VU SOLUTION BY RAJA MUSHTAQ:

0305-5868956

BE PART OF OUR VU GROUP IF U R INTEREST

ED...

HTTPS://CHAT.WHATSAPP.COM/GECIRAU2NITOD4F5DJDIGM

For any help contact 03337435091. Qasimali106376@gmail.com

U tube channel Digital world VU

MCQ No 1 ---------- Technique / Solution can be used to analyze and block inbound email attachments with malicious behavior.

A. Enterprise antivirus
B. Sandboxing
C. Siem solution
D. Fim solution

MCQ No2: OWASP software assurance maturity model (SAMM) undertakes software security testing and validation during ……

A. Governance and deployment
B. Governance and verification
C. Verification deployment
D. Construction and Governance

MCQ No 3: Creating awareness relating to policy and ISMS fall under---------- Clause.

A. Support
B. Operation
C. Performance evaluation
D. Leadership

MCQ No 4: Assigning resources, assignment rules and communicating roles fall under ------- clause.

A. Support
B. Leadership
C. Performance evaluation
D. Operation

MCQ No 5: The objective of COBIT is to help organization---------- --.

A. **Create optical values from it by balancing benefits with risk**

B. Implement a strong governance of it
C. Manage it effectively while ensuring business continuity
D. Create a single page it dashboard

MCQ No 6: In security transformation model ownership of validation of controls lies with

A. IT operation team
B. Business team
C. Info security or consultant
D. IT help desk team

MCQ No 7: where should source code be kept as best practice?

A. Access control system
B. Change control system
C. Version control system
D. Source control system

MCQ No 8: As per ISO27001 Operating procedure should be

A. Confidential
B. Verbally communicated
C. Decided on adhoc basis
D. Documented and available to who need them

MCQ No 9: It seems to conducting a successful security transformation project is more challenging in a?

A. Large size organization
B. Medium size organization
C. Small sized organization
D. Environment where multiple sites are present

MCQ No 10: Stage 2 of security transformation refers to

A. Security Governance

B. Security engineering
C. Security hardening
D. Vulnerability management

MCQ No 11---------- should be used to ensure that critical system files have not been altered.

A. CIS cat pro
B. Qualys vulnerability scanner
C. Security information and event monitoring tools
D. File integrity monitoring tool

MCQ No 12: An authentic information head always ----------

A. Take credit of every thing
B. Never admits mistakes and failure
C. Give credit where it is due
D. Very strict and disciplined

MCQ No 13: Network performance degradation can be faced in ----------step of VM cycle.

A. Preparing the scanner
B. Analyzing the asset
C. Running the scanner
D. Applying the patches

MCQ No 14----------category vulnerabilities have the highest severity in Qualys scan.

A. Level 2 (Not sure)
B. Level 3
C. Level 4
D. Level 5

MCQ No15: ISO31000 guidelines are centered on---------- ?

A. Organization context
B. Leadership and commitment
C. Planning
D. operation

MCQ No 16---------- plays an instrumental role in success of security transformation program.

A. IT team lead by CIO
B. Business team
C. Internal team
D. Highest management

MCQ No17 -------- should be deployed to limit and control that which devices can be connected to the network?

A. 802.1x
B. 802.11g
C. 802.11b
D. 802.11n

MCQ No 18: all network traffic to or from internet must pass through --------- to filter unauthenticated connections.

A. Application layering proxy
B. Session layer filtering proxy
C. Network layer filtering proxy
D. System layer filtering proxy

MCQ No 19: in which phase of Security assessment, assessment method based on report format are decided

A. Report finding
B. Build plan, scope and objectives
C. Assign role
D. Conduct assessment

MCQ No 20: Automated tool should be used to verify and compare the network device configuration with ----------

A. Approved security configuration
B. Recommended security configuration by vendor
C. Latest security configuration released by vendor
D. Default security configuration released by vendor

MCQ No 21: Under security transformation model which team is responsible for validation of control ?

A. Business team

B. Info security team or consultant
C. IT operation team
D. IT help desk team

MCQ No 22: The computer security resources center (CSRC) website guides user to ------ resources?

A. CIS resources on computer , cyber, information security and privacy
B. SANS resources on computer, cyber, information security and privacy
C. NITS resources on computer , cyber, information security and privacy
D. PCI resources on computer , cyber, information security and

privacy MCQ No 23: Complex password should be enforced to survive ?

A. Dictionary attack
B. Injection attack
C. DOS attack
D. Phishing attack

MCQ No 24----------activities are carried out in phase 1 (Pilot phase) of information security transformation program?

A. Perform hardening of Key IT asset in Test environment
B. Understand origination and its security issues
C. Develop ISMC
D. Identify assets for various phases

MCQ No 25: Candidness quality of information security head means that he--- ?

A. Promote performance and merit
B. Encourage-solo flight of team member
C. Honesty and straight talk
D. Adjust players in right position

MCQ No 26----------protocol used for Assigning address dynamically?

A. DCP
B. HTTP
C. DHCP
D. IP

MCQ No 27--------Team has primary ownership of vulnerability management process?

A. Information security team.
B. IT operation team
C. Business team
D. Risk and compliance team

MCQ No 28---------Rules are mentioned relate to C++ security hardening?

A. Seven
B. Eight
C. Nine
D. Ten

MCQ No 29--------is goal f performing audit

A. Testing Security that is Assumed to be secure
B. Technical assessment design to achieve specific goals
C. To fix as many things are possible and efficiently as possible
D. Focuses on how on existing configuration compare to standard

MCQ No 30. Under security transformation model which team is responsible for implementing controls?

A. It operation team
B. Security consultant
C. Risk compliance team
D. Business team

MCQ No 31: In---------- assessment tester has full access to all internal information about the target?

A. White box assessment
B. Grey box assessment
C. Black box assessment
D. Risk assessment

MCQ No 32----------assessment is designed to determine whether an attacker can achieve specific goals when facing your current security posture?

A. Threat assessment
B. Bug bounty hunting
C. Penetration testing
D. Red team exercise

MCQ No 33----------are the key benefits of security transformation project implementation to an organization?

