You tube channel Digital world VU

CS 205 past papers files and Important Questions for Final exams Fall 2022

Made by Muhammad Qasim Ali

For any query contact 03337435091. Qasim.tahir.sngpl.com.pk

Q No: 1: 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

• Celebrate Success! – Hold team celebrations – Recognize quiet workers and background workers as well – Promote team achievements

Q No 02: Security transformation project:

• Security transformation project:

– Project initiation: 2 Mths

You tube channel Digital world VU

– 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 03: 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. – This is the most fundamental step in defining security goals in a way that's both measurable and aligned with the organization's real business risk.

• **Education & Guidance:** – Focused on arming personnel involved in the software lifecycle with knowledge and resources to design, develop, and deploy secure software. – With improved access to information, project teams will be better able to proactively identify and mitigate the specific security risks that apply to their organization.

• **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. – A driving theme for improvement within this Practice is focus on project-level audits that gather information about the organization's behavior in order to check that expectations are being met.

Q no 4: IT Security functions

– Network security

– Systems security

– Application & database security

– Mobile security

Q No 5: 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 6: 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 7: What is a patch?

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

– "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 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

– Defects in clients like web browsers, email programs, image viewers, instant messaging software, and media players may allow malicious websites, etc. to infect or compromise your computer with no action on your part other than viewing or listening to the website, message, or media

Q No 08: 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 09: very important. Security Breach in 2014

How much card played: • 56 million payment cards compromised

How much people effected; Affected 78.8 million individuals

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

• 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).

– The stolen payment cards were used to put up for sale and bought by carders. The stolen email addresses were helpful in putting together large phishing campaigns.

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: Topic no 46: What Does "Box Security" Mean? (Important repeated)

