1411E1187

Candidate's Seat No :_____

M.Sc. Sem.-3 Examination

502

Cyber Security & Forensics (EA)

November-2025

Time : 2-30 Hours] **[Max. Marks : 70**

Question 1 Answer the following questions:

i. Explain how the mandatory clauses (4–10) would guide this process.Case: ABC Tech Pvt. Ltd., a growing IT services company, handles sensitive client data across multiple international offices. The organization has decided to adopt ISO 27001:2022 to improve its data security posture. As a cybersecurity consultant, outline the key steps ABC Tech should follow to establish an Information Security Management System (ISMS) in compliance with ISO 27001:2022 — 7Marks

ii. A CEO statement expressing the company's commitment to protecting information assets and meeting all legal and regulatory obligations. Under which ISO clause is this explained and justify with its sub clause. — 7Marks

OR

i. Discuss the requirements of Organizational Roles, Responsibilities, and Authorities. Explain the two primary responsibilities that top management must assign authority. Provide examples of documentation (evidence) an auditor might seek to verify that roles and responsibilities for information security are clearly defined and effectively communicated. — 7Marks

ii. Explain the PDCA model in the context of ISMS and how each phase contributes to continual improvement. What are the three guiding principles of ISO 27001? — 7Marks

Question 2 Answer the following questions:

i. Explain why this migration constitutes a major change that requires formal planning within the ISMS. Mention in detail the four critical aspects that the organization must consider and plan for before implementing this change.E-Comm Retail, an online retailer, currently stores all customer data in its own private data center. To reduce costs and improve availability, Top Management mandates a major change in migrating all customer data and e-commerce applications to a public cloud platform (AWS). This migration will significantly alter the ISMS scope and control environment. — 7Marks

ii. Explain in detail the risk management process.DataSecure Hub, a cloud backup service, identified a High risk that a critical dataencryption key could be — 7Marks

compromised due to a phishing attack targeting administrators.The current likelihood is Frequent and the impact is Catastrophic. The management team has decided to Reduce the risk

OR

i. Outline the five key aspects (what, when, with whom, how, and who) an organization must define when planning for Information Security Communication. Describe the control requirements of Control of Documented Information, focusing on how documentation and records must be protected throughout their lifecycle, including management of distribution, retrieval, and disposition. 7Marks

ii. Explain the critical flow of activities from Planning to Support that ensures an Information Security Management System (ISMS) is both defined and operational. Detail how the outcomes of Clause 6.1 directly influence both Clause 7.2 and Clause 7.3. Justify why insufficient attention to competence and awareness will inevitably lead to non-compliance with Clause 8. 7Marks

Question 3 Answer the following questions:

i. Explain the requirements of Clause 9.1. Detail three key areas or metrics that an organization should monitor and measure to assess ISMS performance. Justify why monitoring the metrics is not sufficient and why a separate step of analysis and evaluation is essential to determine the effectiveness of the ISMS. 7Marks

ii. Explain the required actions an organization must take immediately after a Nonconformity (NC) is identified. Detail the two primary steps of the subsequent Corrective Action Process, focusing on the critical role of Root Cause Analysis (RCA) and the requirement to prevent recurrence. Justify why documenting all corrective actions and their results is mandatory. 7Marks

OR

i. What steps should an organization take to implement continual improvement in its ISMS, and how can it effectively document and monitor these efforts for ongoing ISO 27001 compliance? 7Marks

ii. How can organizations implement an effective monitoring and measurement program for their ISMS? Discuss the tools and techniques that can align this program with the organization's information security objectives. 7Marks

Questions 4 Answer the following questions:

i. What are organizational control? How does the organizational control process work?Explain all the types of organisational control. 7Marks

ii. Analyze the role of personnel in identifying and reporting information securityincidents within the framework of ISO 27001:2022. What strategies can organizationsimplement to encourage prompt reporting of security incidents? 7Marks

OR

i. Discuss the importance of physical controls in an ISMS, focusing on how newphysical security monitoring measures enhance protection against environmentalthreats and unauthorized access in ISO 27001:2022. 7Marks

ii. What are technological controls? Explain the role of technology controls incybersecurity. 7Marks

Questions 5: Attempt any Seven out of Twelve. 14 Marks

1. How do you assess the likelihood and impact of a risk?
2. How do you monitor and review the effectiveness of risk management?
3. What are the benefits of implementing an effective risk management process?
4. Explain the control of documented information.
5. What is the difference between physical, administrative, and technical controls?
6. Give example of technological control in governance and surveillance.
7. What is ISO 27001:2022?
8. If the company is certified under ISO 27001:2013, when will they have to comply with the newest version?
9. What is the Statement of Applicability (SoA)?
10. What are the four categories of Annex A controls?
11. Who can issue ISO 27001 certification?
12. Does ISO 27001 cover GDPR?