A. IT team get experience and aware of security
B. Prevention of attack
C. IT team gets incentives
D. Management becomes aware of IT team capability

MCQ No 34----------action is recommended for organization having very good security posture and has a score higher than 85%?

A. Go for risk assessment
B. Third party security review
C. Go for ISO27001 certification
D. Information security transformation program

MCQ No 35: Version of security related updates should be applied on network devices?

A. Latest
B. Default
C. Latest and stable
D. Oldest

MCQ No 36: Most of the problem associated with week security posture is due to-------?

A. Lack of awareness
B. Lack of funds
C. Lack of experience

D. Lack of commitment

MCQ No 37: The information security policy need to be ---------- ?

A. Review once in three year
B. Update once in five year
C. Locked in drawer and kept confidential
D. Regularly reviewed and approved for the changes

MCQ No 38: In case of financial sector ---------- regulations need to be reviewed and understood to raise management support for security transformation?

A. SBP
B. PTA
C. PEMRA
D. PEPRA

MCQ No 39: Inventory of authorized and unauthorized software control require making a list of---- ?

A. Authorized access and version
B. Authorized operating system and version
C. Authorized software and version
D. Unauthorized software and version

MCQ No 40: Which principle should be used when setting up a user in data base?

A. Principle of normal user
B. Principle of administrative user
C. Principle of least privilege
D. Principle of highest privilege

Q. 41 ……..which team has primary owner ship in vulnerability management?

ANS: Information security team

Q. 42. Steps involved in vulnerability management?

Ans: Identify, classify, remediate, and mitigate the vulnerability

Q. 43: For creating scanning policies, qualys built in policies library include. Ans: CIS and DISA policies

Q. 44. What is the first step in automated mechanism of security hardening and validation??

Ans: Scan an IT asset using Qualys nessus compliance scan

Q. 45. There are ------benefits of version control.

ANS: SEVEN

Q. 46: ISO 31000 guidelines are centered on?

Ans: Leadership and commitment.

Q. 47: creating awareness related to policy and ISMS fall under??? :

ANS: Support

48- chose the correct statement:

- Allow all IP address

- Deny all IP address

- Deny communication with known malicious IP address

- Allow communication with unused IP address

49: In small sized security organization in Pakistan, It is likely the number of security stall will ?

Ans: 1-5 or 2-4

50: In Medium sized security organization in Pakistan, It is likely the number of security stall will ? Ans: 10-15

51: In Large sized security organization in Pakistan, It is likely the number of security stall will ?

Ans: 30

52: What was the old name ISO27002:2013?

Ans: ISO17799

53: In PHP Guidelines " display error" shows

A. On

B. off

C. True

D. False

54: Android managers set as

A. **True**

B. **false**

C. **Enable**

D. **Disable**

55. by default Android managment set as (is ka ans hai NoT ENABLE But option main not enable ni hai ap jo laga lo)

A. **True**

B. **False**

C. **Enable**

D. **Disable**

56. what is the Fifth layer of CSMM

Ans: Monitored

57. what is the Sixth layer of CSMM

Ans: Secured

58: The number of ports is configurable, but the default scan

Ans: approximately 1900 TCP ports and 180 UDP ports.

Q No 01: very important. Security Breach in HOME Department 2014

How much card played: • 56 million payment cards compromised

Which kind of vulnerability exploited: Then they exploited a zero-day vulnerability in Windows Or Exploitable vulnerabilities were found in anthem network

How much mail used : The malware was also able to capture 53 million email addresses.

• 56 million payment cards compromised

• Early September 2014

zero day vulnerability exploited

• Sequence of events: – The attackers were able to gain access to one of Home Depot's vendor environments by using a third-party vendor's logon credentials

– Then they exploited a zero-day vulnerability in Windows, which allowed them to pivot from the vendor-specific environment to the Home Depot corporate environment.

– Once they were in the Home Depot network, they were able install memory scraping malware on over 7,500 self-checkout POS terminals (Smith, 2014).

– This malware was able to grab 56 million credit and debit cards. The malware was also able to capture 53 million email addresses (winter, 2014).

Topic no 125: Security Breach Case Study 2: Anthem

How much People effected : Affected 78.8 million individuals

How Much Account used or Utilized: The attacker utilized at least 50

accounts which way used : A phishing email containing malicious content

(Also MCQZ) How much system compromised: compromised at least 90

systems

Q No 2: Topic No 145: WHAT IS SECURITY ENGINEERING?

- Security Engineering is the third layer of the Security Transformation Model
- Consists of more in-depth and complicated security activities which take more time and effort
- Many times related to security architecture
- Types of activities for security engineering:
- FW granular access lists
- Building an effective DMZ architecture
- Segregating the network with VLANs
- Adding a security tool such as SIEM, FW, DLP, NAC, etc
- App-DB encryption

Q no 3: Topic No 146: WHAT IS THE OBJECTIVE OF SECURITY ENGINEERING? (MOSTLY)

- Security architecture as per best-practices
- The right security devices in the right places

• Effective security configuration of security devices (features)

• Optimum operation of security devices

• Aggregate controls

Examples:

• FW first and then IPS

• Edge FW, data center FW

• Malware protection at the network edge

Q No 04: Steps in Security engineering: (Repeated)

– Assess risk profile

– Research security solutions

– Design security architecture

– Implement security controls & solutions

– Test and validate security posture

Q No 05: Security transformation project:

• Security transformation project time line:

– 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)

Q no 06: Software Assurance Maturity Model (SAMM) Governance Phase: (Repeated in exams)

• OWASP Software Assurance Maturity Model (SAMM) Governance Phase:

– Strategy & Metrics

– Education & Guidance

– Policy & Compliance

• Strategy & Metrics: – Focused on establishing the framework within an organization for a software security assurance program. –

• Education & Guidance: – Focused on arming personnel involved in the software lifecycle with knowledge and resources to design,

• Policy & Compliance: – Focused on understanding and meeting external legal and regulatory requirements while also driving internal security standards to ensure compliance in a way that's aligned with the business purpose of the org.

Q no 07: IT Security functions

– Network security

– Systems security

– Application & database security

– Mobile security

Q no 8: What is a patch?