• "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

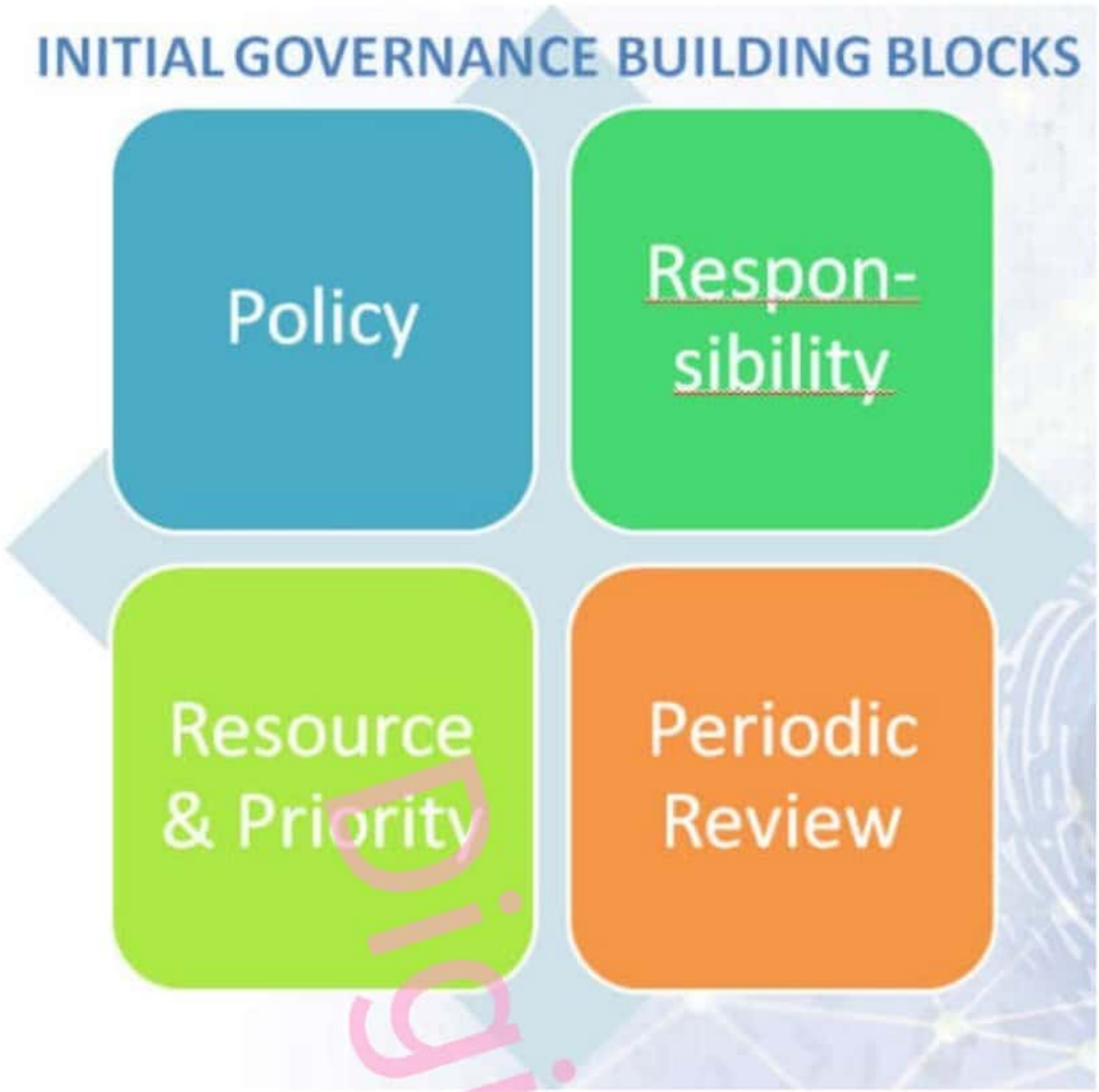
– Network Forensics

– Others

Q No 13: 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: 14: Info security governance initial block detail.

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 15: Topic No 198: How To Build Effective InfoSec Governance? (Imp Repeated)

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

– Leadership

– Strategy

– Structure

– Reporting

– Project management

– Culture

You tube channel Digital world VU

Q NO *** : 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.

20.4: Include Tests for Presence of Unprotected System Information and Artifacts

• Include tests for the presence of unprotected system information and artifacts that would be useful to attackers, including network diagrams, configuration files, older penetration test reports, e-mails or documents containing passwords or other information critical to system operation.

20.5: Create Test Bed for Elements Not Typically Tested in Production

• Create a test bed that mimics a production environment for specific penetration tests and Red Team attacks against elements that are not typically tested in production, such as attacks against supervisory control and data acquisition and other control systems.

20.6: Use Vulnerability Scanning and Penetration Testing Tools in Concert

• Use vulnerability scanning & penetration testing tools in concert. The results of vulnerability scanning assessments should be used as a starting point to guide & focus pen testing efforts.

