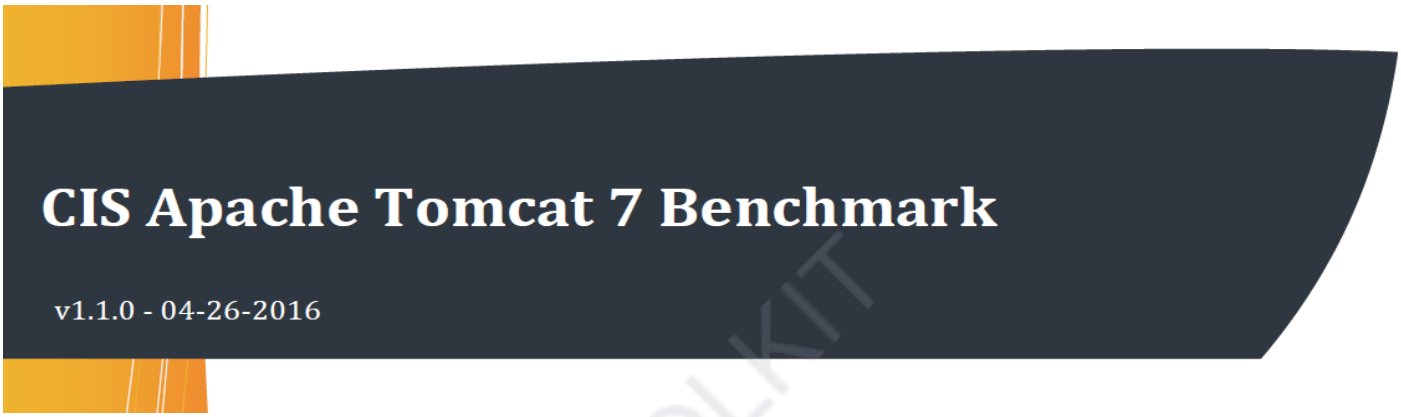
CCI-000225
The organization employs the concept of least privilege, allowing only authorized accesses for users (and processes acting on behalf of users) which are necessary to accomplish assigned tasks in accordance with organizational missions and business functions

NIST SP 800-53 :: AC-6
NIST SP 800-53A :: AC-6.1
NIST SP 800-53 Revision 4 :: AC-6

Module: 74
case study – security hardening – Apache server

Case Study Security Hardening – Apache

CIS Benchmarks case study (Apache Tomcat 7)



April 26, 2016

94 pages PDF doc

7.7 (page 65); Configure log file size limit (Scored)

Profile applicability:

Level 2

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 fill a drive or partition containing the log files

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

Audit: Validate the max file limit is not greater than the size of the partition where the log files are stored.

Remediation: Create the following entry in your logging.properties file. This field is specified in bytes:

