

CS205 (Live Quiz)

Mid Term

PAID VU LMS HANDLING by Mam Mehwish

03184148783

Past Papers for Mids./Finals are also Available

1. For security hardening of Internet Explorer browser, users can allow or deny add-ons through
 - Work Group
 - Active Directory
 - Domain Admins
 - ✓ Add-On Manager
2. As per CIS control "sa" login account must be
 - ✓ RENAMED
 - UNCHANGED
 - DELETED
 - DISABLED
3. In Active Directory Domain, ._.-_- group is a highly privileged group.
 - The Domain Member
 - The Domain Guests
 - The Domain Users
 - ✓ The Domain Admins
4. Shells with permissions give the ability to maliciously modify the shell to obtain unauthorized access.
 - world/group-delete
 - world/group-append
 - world/group-read

- ✓ world/group-write
5. **What is the function of security team in security hardening?**
- Ensure IT ops team receives required guidance and support
 - Report the completion of controls implementation to ISMC
 - Study the security controls
 - ✓ Conduct validation of implemented security controls
6. **Which variants of Microsoft SQL server exist on CIS website?**
- 2012, 2014, 2016
 - 2008, 2012, 2014
 - ✓ 2008, 2012, 2016
 - 2003, 2008, 2012
7. **What does DR plan include?**
- Directions for how to reach recovery site
 - All of the given
 - A diagram of entire network and recovery site
 - Key personnel and DR team contact details
 - ✓ All of the given
8. **What does check content explain about rule in DISA STIG?**
- Tells how to apply control
 - Describes the control
 - Describes the benefit of implementing control
 - ✓ Tells how to check whether control is implemented or not
9. **Which of the following protocols are used for remote administration of a system?**
- ✓ SSH & Telnet
 - TCP and IP
 - SSH and FTP
 - TCP and UDP
10. **If account lockout feature value is set to "0" on a MS 2012 member server then?**

- Will require administrator to unlock the account
- The account will be locked and system will have to be rebooted
- Will have to disconnect from network
- ✓ The account will never be locked despite of several failed login attempts

1. As per ISACA, risk should be managed so that:

- ✗ People do not have accidents in the workplace
- ✗ The board and senior management may be entitled to bonuses
- ✗ The organization is profitable
- ✓ There is an acceptable level of assurance and predictability to the desired outcomes of any organizational activity

2. What is the advantage of offsite backup in an enterprise IT network?

- ✗ Less expensive than onsite backup
- ✗ Immediate access to data
- ✓ Data will be preserved in case of some catastrophic event
- ✗ Internet access not needed for taking or restoring backup

3. During the "test/validate" stage:

- ✗ All security projects & activities are presented on a dashboard
- ✗ A third-party is invited for review
- ✓ The information security team conducts a review of correctness and coverage of security control implementation
- ✗ The security project charter is reviewed

4. A guideline:

- ✗ Applies to the entire organization
- ✗ Is for satisfying audits only
- ✓ A statement of best practice that further elaborates the procedure/SOP
- ✗ Is mandatory

5. People, process, and technology can be described as:

- A three-tiered approach for cyber security standards implementation
 - A business implementation approach for effective project management
 - Three important areas which have to be addressed for effective information security implementation
 - The responsibility of top management
6. Policies and procedures are part of _____ layer in information security transformation framework:
- Security governance
 - Security engineering
 - Vulnerability management
 - Security hardening
7. The following clause from NIST SP800-50 document refers to: "strives to produce relevant and needed security skills and competencies":
- Training
 - Education
 - Job description
 - Awareness
8. "CIS security benchmarks will be used to harden all IT assets." For security hardening, the above statement can be best described as:
- A procedure
 - A recommended action
 - A standard
 - A guideline
9. The ITU global cyber security index (GCI) covers:
- Legal, technical, organizational, capacity building and cybercrime
 - Legal, technical, organizational, capacity building and cooperation
 - Legal, technical, organizational, business and cooperation
 - Legal, technical, military, capacity building and cooperation

10. One of the challenges in effective implementation of a security transformation project in a small-sized organization is:

- X Lack of a disaster recovery (DR) site
- X Multiple data center sites
- X Old and outdated IT environment
- Adhoc culture and lack of discipline

"CIS security benchmarks will be used to harden all IT assets" For security hardening, the above statement can be best described as:

- A) A guideline
- B) A procedure
- C) A standard
- D) A recommended action

2. How high availability can be designed in an enterprise IT network?

- A) At device level (combination of multiple redundant devices)
- B) All of given
- C) At device level (within single device)
- D) At system level (data center or service)
- B) All of given

3. Authentication, access control, data confidentiality, data integrity, non-repudiation, availability are covered by

- A) None of the given
- B) Security attack
- C) Security service
- D) Security mechanism