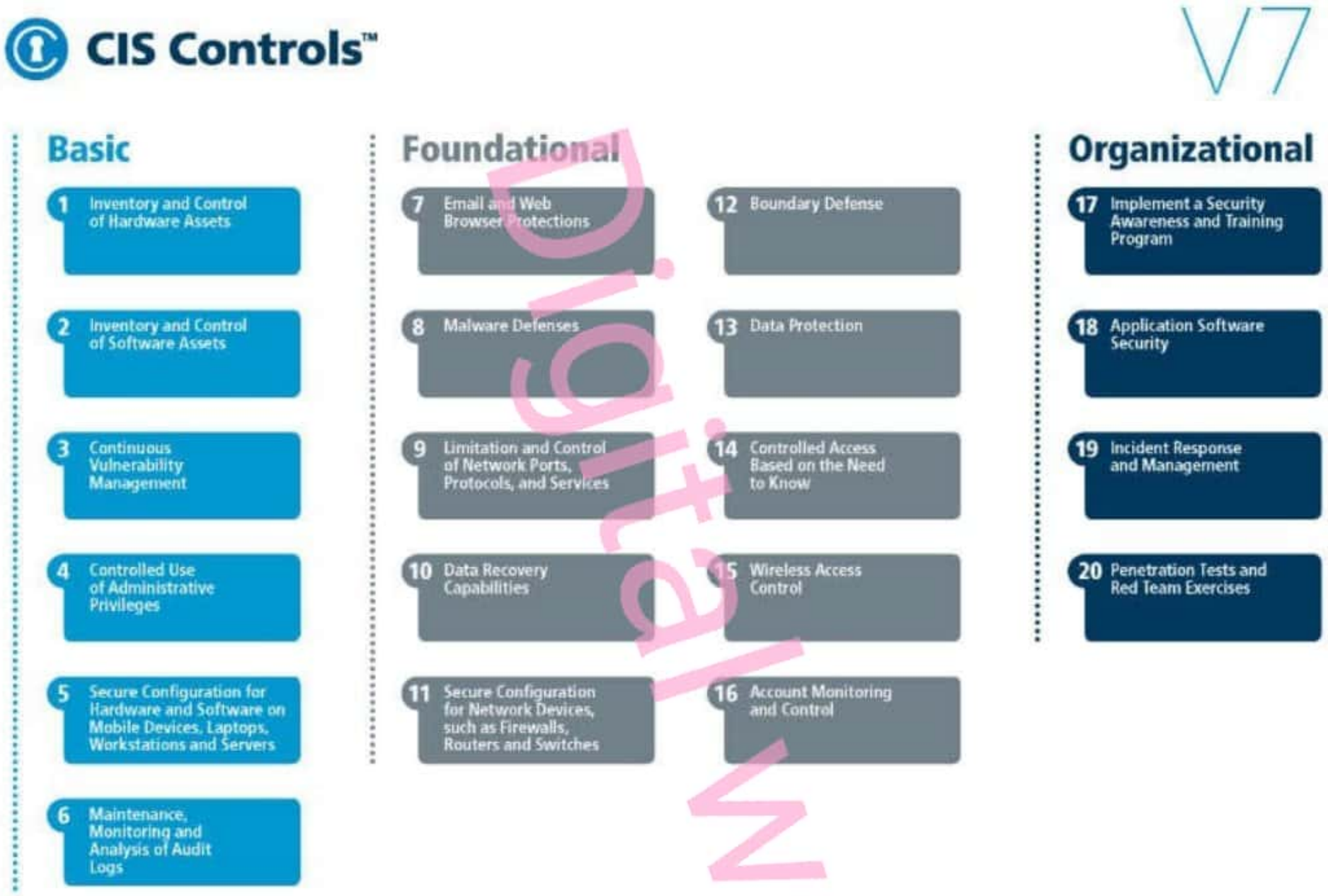
20.7: Ensure Results from Penetration Test are Documented Using Open, Machine readable Standards

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

20.8: Control and Monitor Accounts Associated with Penetration Testing

• Any user or system accounts used to perform penetration testing should be controlled and monitored to make sure they are only being used for legitimate purposes, and are removed or restored to normal function after testing is over.

Most Important: (read and keep in mind about steps Basic Foundational and organizational)



Q NO 16: Monitor and Detect Any Unauthorized Use of Encryption

You tube channel Digital world VU

• 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 17: 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 18: 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