java.util.logging.FileHandler.limit=10000

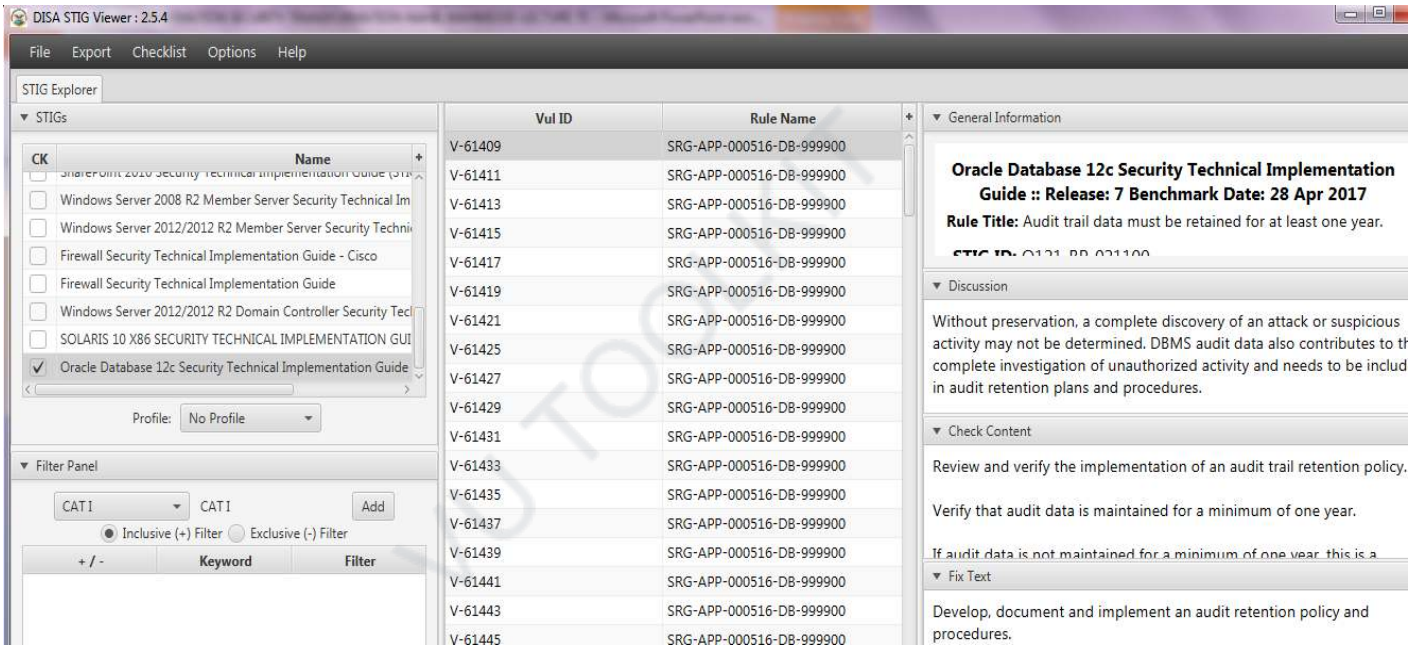
Default Value: No limit by default

Module: 75
case study – security hardening – Oracle Solaris server

Security Hardening – Case Study – Oracle

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

STIGVIEWER WINDOW



General Information:

Rule Title: The Oracle Listener must be configured to require administration authentication

STIG ID: O121-BP-022700

Severity: CAT I

Discussion:

Oracle listener authentication helps prevent unauthorized administration of the Oracle listener. Unauthorized administration of the listener could lead to DoS exploits; 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. Unauthorized access can result in stopping of the listener (DoS) and overwriting of listener audit logs.

Check Content:

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

For Windows hosts, view all Windows services with TNSListener embedded in the service name

The service name format is:
Oracle[ORACLE_HOME_NAME]TNSListener
View the STIGVIEWER for Unix hosts...

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.

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.

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.

CCI (Control Correlation Identifier):

CCI: 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

Module: 76
case study – security hardening – MS SQL server

Case Study Security Hardening – MS SQL

- CIS Benchmarks case study (MS SQL Server 2012)

- September 30, 2016
- 73 pages PDF doc

2.14 Ensure 'sa' Login Account has been renamed (Scored)

Profile applicability:

Level 1 database engine

Description: The sa account is a widely known and often widely used SQL Server account with sysadmin privileges.

Rationale: It is more difficult to launch password-guessing and brute-force attacks against the sa account if the username is not known.

Audit: Use the following syntax to determine if the sa account is renamed:

SELECT name

FROM sys.server_principals WHERE sid = 0x01;

A name of sa indicates the account has not been renamed

Remediation: Replace the different_user value within the below syntax and execute rename the sa **login:**

ALTER LOGIN sa WITH NAME = <different_user>;

Impact: It is not a good security practice to code applications or scripts to use the sa account 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.