– "A patch is a piece of software designed to update a computer program or its supporting data, to fix or improve it. This includes fixing security vulnerabilities and other bugs"

What are general steps for patch management? (yeh steps mostly ate hain exams main)

Step1: Establish baseline IT assets inventory

Step 2: Gather software patch and vulnerability information

Step3: identify vulnerability relevancy and filter to assign to end point

Step 4: review approve and mitigate patch management

What is patch management?•

– Patch management is an area of systems management that involves acquiring, testing, and installing multiple patches (code changes) to an administered computer system.

Patch management tasks :• – Maintaining current knowledge of available patches, deciding what patches are appropriate for particular systems, ensuring that patches are installed properly, testing systems after installation, and documenting all associated procedures, such as specific configs required.

Risk of not patching:• – By not applying a patch you might be leaving the door open for a malware attack

– Malware exploits flaws in a system in order to do its work. In addition, the timeframe between an exploit and when a patch is released is getting shorter

Q No: 09: Topic No 283: Key Leadership Qualities Of InfoSec (Head IMP Repeating)

• Lets examine the key leadership qualities of the Information Security Head or the key resource driving the Security Transformation Program

• Authenticity

• Candidness

• Fairness & fair play

• Team environment

• Recognizing talent and hard work

• Celebrating success!

• Authenticity –

IT is complex – No one person "knows-it-all" – Communicate that each individual has limitations – Admit mistakes and failures – Give credit where it is due

• Candidness: – Call a spade a spade – Honesty and straight-talk – Hear feedback and give respect to views of everyone

• Fairness & Fair Play: – Promote performance and merit – Adjust players in the right positions based on their strengths – Coach and guide team to perform and achieve results

• Team Environment: Discourage solo-flight and promote team consensus, team reviews, and team achievements – Single out and coach individuals playing turf tactics

• Recognize Talent & Hard Work: – Identify self-promotion versus talent combined with hard work – Encourage hard workers who are team players

Q no 10: Roles & responsibilities in security governance.

• Roles & responsibilities:

– Is right person working at the right place?

– Do key people tasked with security governance & documentation has the right skills and experience to build documentation?

– Are staffs aware of their responsibilities related to security governance documentation …policies, SOPs, checklists, etc?

– Is documentation and process approach part of staff JDs & appraisal?

Q No 11: Four-layer security transformation model or Four pillars of security transformation model

• 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

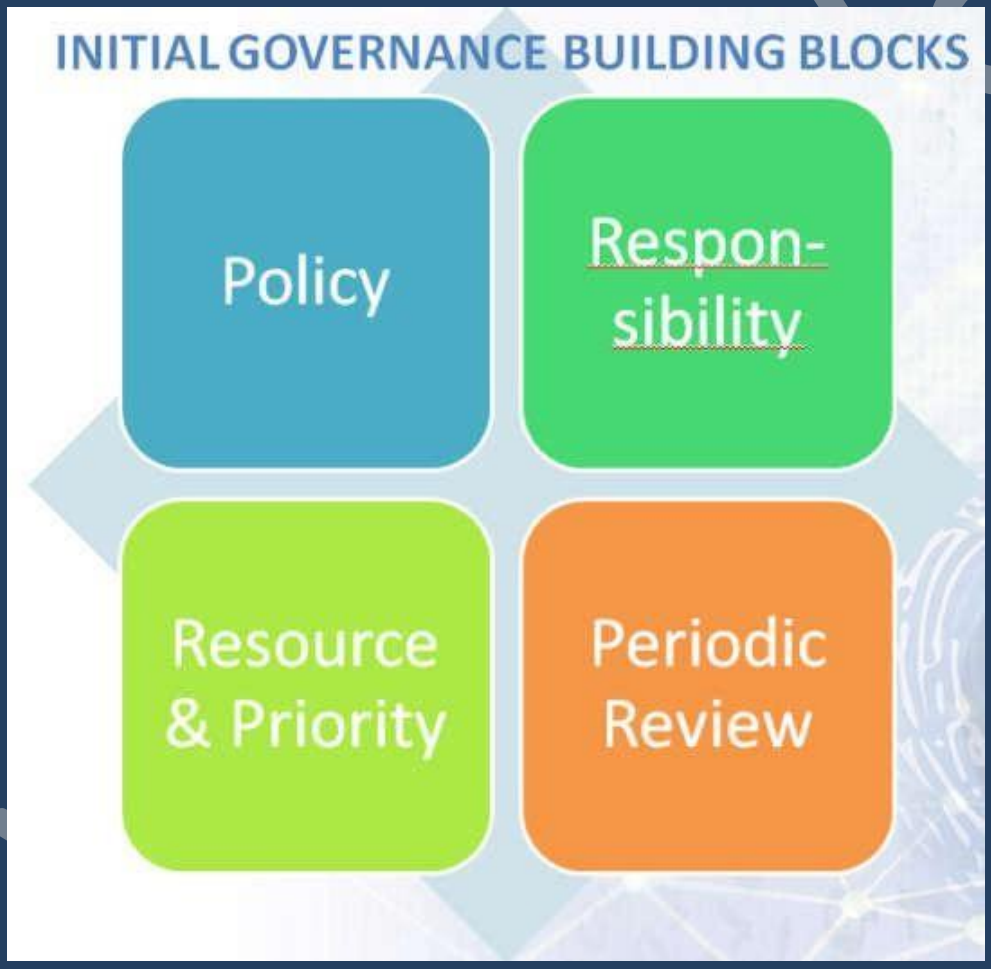
3. **Security Engineering; More complex security design & solutions**

4. **Security Governance; Managing the information security program**

Q No 12: Info security Governance initial Block.

