CS 205 Fall 2024 File Objective Subjective 2024

CS 205 Final Term file Made BY M. Qasim Ali 03337435091

U tube channel QASIM KHAN WORLD

For any help contact 03337435091

MCQ No 1: Creating awareness relating to policy and ISMS fall under ---------- Clause.

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

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: -------- 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 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 least 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: pformance 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
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 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**

42. Steps involved in vulnerability management?

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

43: For creating scanning policies, qualys built in policies library include.

Answer: CIS and DISA policies

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

Ans: Scan an IT asset using Qualys nessus compliance scan

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

ANS: SEVEN

46: ISO 31000 guidelines are centered on?

Ans: Leadership and commitment.

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 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 management 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.

59: Guidelines should be

A. Open to interpretation.

B. Strictly enforce

C. Pasted on the notice board for easy visibility

60: Which of the following changes are easiest to prioritize and implement?

A. Emergency change

B. Standard change

C. Unknown change

D. Normal change

61: In which format results of penetration testing should be documented?

A. XML format

B. Excel format

C. Machine readable standard

D. PDF format

62: When a Flaws in infrastructure related to service need to be addressed immediately, this would be a?

A. Predictable change

B. Emergency change

C. Normal change

D. Standard change

63: The total numbers of discretionary controls in appendix a5 through a18 are:

A. 114

B. 121

C. 20

D. 10

64: One of the challenges of iso27001:2013 (isms) is that:

A. Is short and concise

B. It is generic and not specific

C. It has too few mandatory requirements

D. The annexure does not always apply to every type of organization

65: With how many time sources the clocks of all relevant information processing systems should be synchronized to record events and generate evidence

A. Single time source

B. At least four time sources

C. At least two time sources

D. At least three time sources

66: The ciso should be able to complete his or her own Technical knowledge by?

A. Seeking extra buget from board

B. Relying on it department to implement security controls

C. Building a god team

D. Outsourcing work to a third parties

67: While Implementing 4-layer security transformation model?

A. There should be absolutely no policy inline

B. Policies and procedure are not all required

C. It is suggested to have a high level and minimal policy in place

68: which of the following come at the center of Risk management process?

A. Context of organization

B. Planning and operation

C. Leadership and comment

D. Risk Assessment and risk treatment

69: If multi-factor authentication is not supported then user accounts shall be required to?

A. Use short passwords which are easy to remember

B. Use same password on all the systems

C. Use passwords longer than 14 characters

D. Use default passwords

70: free Nessus scanner offer trial version

A. 7
B. 15
C. 30
D. 45

71: is responsible for security design.

Ans : NETWORK/IT SECURITY ASSISTED BY VENDOR

72. UEM Tools combine the management of multiple endpoint types

Ans: In a single console

73.Use of entity framework is a very effective

Ans: SQL injection prevention mechanism

74. How vulnerability can be fixed in a system.

ANS: Through scanners

75- : Limit Use of type of scripting languages should "be used in email clients and web browser (Topic 159 for more detail)

Subjective Part QASIM KHAN WORLD u tube channel 03337435091

Question No 01: What is information security By SANS

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

What is Security hardening Define?

Ans: Security Hardening is the process of configuring the IT assets to maximize security of the IT asset and minimize security risks

Question nu 04: How many layers involved in information security transformation frame work? You are required to write the name.

Ans: 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.03 : Write any five steps in information security programns:

Ans

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

Q No. 04: Who Are The Players In Information Security?

• Government
• Industry & sectors
• International organizations
• Professional associations
• Academia and research organizations
• Vendors and supplier

Q No 05: Bangladesh Bank SWIFT Hack – Feb 2016

send more than three dozen fraudulent money transfer requests.
– USD 81 million stolen
– Total impact could have been USD 1 billion

Recover 19 Million

Not claim : 81 million

Q No 06: 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 07: 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. 08: SSh protocols versions names

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.

Q No 09: Info security Governance 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 10: 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
Risk management	Mature
Recourse and priority	Initial

Q No 11: 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:** –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 12: 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

Q No 13: 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 14: Topic No 254: CYBER SECURITY MATURITY MATRIX

Sr No	Layer
1	FOUNDATION
2	FUNDAMENTALS
3	Hardened
4	PROTECTED
5	MONITORED
6	. SECURED

I. FOUNDATION (with detail if sir Ask)

Edge FW With Filtering
Active Directory (WS/S)
Licensed Enterprise AV (WS/S)
Licensed Windows OS (WS/S) Or Open Source