Default Value: By default, the 'sa‘ account name is 'sa'

References: https://msdn.microsoft.com/en-us/library/ms144284(v=sql.110).aspx (Choose An Authentication Mode)

Module: 77
case study – security hardening – Oracle DB server

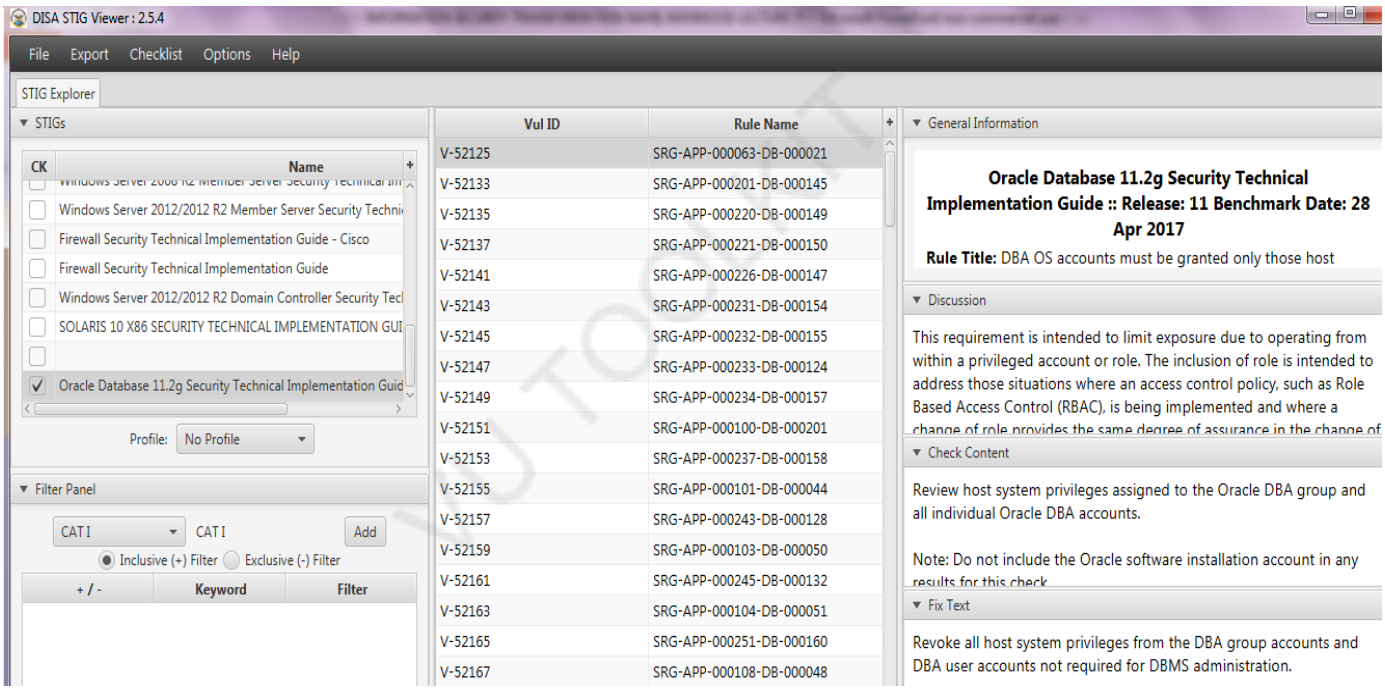
Security Hardening – Case Study – Oracle

Oracle database 11.2g

DISA, Release 11

28 April 2017

STIGVIEWER WINDOW



General Information:

Rule Title: The Oracle REMOTE_OS_ROLES parameter must be set to FALSE.

STIG ID: O112-BP-022000

Severity: CAT I

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.

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

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

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;

Fix Text:

The above SQL*Plus command will set the parameter to take effect at next system startup

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

Module: 78
Case study security hardening – Windows 8 Workstation

Case Study Security Hardening – Windows 8

CIS Benchmarks case study (Windows 8.1)

January 31, 2017

891 pages PDF doc

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

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 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.

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

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:

HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\Windows Error Reporting:AutoApproveOSDumps

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

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

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

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

References:

CCE-33927-5

Critical Controls:

13 Data Protection

Module: 79
A

Module: 72
A