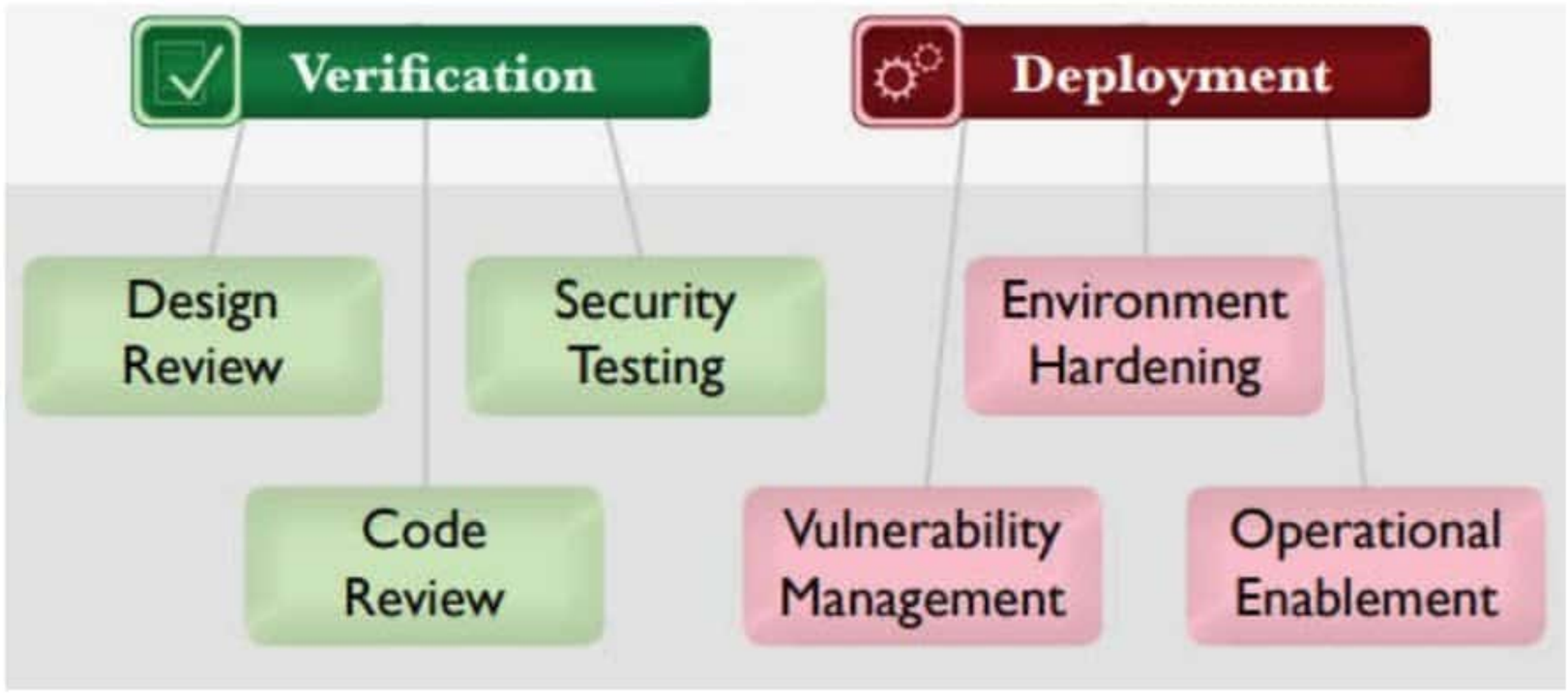
• OWASP Software Assurance Maturity Model (SAMM) Verification Phase:

– Design Review

– Code Review

– Security Testing

You tube channel Digital world VU



Q Bo 19: 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 20: topic 235 RISK MANAGEMENT – FRAMEWORK

– RISK MANAGEMENT – FRAMEWORK

• The principles of risk management and the framework are closely related.

• For example, one of the principles is that risk management should be integrated and one of the components of the framework is **integration.**

• The principle outlines what must be achieved, and the framework provides information on how to achieve the required **integration.**

• The ISO 31000 guidelines are centered on leadership and commitment.

• The effectiveness of risk management will depend on its integration into all aspects of the organization, including decision-making.

• The remaining components of the framework are **design, implementation, evaluation** and **improvement**. This approach is often represented in management literature as plando-check-act.

• ISO 31000 provides narrative description of how the framework should support risk management activities in an organization.

You tube channel Digital world VU

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

RISK MANAGEMENT FRAMEWORK

- ARCHITECTURE
- STRATEGY
- PROTOCOLS

Table 2: Risk management framework

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

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

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

Q No 21: 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.

Plan:

1. Identify intended benefits of the RM initiative and gain board support

2. Plan the scope of the RM initiative and develop common language of risk

3. Establish the RM strategy, framework and the roles and responsibilities

Implement:

4. Adopt suitable risk assessment tools and an agreed risk classification system

5. Establish risk benchmarks (risk criteria) & undertake risk assessments

6. Determine risk appetite and risk tolerance levels and evaluate the existing controls

Q No 22: Topic No 234: ISO31000:2018 – RISK MANAGEMENT – 8 **PRINCIPLES**
PRINCIPLES:

1. Framework and processes should be customized and proportionate.
2. Appropriate and timely involvement of stakeholders is necessary.
3. Structured and comprehensive approach is required.
4. Risk management is an integral part of all organizational activities.
5. Risk management anticipates, detects, acknowledges and responds to changes.
6. Risk management explicitly considers any limitations of available information.
7. Human and cultural factors influence all aspects of risk management.
8. Risk management is continually improved through learning and experience.

 The first five principles provide guidance on how a risk management initiative should be designed, and principles six, seven and eight relate to the operation of the risk management initiative.