Initial

- **Policy**
- **Responsibility**
- **Recourse and priority**
- **Periodic review**



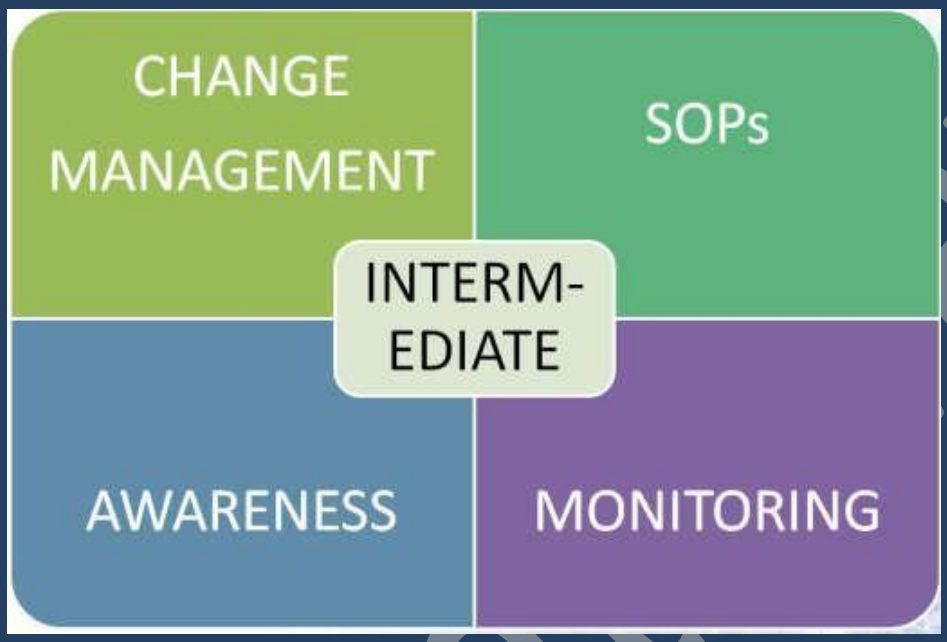
Intermediate

- **Change management**

-

- **SOP,s**
- **Awareness**

- **Monitoring**



Mature

- **Risk management**
- **Internal audit**
- **Incident management**

Q No: 13: Info security governance initial block detail. (most repeating)

ACTIVITY	RESPONSIBLE	DETAIL
POLICY	DEVELOPED BY CISO SIGNED OFF BY BOARD/EXECUTIVE	SETS THE SCOPE, OBJECTIVES, FRAMEWORK, REQUIREMENTS
RESPONSIBILITY & AUTHORITY	BOARD/EXECUTIVE	ASSIGNS ROLES, RESPONSIBILITIES, AND AUTHORITY FOR INFOSEC PROGRAM
RESOURCE ASSIGNMENT & PRIORITY SETTING	BOARD/EXECUTIVE	ALLOCATION OF RESOURCES AND BUDGET FOR THE INFOSEC FUNCTIONS
PERIODIC REVIEW	BOARD/EXECUTIVE	MONITOR AND REVIEW THAT THE GOALS OF THE INFOSEC PROGRAM ARE BEING MET

Q No 14: Topic No 198: How To Build Effective Info Sec Governance? (Imp Repeated)

• Key success factors: (*see also minor detail of all these 06 points*)

– Leadership

– Strategy

– Structure

– Reporting

– Project management

– Culture

• Leadership: – Executive management role – Tone at the top Drive pressing priority – Approves budgets and resources – Periodic review of progress

• Strategy: – How the objectives will be practically achieved while achieving the technical, governance, and performance goals – How the organization will gear up and focus for the security transformation

• Structure: – CS205 Information Security By Digital World Vu Sabahat Jabeen Page 54 – What hierarchies, team structures, reporting lines, and resources will come together – How will different teams work together to achieve the common goals?

• Reporting: – What will be reported? – What will be the frequency of reports? – Who will perform review and assurance? – Who will monitor and track progress?

• Project Management: – How will an exceptional execution discipline be built? – How will milestones and performance be tracked? – How will project management best-practices be utilized?

• Culture: – How will an open, cooperative, authentic, and committed culture be built? – How will contention and conflict be eliminated? – How will a performance driven culture be promoted?

Q NO 15 : Pen test and Red team Exercise (look a minor review on these steps)

: Establish a Penetration Testing Program

• Establish a program for penetration tests that includes a full scope of blended attacks, such as wireless, client-based, and web application attacks.

20.2: Conduct Regular External and Internal Penetration Tests

• Conduct regular external and internal penetration tests to identify vulnerabilities and attack vectors that can be used to exploit enterprise systems successfully.

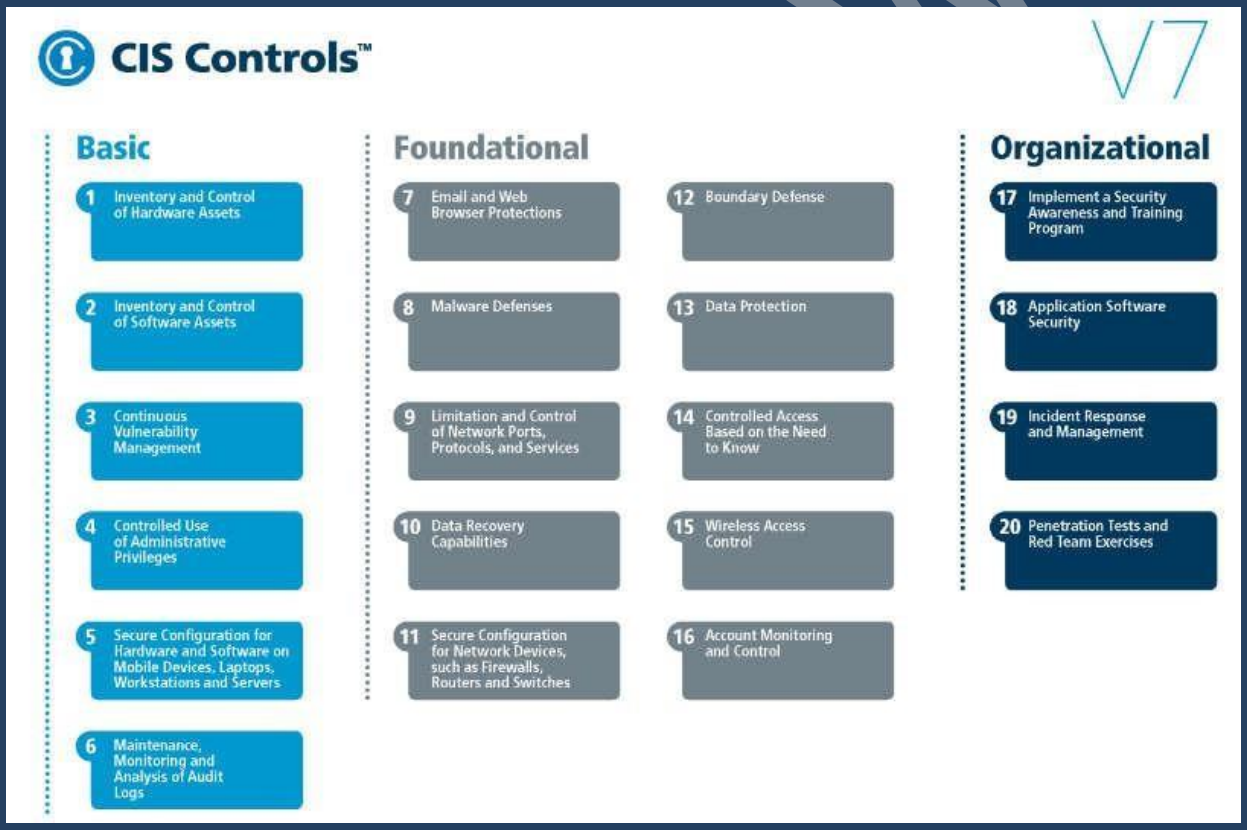
20.3: Perform Periodic Red Team Exercises