4. ISO 27001:2013 (ISMS) clause 5.1 talks about _____

- A) Policy and objectives, integration into processes, resources, communication, promoting continual improvement, intended outcomes
 - B) None of the given
 - C) Policy, resources, continual improvement, quarterly board review
 - D) Internal audit
 - A) Policy and objectives, integration into processes, resources, communication, promoting continual improvement, intended outcomes
-

5. There are main pillars of information security.

- A) Confidentiality
 - B) Integrity
 - C) Availability
 - D) All of the above
-

6. IT/ Infosec Teams require information security project report at

- A) Quarterly
 - B) Monthly
 - C) Daily
 - A) Quarterly
-

7. What information needs to be backed up in an enterprise IT?

- A) OS configuration backups
 - B) Database and application data
 - C) Network configuration files
 - D) All of the above
-

8. Identifies issue and scope.

- A) Standard
- B) Procedure

- C) Guideline
-

9. Layer 2 of the security transformation model emphasis on

- A) Identifying vulnerabilities through a risk-based approach
 - B) Security governance
 - C) PCI
 - D) Vulnerability management program
-

10. The information security transformation model:

- A) Four layers, with the first layer being on the bottom: security hardening
- B) Is an international model developed by ISACA and is widely deployed globally
- C) Necessary, however, models are only for reference purposes
- D) Have four layers with the first and most important layer on the top: security governance

1. Regulation of the industry is important in order to _____.

Options:

- A) Protect the economy from being derailed
- B) Protect from website defacement
- C) Ensure excessive profit is not extracted
- D) Drive effective security adoption, and implementation and protection of critical national infrastructure

Correct Option: C

2. 'Security is everyone's responsibility' means that _____.

Options:

- A) Responsibility should be avoided by outsourcing it functions to third-parties
- B) It is all about good planning
- C) Insurance companies should be engaged to transfer risk
- D) Everyone has a role to play to implement information security in the organization

Correct Option: D

3. The 4 layer security transformation model and ISMS requirements and controls_____.

Options:

- A) Are both separate security projects
- B) Are both separate security programs
- C) May form essential elements of the security program
- D) None of the given

Correct Option: C

4. People, process, and technology together form_____.

Options:

- A) An international cyber security standard
- B) A holistic approach to information security
- C) An approach to security project management
- D) An approach to security project management

Correct Option: B

5. What do you mean by RTO in a business continuity plan?

Options:

- A) Both a & b
- B) Maximum downtime an organization can handle
- C) Minimum frequency of backups
- D) Maximum age of files that an organization must recover from backup storage for normal operations to resume after disaster

Correct Option: D

6. An information security program is_____.

Options:

- A) In fact a cyber security program
- B) The sum total of all security activities planned and executed by the organization
- C) The activity charter of information security department
- D) The sum total of all security audit and assessment activities planned and executed by management

Correct Option: B

7. The typical enterprise IT network has been characterized to help in understanding_____.

Options:

- A) IT components, architecture of the network, and security devices and placement
- B) Audit approach
- C) Security scope
- D) Network layout for technical staff

Correct Option: A

8. Security in the trenches refers to_____.

Options:

- A) Security intelligence
- B) Most basic security hardening activities usually carried out by junior staff
- C) Vulnerability management
- D) A form of ransomware

Correct Option: B

9. How is information security implemented?

Options:

- A) With the help of an information security program
- B) By the business
- C) By IT security teams
- D) By management

Correct Option: B

10. The information security transformation framework is recommended for _____.

Options:

- A) Research organizations and academia
- B) Effective implementation of information security given the current challenges of information security in Pakistan
- C) Information security governance
- D) Military and law enforcement organizations

Correct Option: C

1. _____ are important tasks where the information security manager should be involved.

Options:

- A) Security webinars
- B) Signing off critical change requests, monitoring the vulnerability management program, facilitate incident management process
- C) Threat intelligence
- D) Developing SOPs and guidelines

Correct option: B) Signing off critical change requests, monitoring the vulnerability management program, facilitate incident management process

2. The 4 layer security transformation model and ISMS requirements and controls

_____.

Options:

- A) Are both separate security programs
- B) Are both separate security projects
- C) May form essential elements of the security program
- D) None of the given

Correct option: C) May form essential elements of the security program

3. As per ISACA, risk should be managed so that _____.

Options:

- A) The board and senior management may be entitled to bonuses
- B) The organization is profitable
- C) There is an acceptable level of assurance and predictability to the desired outcomes of any organizational activity
- D) People do not have accidents in the workplace

Correct option: C) There is an acceptable level of assurance and predictability to the desired outcomes of any organizational activity

4. A policy is _____.

Options:

- A) Not mandatory but a guideline only
- B) Mandatory and applies to the entire organization; signed off by senior management
- C) Mandatory and limited in scope to a department
- D) Signed off by the information security department

Correct option: B) Mandatory and applies to the entire organization; signed off by senior management

5. What is the best description of a security standard or framework?

Options:

- A) Blueprint or roadmap for achieving information security objectives
- B) A diagram showing architecture of program
- C) Iso27001:2013 (isms)
- D) Minimum security baseline

Correct option: A) Blueprint or roadmap for achieving information security objectives

6. Layer 2 of the security transformation model emphasis on _____.

Options:

- A) Security governance
- B) Identifying vulnerabilities through a risk-based approach

C) PCI

D) Vulnerability management program

Correct option: B) Identifying vulnerabilities through a risk-based approach

7. Vulnerability management program

Options:

A) Identification

B) Authentication

C) Policy

D) Risk

Correct option: A) Identification

8. As per ISACA, risk _____.

Options:

A) A necessary part of the business

B) Should be eliminated altogether for best security implementation

C) Is a complex concept which only senior management should address at board level

D) Is usually accomplished by ensuring that the impact of threats exploiting vulnerabilities is within acceptable limits at an acceptable cost

Correct option: D) Is usually accomplished by ensuring that the impact of threats exploiting vulnerabilities is within acceptable limits at an acceptable cost

9. Which of the following statements is false?

Options:

A) PCI-DSS has six broad goals and twelve requirements

B) Iso27001:2013 has ten short clauses and a long annex with 14 sections, and 113 controls

C) COBIT has five enablers and seven principles

D) PCI-DSS is applicable only to credit card related industry

Correct option: D) PCI-DSS is applicable only to credit card related industry

1. Which of the following programs is relevant when we are simply trying to “focus attention on security”?

- A) Security education
- B) A degree program
- C) Security training
- D) A degree program
- ****Correct Option:**** C) Security training

2. _____ assigns quantifiable measures.

- A) Guideline
- B) Procedure
- C) Standard
- D) Policy
- ****Correct Option:**** C) Standard

3. A _____ is a blueprint or roadmap for achieving Information Security objectives.

- A) Training
- B) Standard
- ****Correct Option:**** B) Standard

4. The information security manager must _____.

- A) Be delegated and authorized by senior management to run the information security program
- B) Have minimum 10-12 years of related experience
- C) Be holding important certifications from ISACA, isc2, and EC-council
- D) Report directly to the CEO for effective implementation of the security program
- ****Correct Option:**** A) Be delegated and authorized by senior management to run the information security program

5. Information security management committee requires information security project report at _____ basis.

- A) Weekly
- B) Monthly
- C) Daily
- D) Quarterly
- ****Correct Option:** D) Quarterly**

6. Security in the trenches refers to _____.

- A) Vulnerability management
- B) Security intelligence
- C) Most basic security hardening activities usually carried out by junior staff
- ****Correct Option:** C) Most basic security hardening activities usually carried out by junior staff**

7. Regionally, the most well developed cyber security strategy and framework developed by Singapore by ITU is at rank _____.

- A) 1
- B) 2
- C) 3
- D) 4
- ****Correct Option:** A) 1**

8. As per ISACA, risk should be managed so that _____.

- A) The board and senior management may be entitled to bonuses
- B) The organization is profitable
- C) There is an acceptable level of assurance and predictability to the desired outcomes of any organizational activity
- D) People do not have accidents in the workplace
- ****Correct Option:** C) There is an acceptable level of assurance and predictability to the desired outcomes of any organizational activity**

9. People, process and technology can be described as_____.

- A) Three important areas which have to be addressed for effective information security implementation
- B) A business implementation approach for effective project management
- C) The responsibility of top management
- D) A three-tiered approach for cyber security standards implementation
- ****Correct Option:**** A) Three important areas which have to be addressed for effective information security implementation

10. What are the three types of redundant site models in an enterprise network?

- A) Hot site, cold site and warm site
- B) Both a & b
- C) Highly available site, fault tolerant site and DR site
- D) Primary site, secondary site and DR site
- ****Correct Option:**** A) Hot site, cold site and warm site

MAM MEHWISH 03184148783

👩👩 Paid Vu Lms Handling 👩👩

◆ 1 GDB= Rs 100

◆ 1 Quiz= Rs 200

◆ 1 Assignment=Rs 250

◆ Agr complete handling krwatey hain 1 subject ki with all activities= Rs 500 (Half Semester) ◆

LECTURES Play Service Available In Very Low Price. 📄

👩👩 80-100% Marks Guaranteed 👩👩

👩 Miss Mehwish:03184148783 👩

MAM MEHWISH 03184148783