CYBER SECURITY MATURITY MATRIX - OVERVIEW

SECURITY MATURITY LEVEL	MINIMUM CHARACTERISTICS
VI. SECURED	Red Team Penetration Testing
	Security Orchestration, Automation, & Incident Response
	Threat Protection
	Threat Simulation
V. MONITORED	Security Operations Center (SOC) Implementation
	Critical Data Encryption
	Data Loss Prevention (DLP) Solution
	SIEM Solution For Security Events Detection
IV. PROTECTED	ISO27001:2013 (ISMS) Certification
	External/Internal Penetration Test (Critical Assets)
	Software Source Code Review For Critical Applications
	CIS 20 Critical Security Controls
III. HARDENED	Software Security Hardening Program
	NGN FW At Data Center Entry Point With Filtering
	CIS Security Benchmarks Hardening Of All IT Assets
	Min Monthly Credential Based VM Cycle
II. FUNDAMENTALS	Network Segmentation With VLANs By Dept/Service, & DMZ
	Edge NGN FW With Web, Email, Anti-malware Filtering
	Min Quarterly Credential Based VM Cycle
	Licensed Or Open Source VM Tool
I. FOUNDATION	Edge FW With Filtering
	Active Directory (WS/S)
	Licensed Enterprise AV (WS/S)
	Licensed Windows OS (WS/S) Or Open Source

Q No 15: Types of security testing: (IMP)

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

Q No 16: Which vulnerability scanner is used to look for both code based and configuration based vulnerability?

Answer: Use a SCAP-validated vulnerability scanner that looks for both code-based vulnerabilities and configuration-based vulnerabilities.

Question 17: In the Qualys Guard scanning methodology once the TCP port scanning has been performed mention the detection test?

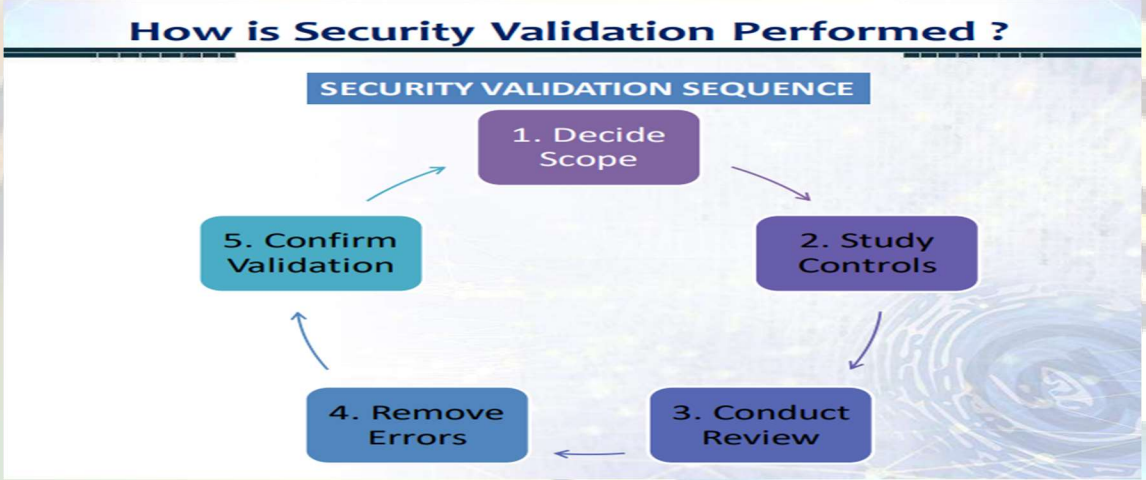
Answer: OS Detection

− Once the TCP port scanning has been performed, the scanner tries to identify the operating system running on the host.
− This detection is based on sending specific TCP packets to open and closed ports.

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



Q no 19: 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

Q No 20: 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

Q No 21: 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. 22: Mention any two factors behind insecure software.

01, Connectivity,

02, Extensibility.

03. Complexity:

Q No 23: Write name of any five activities performed in accreditation process.

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

Q No. 24: 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

Q No 25: Yeh question atta hai Responsibility ni hoti to apne activity and Detail ko 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

Q No 26: What type of assets do not have a CIS/DISA STIG?