• Perform periodic Red Team exercises to test organizational readiness to identify and stop attacks or to respond quickly and effectively.

. 20.7: Ensure Results from Penetration Test are Documented Using Open, Machine readable Standards

• Wherever possible, ensure that Red Teams results are documented using open, machine readable standards (e.g., SCAP). Devise a scoring method for determining the results of Red Team exercises so that results can be compared over time.

Q No 16: Most Important: (read and keep in mind about steps Basic Foundational and organizational)



Q NO 17: Monitor and Detect Any Unauthorized Use of Encryption

• Monitor all traffic that is encrypted with protocols such as SSL or TLS leaving the organization and detect any unauthorized use of encryption.

Q No 18: Topic No 262: What is Security Validation?

• What does security validation mean?

– To confirm via walk-through of system or device that the security controls implemented by an IT team have actually been implemented correctly

• Who implements the security controls?

– Under the Security Transformation Model, security controls are implemented by the IT teams

• Who conducts security validation?

– Security controls are validated by the Information Security team or by a third party consultant following the principle of segregation of duty

• Why do we need to validate security controls?

– To check the completeness of the controls

– To check the correctness of the controls

– As an overall assurance

Q No 19: Topic No 268: Software Security Testing & Validation–1 (imp)

• The OWASP Software Assurance Maturity Model (SAMM) undertakes software security testing & validation during the following phases:

– Verification

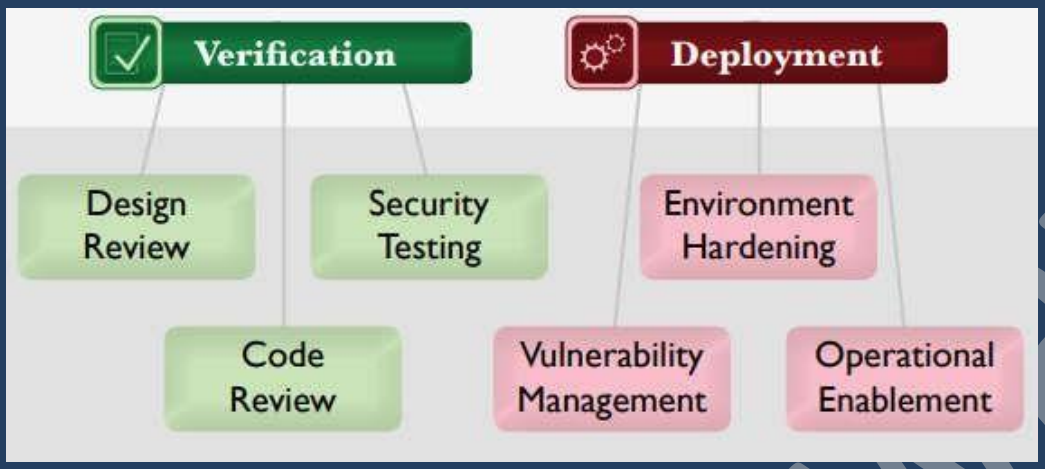
– Deployment

• OWASP Software Assurance Maturity Model (SAMM) Verification Phase:

– Design Review

– Code Review

– Security Testing



Q Bo 20: Topic No 270: Embedding Info Sec In to Project Management (IMP)

- **PMIs five phases of project management:**
- **Initiate**
- **Plan**
- **Executing**
- **Controlling**
- **Closing (Also see these steps minor look for detail).**

Q No 21: topic 235 RISK MANAGEMENT – FRAMEWORK

– **RISK MANAGEMENT – FRAMEWORK**

1: Risk architecture,

2: Strategy and

3: Protocols of the organization

03337435091. Qasimali106376@gmail.com

• This is often referred to as the risk architecture, strategy and protocols of the organization,

Table 2: Risk management framework

Risk management architecture
- Committee structure and terms of reference
- Roles and responsibilities
- Internal reporting requirements
- External reporting controls
- Risk management assurance arrangements

Risk management strategy
- Risk management philosophy
- Arrangements for embedding risk management
- Risk appetite and attitude to risk
- Benchmark tests for significance
- Specific risk statements/policies
- Risk assessment techniques
- Risk priorities for the present year

Risk management protocols
- Tools and techniques
- Risk classification system
- Risk assessment procedures
- Risk control rules and procedures
- Responding to incidents, issues and events
- Documentation and record keeping
- Training and communications
- Audit procedures and protocols
- Reporting/disclosures/certification

Q No 22: Topic No 237: ISO31000:2018 – RISK MANAGEMENT – HOW TO IMPLEMENT

A Risk Practitioners Guide To ISO31000:2018 Successful implementation of a risk management initiative is an ongoing process that involves working through 10 activities below on a continuous basis. These activities relate to:

(1) **Plan;**

(2) **Implement;**

(3) **Measure; and**

(4) **Learn.**

Risk management Frame work 05 component:

1. **Integration,**
2. **2 designs,**
3. **3 Implementation,**
4. **4. Evaluation ,**
5. **5 Improvement**

Q No 24: What is an internal security assessment? (Q yeh aye ga what is internal assessment, mention any one reason definition k bad neche se koi se kuch steps bata dena)

DEFINATION: An effort to assess the security posture, risks, or vulnerabilities for any project, service, application, or device

• When is an internal security assessment required?