Risk management Frame work 05 component:

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

Q No 23: 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 No24: 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 25: Which steps are include in ensuring INFOSEC ASPECTS OF BUSINESS CONTINUITY MNGMT

You tube channel Digital world VU

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 26: 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 27: What are five steps in business continuity plan management. (please verfy this)

Five phases of development and maintaining business continuity plan

Phase1: Initiation

Phase 2: Business impact analysis

Phase 3: Development recovery strategies

Phase 4: Implementation

Phase 5: Test and monitor

IMPORTANT TOPIC ↓ ↓

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)

What are some of the common vulnerability scanners?

- OpenVAS
- Nessus
- Qualys
- Rapid7

Zero-day exploit:

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

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

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

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.
• It tries to use exactly the same discovery and information 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.

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

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

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

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

Pakistan's InfoSec paradigm

– Governance overkill
– Reactive
– Superficial
– Complete absence of underlying security controls

Topic No 198: How To Build Effective InfoSec Governance?

Topic No 202: Role Of CISO In Driving Infosec Program

Topic No 203: Key Inhibitors For Security Program Failure

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.

Topic No 211: ISMS: Leading InfoSec 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

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 realising benefits and optimising 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 optimises IT investment and use for the
benefit of stakeholders (ISACA)

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

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

- **T**hose 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.

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

You tube channel Digital world VU

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?**

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

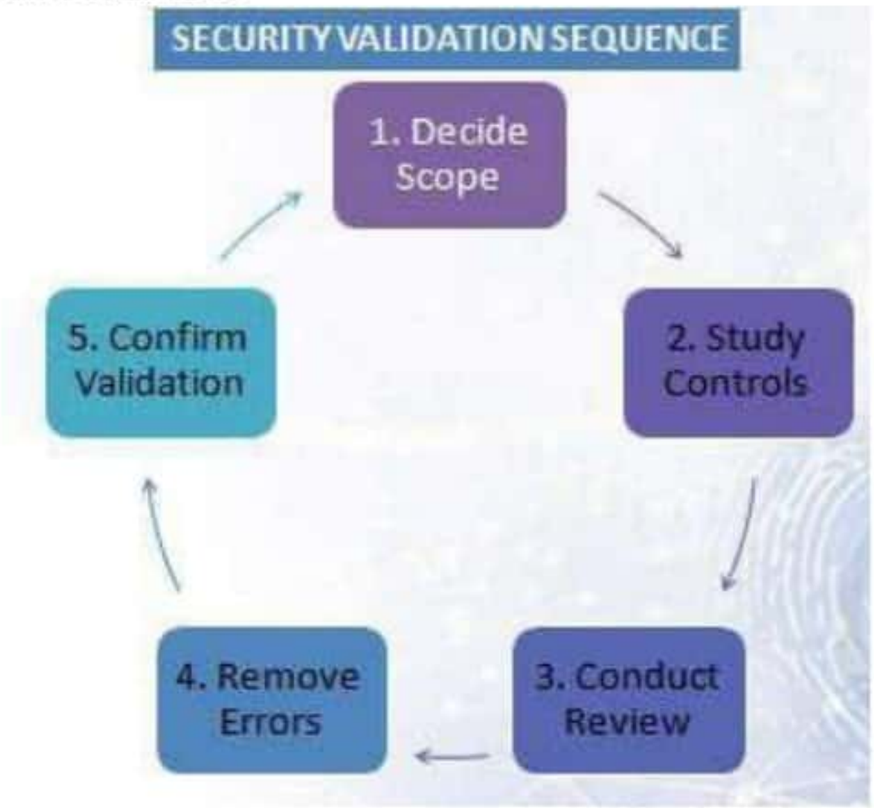
I. the IT teams

II. Who conducts security validation?

Security controls are validated by INFORMATION SECURITY TEAM or by 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**



Types of security testing:

– Vulnerability assessment (VA)

- Penetration testing (PT)
- Other security tests through various automated tools
- Code review (initiated in test environment)

What is security accreditation?

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

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

Topic No 270: Embedding Info Sec In to Project Management

- PMIs five phases of project management:

- Initiate
- Plan
- Executing
- Controlling
- Closing

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

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

- Regulatory fines, legal consequences

• **Prevention Of Fraud & Pilferage:**
– An effective Information Security Program makes it harder to conduct fraud, abuse, or misuse without getting detected
– Controls in business process
– Audits
• **A Reliable & Robust IT Setup**:– Business continuity & DR– Redundancy– Backups– Capacity management – Change management

Types of network redundancy.

What are Five steps in business continuity plan management.