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

– Other applications such as asterisk deployments

Q No 27: Typical security tools used in an enterprise:

– Enterprise antivirus
– MS Active Directory (AD)
– Vulnerability manager
– Logs management
– Network & performance monitoring
Automated backups

Q No 28: Topic No 25: Major Components: Enterprise IT Network

- Edge router
- NGN FW
- DMZ:
- IPS & N-DLP
- Distribution switch
- Data center switch & FW
- Access switch

• NAC

Q No 29: Comparison of CIS Vs DISA

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

Q No 30: CIS benchmark in profile applicability

– Profile applicability (ASA 8.X, ASA 9.X)
– Description
– Rationale
– Audit
– Remediation
– Default value
– References

Q No 31: Disa STIG component/content names

STIG content:

– General information (title)

– Discussion
– Check content
– Fix text
– CCI (References)

Q No 32: OWASP Software Assurance Maturity Model (SAMM) Governance Phase:

– Strategy & Metrics
– Education & Guidance
– Policy & Compliance

Q No 33: OWASP Software Assurance Maturity Model (SAMM) Construction Phase:

– Security Requirements
– Threat Assessment
Secure Architecture

Q No 34: 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

- OWASP Software Assurance Maturity Model (SAMM) **Governance Phase:**

Q No 35: What is business continuity? (BC.)

– Business Continuity (BC) is the capability of the org to continue delivery of products or services at acceptable predefined levels following a disruptive incident

Q No 36: How web and email can secured against malware and attacks in enterprise.

To secure web and email in an enterprise, implement antivirus software, firewalls, and intrusion detection systems. Train employees on security best practices, use email encryption, update software, employ MFA, monitor traffic, backup data, and conduct security assessments

Q No 37: Software security flow?

Software security flow refers to the systematic process of identifying, assessing, and mitigating security risks and vulnerabilities in software applications, following a structured approach to ensure the development of secure and robust software systems.

Q No 38: Remote exploit: **(Yeh remote local wala table shape main bhe a sakta hai)**

– A remote exploit works over a network and exploits the security vulnerability **without any prior access** to the vulnerable system.

• **Local exploit:**

– **A local exploit requires prior access to the vulnerable** system and usually increases the privileges of the person running the exploit past those granted by the system administrator.

Q No 39: Ensure Use of Only Fully Supported Browser & Email Clients:

Ensure that only **fully supported web browsers & email clients are allowed** to execute in the org, ideally only using the latest version of the browsers & email clients provided by the vendor.

Q No 40: This table was given and arrange this

Whose Responsibility Is InfoSec Governance ?

TYPICAL ORGANIZATIONAL TIERS AND RESPONSIBILITIES

TIER	RESPONSIBILITY
BOARD (STEERING COMMITTEE)	ORGANIZATIONAL COMMITMENT, APPROVE BUDGET, DIRECT
IT MANAGEMENT (CIO)	REVIEW, MONITOR, PROPOSE
CISO/SECURITY HEAD	PLAN, BUILD, RUN
IT & SECURITY TEAMS	IMPLEMENT/EXECUTE

Q No 41: Question: Mention the name of frame work against which nessus scanner gives configuration auditing feature?

Answer: – Configuration auditing:

CERT,

CIS,

COBIT/ITIL,

DISA STIGs,

FDCC, ISO,

NIST,

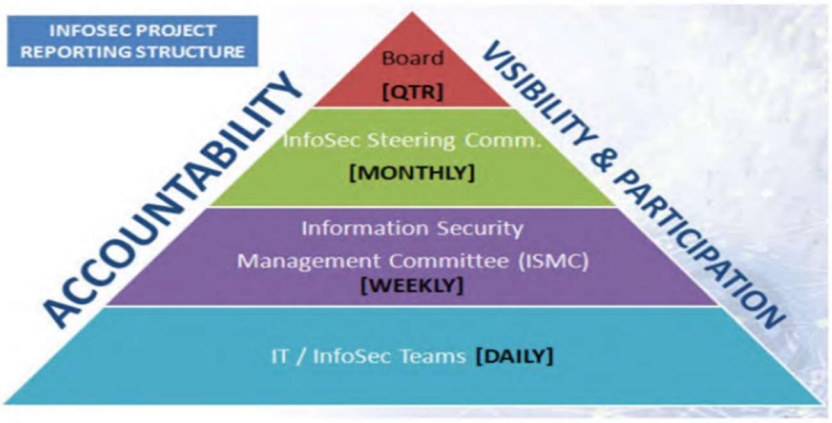
NSA

Q No 42: Identify two security function from the Asset management helps with the following security functions:

Answer: Patch management

Enterprise tracking and reporting

– Annual appraisals, security awards and recognition



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

Q No 43: **Three types of redundant site models:**

• Hot site • Expensive site

Cold site • Cheapest

• warm site

– 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

Q No 44: Backup considerations:

– What to backup?

– Backup location?

– Freq of backup?

– Backup operator?