– Launch of a new IT project or service

– When an incident has occurred

– On change of leadership

– Regulatory or compliance requirements.

Q No25: What is the purpose of effective toll scanning? (an search from google)

To perform external and internal reconnaissance of available infrastructure component, network scanning tool can be used. A network scanning tool aims to identify active hosts on a network, either to attack them, or to assess vulnerability in the network.

Q No 26: Which steps are include in ensuring INFOSEC ASPECTS OF BUSINESS CONTINUITY MNGMT

INFORMATION SECURITY INCIDENT MANAGEMENT

A.16.1 **MNGMT OF INFOSEC INCIDENTS & IMPROVEMENTS**
A.16.1.1 **RESPONSIBILITIES & PROCEDURES**
A.16.1.2 **REPORTING INFOSEC SECURITY EVENTS**
A.16.1.3 **REPORTING INFOSEC WEAKNESSES**
A.16.1.4 **ASSESSMENT OF & DECISION ON INFOSEC EVENTS**
A.16.1.5 **RESPONSE TO INFOSEC INCIDENTS**
A.16.1.6. LEARNING FROM INFOSEC INCIDENTS
A.16.1.7 COLLECTION OF EVIDENCE

Q No 27: Types of Network redundancy (verify this also)

AVAILABILITY OF INFORMATION PROCESSING FACILITIES

Information processing facilities shall be implemented with redundancy sufficient to meet availability requirements.

Different types of network redundancy include (This one Ans not sure)

- Multiple spanning trees
- Ring network
- Diverse trunking
- Multi protocol labe

Q No 28: What are five steps in business continuity plan management. (please verfy this)

Five phases of development and maintaining business continuity plan

Phase1: Access your risk (natural disaster, cyber attack, ransom ware, data corruption,)

Phase 2: Business impact analysis

Phase 3: Identify critical assets

Phase 4: Back up your data

Phase 5: Plan for recovery. 6. Test your plan

IMPORTANT TOPIC ↓↓

What is vulnerability?

– Vulnerability is a cyber-security term that refers to a flaw in a system that can leave it open to attack. Vulnerability may also refer to any type of weakness in a computer system itself, in a set of procedures or in anything that leaves information security exposed to a threat.

What is vulnerability management? – Vulnerability management is the "cyclical practice of identifying, classifying, remediating, and mitigating vulnerabilities" •

What is vulnerability assessment (VA)? – A process that defines, identifies, and classifies the security holes (vulnerabilities) in a computer, network, or communications infrastructure

Q No 29: Topic no 118: What Are The Steps In VM Lifecycle?

VM Steps:

1. **Analyze assets**

2. **Prepare scanner**
3. **Run vulnerability scan**
4. **Assess results**
5. **Patch systems**
6. **Verify (re-scan)**

Q No 30: What are some of the common vulnerability scanners?

– Open VAS
– Nessus
– Qualys
– Rapid7

Free tool offered. By Qualys

(IMP

) Browser check

SSL

Qualys Free Scan

1. Vulnerability – 2. OWASP – 3. Patch Tuesday – 4. SCAP

Zero-day exploits:

– A zero day vulnerability refers to a hole in software that is unknown to the vendor. This security
Hole is then exploited by hackers before the vendor becomes aware and hurries to fix it This exploit is called a zero day attack.

Q No 31: Topic no 127: Who Conducts Vulnerability Management?

• **A**

SN	ACTIVITY	TEAM	SUPPORTED BY
1	ANALYZE ASSETS	INFOSEC	IT OPS TEAM
2	PREPARE SCANNER	INFOSEC	-
3	RUN VULNERABILITY SCAN	INFOSEC	-
4	ASSESS RESULTS	INFOSEC	IT OPS TEAM
5	TEST & PATCH SYSTEMS	IT OPS TEAM	INFOSEC
6	VERIFY (RE-SCAN)	INFOSEC	IT OPS TEAM
7	REPORT FINDINGS	INFOSEC	IT STEERING COMMITTEE

Q No 32: Topic no 129: Qualys Features

• Qualys:
– Cloud-based service
– On-premise device
– Complete suite
– Scalable and immediate deployment
– Asset discovery; find and organize hosts
– Prioritize & manage remediation tickets
– Continuous monitoring service
– Policy compliance scanning
– Qualys Secure Seal for websites

Q No 33: Topic no 136: How Do VM Scanners Work?

• Lets take a look at Qualys scanning technique:
• Qualys Guard scanning methodology mainly focuses on the different steps that an attacker might follow
in order to perform an attack.

• gathering techniques that will be used by an attacker.

– Checking if the remote host is alive

– The first step is to check if the host to be scanned is up and running in order to avoid wasting time on scanning a dead or unreachable host

– Firewall detection

– The second test is to check if the host is behind any firewalling/filtering device. This test enables the scanner to gather more information about the network Infrastructure and will help during the scan of TCP and UDP ports.

– TCP / UDP Port scanning

– The third step is to detect all open TCP and UDP ports to determine which services

Are running on this host. The number of ports is configurable, but the default scans Is approximately 1900 TCP ports and 180 UDP ports.

Q No 34: Topic no 141: VM Challenges & Pitfalls

Challenges:

– Internal expertise on VM tool
– Not enough support from IT teams
– Vulnerability patching causing application failure
– Management support

Q No 35: Topic no 142: IT Asset Management Challenges

• The typical enterprise has hundreds or thousands of IT assets with a fast-paced business environment

• Tough challenge to keep all IT assets tracked and updated with all the right software patches and updates

• Challenges:

– Asset discovery & tracking
– Antivirus status
– Windows & OS updates
– Patch management
– Change management

Why is security governance at stage 4?
– First build a building and then manage it
– First 2 stages build up the essential foundation
– 3rd stage implements advanced security measures
– Then (4th stage) it is time to manage

Q no 38: Pakistan's InfoSec paradigm
– Governance overkill
– Reactive
– Superficial
– Complete absence of underlying security controls

Q NO 39: Topic No 198: How To Build Effective InfoSec Governance?

Q No 40: Topic No 202: Role Of CISO In Driving Info sec Program

Q No 41: Topic No 203: Key Inhibitors For Security Program Failure

Q No 42: Topic No 207: Security Documentation: Standards

Policies:
Policies are formal statements produced and supported by senior management. They can be organization-wide, issue-specific or system specific. Your organization's policies should reflect your objectives for your information security program.

Standards
Standards are mandatory actions or rules that give formal policies support and direction. One of the more difficult parts of writing standards for an information security program is getting a company-wide consensus on what standards need to be in place.

Compulsory and must be enforced to be effective. (This also applies to policies!)

Procedures
Procedures are detailed step by step instructions to achieve a given goal or mandate. They are typically intended for internal departments and should adhere to strict change control processes.

Guidelines
Guidelines are recommendations to users when specific standards do not apply. Guidelines are designed to streamline certain processes according to what the best practices are. Guidelines, by nature, should be open to interpretation and do not need to be followed to the letter.

Q No 43: Topic No 211: ISMS: Leading Info Sec Governance Framework

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

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

Q No 44: What is ISO27002:2013?

– Information technology -- Security techniques -- Code of practice for information
security controls
– Renamed from ISO 17799

• PCI Data Security Standard (DSS):
– Designed to ensure that ALL companies that accept, process, store or transmit
– Managed by Security Standards Council
– 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

Topic No 231: 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)

Q No 45: Topic No 230: NIST FRAMEWORK

• The Computer Security Resource Center (CSRC) website guides users to NIST resources
on computer, cyber, and information security and privacy.

• Its content includes publications, projects, research, news and events from the NIST
Information Technology Laboratory's (ITL) two security divisions

Q No 46: Types of Changes:

Standard changes are changes to a service or to the IT infrastructure where the implementation process and the risks are known upfront.

Normal Changes
• Those that must go through the change process before being approved and implemented. If they are determined to be high-risk, a change advisory board must decide whether they will be implemented.

Emergency Changes
• Arise when an unexpected error or threat occurs, such as when a flaw in the infrastructure related to services needs to be addressed immediately.

Q No 47: Topic No 243: PROJECT MANAGEMENT FOR INFOSEC: PART 1

• PART 1:

– Importance Of Project Management For Information Security

• CYBER SECURITY CHALLENGES:
– Reactive
– Superficial
– Contention
– Box-Approach
– Governance-Overkill

Q No 48: Topic No 254: CYBER SECURITY MATURITY MATRIX

I. FOUNDATION, II. FUNDAMENTALS, III. HARDENED, IV. PROTECTED, V. MONITORED, VI. SECURED

I. FOUNDATION
Edge FW With Filtering
Active Directory (WS/S)
Licensed Enterprise AV (WS/S)
Licensed Windows OS (WS/S) Or Open Source
: RED TEAM PENETRATION TESTING
• Red team and blue team
• Attack & defense simulation
• Continuously find holes in security defenses
• Uncover security vulnerabilities before hackers exploit them
• What does security validation mean?
– To confirm via walk-through of system or device that the security controls implemented by an IT team have actually been implemented correctly
• Who implements the security controls?

Security controls are validated by INFORMATION SECURITY TEAM or by THIRD PARTY consultant following the principle of segregation of duty.

Q No 49: Why do we need to validate security controls?

– To check the completeness of the controls
– To check the correctness of the controls
– As an overall assurance

Q No 50: Types of security testing:

– Vulnerability assessment (VA)
– Penetration testing (PT)
– Other security tests through various automated tools
– Code review (initiated in test environment)

Q No 51: What is security accreditation?

– Accreditation is the formal acceptance of the adequacy of the system's Overall security by the management (SANS)

Q No 52: Topic No 267: Embedding Info Sec Lifecycle into SDLC (Yeh pora topic important hai)

- The systems development life-cycle (SDLC) should embed the Information Security Activities forming a sec-SDLC (secure SDLC)
- Software Assurance Maturity Model (SAMM) developed by OWASP
- A guide to building security into software development

Q No 53: Topic No 270: Embedding Info Sec In to Project Management

- PMIs five phases of project management:

– Initiate
– Plan
– Executing
– Controlling
– Closing

Q No 54: Topic No 272: Different Types Of Security Assessments

- Vulnerability assessment
- Penetration test
- Audits
- White box/grey box/ black box assessments
- Risk assessment
- Threat assessment
- Bug bounty
- Red team

Q No 55: Topic No 278: Benefits Of the Security Transformation

- Key Benefits:– Prevention of attacks– Prevention of fraud & pilferage– A reliable & robust IT setu
- Impact of attacks: – Loss of market goodwill– Loss of customer confidence

What are Five steps in business continuity plan management.

Types of network redundancy.

Q No 56: What are objective of applying Cryptography (See topic no 218)

Topic No 218: ISO27001:2013 Controls Appendix; Part 5 In this module lets look at ISO27001:2013 (ISMS) related to cryptography, and physical & environmental security.

A.10.1 CRYPTOGRAPHIC CONTROLS

A.10.1.1 **POLICY ON THE USE OF CRYPTOGRAPHIC CONTROLS**

A.10.1.2 **KEY MANAGEMENT**

A.10.1.2 KEY MANAGEMENT Control: A policy on the use, protection and lifetime of cryptographic keys shall be developed and implemented through their whole lifecycle.

Q No 57: Control as per ISO27001?

Which type should use assest inventory long

: Deploy an automated asset inventory discovery tool and use it to build a preliminary inventory of systems connected to an organization's public and private network

Maintain an asset inventory of all systems connected to the network and the network devices themselves, recording at least the network addresses, machine name(s), purpose of each system, an asset owner responsible for each device…

Q No 58: :Write the name perform actitvities in control validation process?