– Backup checker (verification)? – Backup test & security methods? – Technology & tools used for backup

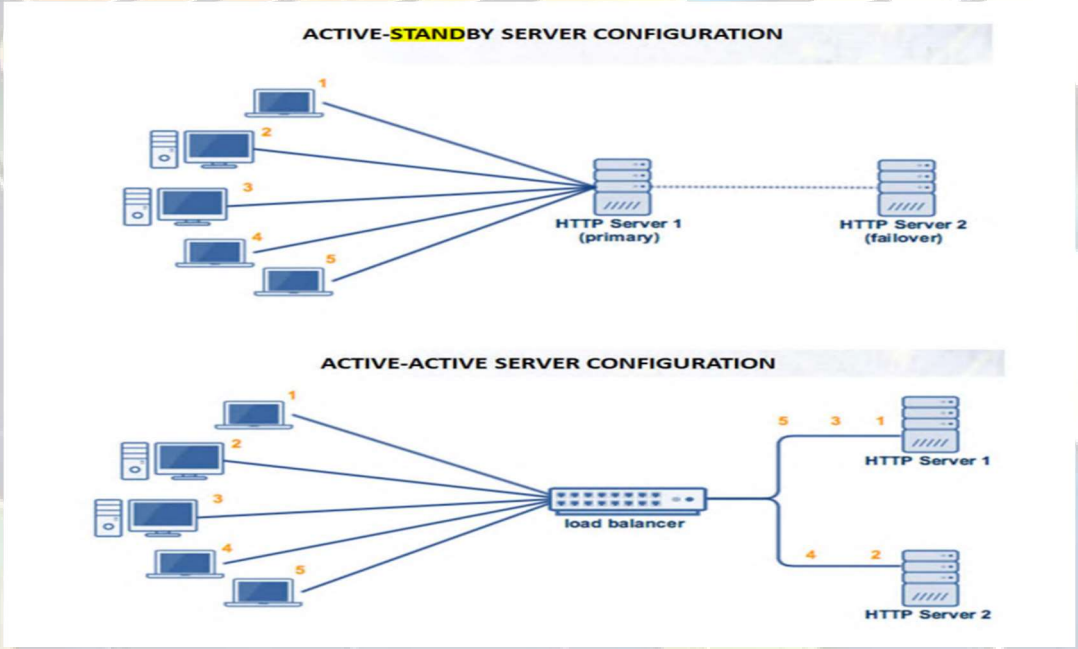
Q No 45. Yeh CAT 1,2, ya 3 wale detail oper niche ho gi arrange kerne ho gi yeh detail.

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

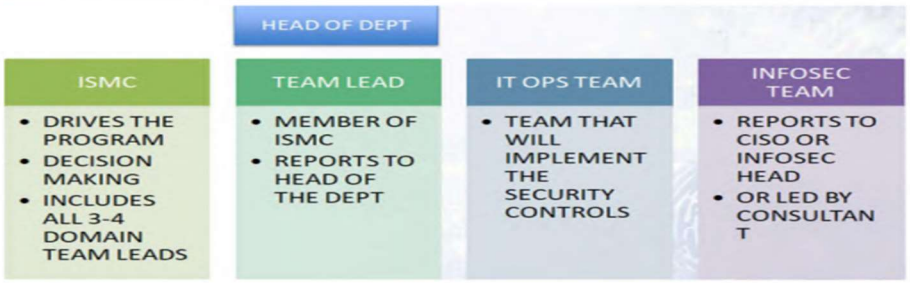
curity

Q No 46: **Write the Names of Common SIEM solution for security Event detection?**

A. LOgRhythm
B. IBM Q-Radar
C. Splunk



Q no 47: 8 Step Methodology.



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

- **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 incident

Allowing Auto play to execute may introduce malicious code to a system	True
Auto play begins reading from a drive as soon media is inserted into the drive	True
– By default, Auto play is disabled on removable drives, such as the floppy disk drive (but not the CD-ROM drive) and on network drives.	True
By default, Auto play is disabled on removable drives,	True

- 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

Major Component of IT Enterprise IT NERWORK

• 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

– Switch port 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 check-in

• UTM – Multi-featured NGN FW device

• Mobile device

– MDM –

Security features for mobile device

• 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

• **Business stakeholders:** – Provide downtime approvals if required – Help to engage other vendors if applicable

Question: Write the First step in automated Security hardening and validation name of tool Used?

Answer: Step 1: Scan an IT asset using Qualys compliance scan, NESSUS compliance scan, or CIS CAT PRO Tool

Question No: Enlist the first five CIS controls that eliminate the vast majority of your organization vulnerability

Ans: Following are the first five CIS control among CIS 20 controls.

A. Inventory of Authorized and unauthorized devices.

B. Inventory of Authorized and unauthorized software.

C. Secure configuration for software of hard ware

D. Continues vulnerability assessment and remediation

. E. Controlled use of administrative privilege.

Question no 12 : 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

Question No 12 : Three pillars of information security Implemention: (yeh implementation hai)

– People
– Process
– Technology