Ans:The activities involve in control validation are typically referred as a "Control testing" or "Security control assessment"

Mention the name of valid section healing in the appendix isms

Types stored in assests inventory just names

Q No 59: Which action a rise management support of security transformation

the extent of work and resources required e) Present your report

Q No 60: Answer the following with respect to vulnerability.

Q; Which team have primary ownership

Ans: Information security team

Q: which team tests the patches in environment?

Ans: IT ops team

Q No 61: Significance of vulnerability management in transformation model? (Ans from chat gpt)

Vulnerability management is crucial in a security transformation model because it helps identify, assess, and prioritize potential weaknesses in an organization's systems, allowing proactive measures to be taken to prevent cyberattacks and safeguard sensitive data

Q No. 62: Mention any two factors behind insecure software.

01, Connectivity,

02, Extensibility.

03. Complexity:

Write name of any five actitites perfprmed in acredation process.

01. Organize, 02. . Prepare Checklist, 3. Confirm Tests , 4. Documentation & Processes (Complete) 5. Team Meeting, 6. Issue Accreditation

Which best practices are to be followed for applying security patches (ONLY steps names)

1. Use a change control process, 2. Read all related documentation, 3. Apply updates on a need- only basis 4. Testing 5. Plan to uninstall 6. Working backup and production downtime 7. Always have roll-back plan 8. Don't get more than 2 service packs behind

What are challenges associated with documented of security projects.

• Process culture absent: Defective & voluminous documentation: Training & awareness

• IT Outsourcing examples: –

Call centers – Hosted servers – Software development – Workstation helpdesk functions – Network services – Any other arrangement

'Topic No 278: Benefits Of The Security Transformation •

Prevention of attacks

– Prevention of fraud & pilferage

– A reliable & robust IT

setup Updatesssss:::

Info sec Governance Block arrange them. (Aise table ho ga usko arrange kerna ho ga. yad ker lo initail intermdiate and mature blocks k Name) sari yad ker lain intial inter and maure

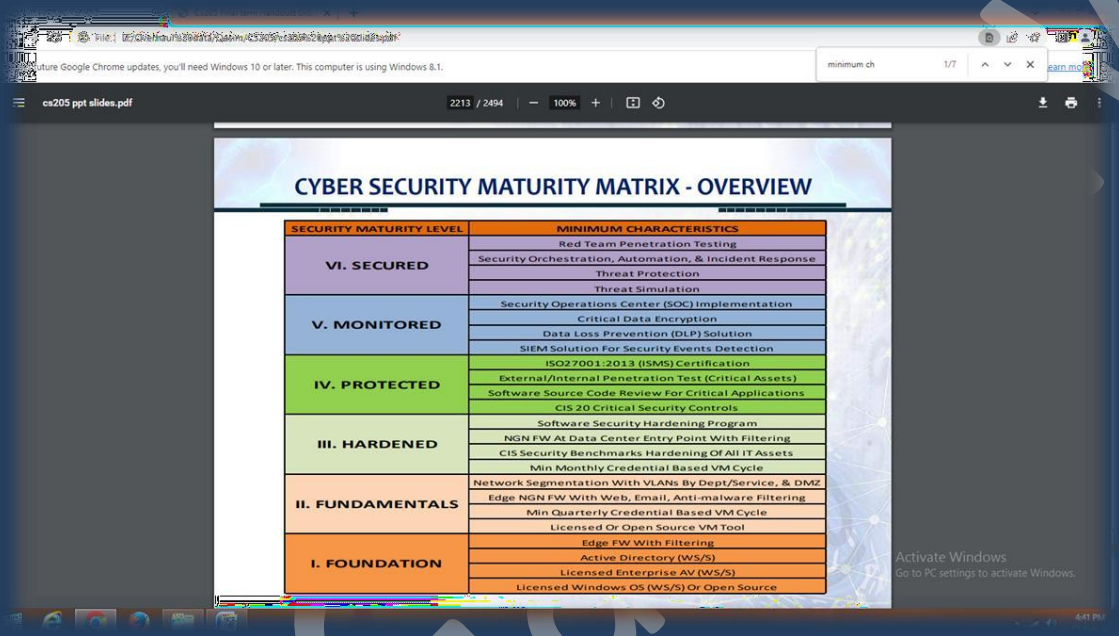
Awareness	Intermediate
Monitoring	Intermediate
Policy	Initial
Periodic review	Initial
Internal Audit	Mature
Responsibility	Initial

Use a SCAP-validated vulnerability scanner that looks for both code-based vulnerabilities (such as those described by Common

– Vulnerabilities and Exposures entries) and configuration-based vulnerabilities (as enumerated by the Common Configuration Enumeration Project).

Question: Arrange the Cyber security maturity matrix (is main yeh oper neche hon ge inko arrange kerna ho ga. is se 2 se 3 question a sakte hain IMP)

Ans:



Yeh question atta hai Responsibility ni hoti to apneactivity and Detailko match kerna ho ga

ACTIVITY	RESPONSIBLE	DETAIL
POLICY	DEVELOPED BY CISO SIGNED OFF BY BOARD/EXECUTIVE	SETS THE SCOPE, OBJECTIVES, FRAMEWORK, REQUIREMENTS
RESPONSIBILITY & AUTHORITY	BOARD/EXECUTIVE	ASSIGNS ROLES, RESPONSIBILITIES, AND AUTHORITY FOR INFOSEC PROGRAM
RESOURCE ASSIGNMENT & PRIORITY SETTING	BOARD/EXECUTIVE	ALLOCATION OF RESOURCES AND BUDGET FOR THE INFOSEC FUNCTIONS
PERIODIC REVIEW	BOARD/EXECUTIVE	MONITOR AND REVIEW THAT THE GOALS OF THE INFOSEC PROGRAM ARE BEING MET

Question• What type of IT assets do not have a CIS/DISA STIG ?

Ans: – Software applications (ASP.NET, PHP,

Other)

– Other applications such as asterisk deployments

جزاک اللہ خیرا کثیرا واحسن الجزاء فی الدنیا والآخرۃ

Thynks...

Regards:vu-Gateway...

For any query cntnct on wytsyp: +92305-5868956