.....X.....X.....

P.T.O

1411E1187 -4 Candidate's Seat No :_____

M.Sc. Sem.-3 Examination

502

Cyber Security & Forensics (EB)

November-2025

Time : 2-30 Hours] [Max. Marks : 70

Question 1 Answer the following questions:

i. Explain the steps involved in implementing a firewall configuration that complieswith PCI DSS requirements. 7Marks

ii. Describe the process an organization should follow to identify and change vendor-supplied default passwords and configurations. What tools or methods can assist in thisprocess? 7Marks

OR

i. Explain the payment card flow and the Overview of CDE with a diagram. 7Marks

ii. Explain the critical relationship between Network Segmentation and the failure toadhere to Secure Configuration. Detail the purpose of separating the Cardholder DataEnvironment (CDE) from the rest of the network via firewalls (Requirement 1). Furthermore,justify why maintaining secure configuration standardsis essential, as even a perfectly segmented CDE could becompromised if the components inside it are not securely configured. 7Marks

Question 2 Answer the following questions:

i. Describe the mandatory key management policies and procedures to protectcryptographic keys used for data encryption. Detail three distinct stages of the keymanagement lifecycle and explain the specific security controls for each stage to prevent thekeys from being compromised or misused. Justify why the destruction of expired orcompromised keys is a crucial part of the lifecycle. 7Marks

ii. Explain the primary risk that PCI DSS Requirement 4 is designed to mitigate duringthe transmission of Cardholder Data (CHD) over open, public networks. Detail the mandatorysecurity measures required by the Requirement regarding the use of strong cryptography.Describe why protocols like WEP and SSL/early TLS versions are explicitly forbidden, andwhat an organization must do to ensure that all transmissions of CHD are protected againstinterception and unauthorized disclosure. 7Marks

OR

i. Explain Requirement 5. Detail the primary reasons why anti-malware 7Marks

E1187-5

solutionsmust be continuously maintained (e.g., signature updates, active scanning). Justify whymerely installing an anti-malware solution is insufficient for compliance, emphasizing theneed for monitoring to ensure the mechanism is active on all systems and processes are inplace to address any malware identified.

ii. Explain Patch Management and Vulnerability Risk Ranking. Justify why all identifiedvulnerabilities must be remediated in a timely manner, emphasizing the difference inremediation timeframes for critical- and high-severity vulnerabilities versus lower-riskvulnerabilities. 7Marks

Question 3 Answer the following questions:

i. Explain the two fundamental principles of Identification and Authentication asrequired by Requirement 8 in Detail. 7Marks

ii. Describe the mandatory procedures for controlling and managing Visitors to the CDEand handling Physical Media in detail. 7Marks

OR

i. Describe the Principle of Least Privilege and how it forms the foundational conceptfor both requirements. Detail the necessary documented informationan organization must maintain to demonstrate that user access rights are strictlyaligned with their job function and business necessity. Explain the requirement in establishingstrong access control measures. 7Marks

ii. Detail the mandatory pieces of information regarding the quality of log data and logmanagement infrastructure. Justify why centralizing security iscritical for effective monitoring and forensic analysis, emphasizing the need for synchronizedsystem time. 7Marks

Questions 4 Answer the following questions:

i. How can organizations respond to suspicious activity detected through accessmonitoring? Outline the steps involved in an incident response plan specific to unauthorizedaccess attempts. Explain the importance of real-time monitoring of access to networkresources. 7Marks

ii. What are the key components of a penetration testing report? Discuss the role ofinternal and external penetration testing. How do these tests differ, and what specificobjectives should each type of aim to achieve? 7Marks

OR

i. What are the primary objectives of a PCI DSS audit? How do they enhance the 7Marks

P.T.O

securityof cardholder data, and what preparation steps, including necessary documentation, shouldorganizations take before the audit?

ii. Discuss the importance of fostering a culture of security within the organization tosupport continuous improvement in PCI DSS compliance. What strategies can leadershipimplement to promote this culture among employees? 7Marks

Questions 5: Attempt any seven out of twelve. 14 Marks

1. What is the definition of 'merchant'?
2. What constitutes a Service Provider?
3. Are debit card transactions in scope for PCI? Explain.
4. What is PA-DSS?
5. What is an Approved Scanning Vendor (ASV)?
6. Is Application Penetration Testing part of Penetration Testing in PCI DSS?
7. What is meant by "adequate network segmentation" in the PCI DSS?
8. Do I need vulnerability scanning to validate compliance?
9. Does PCI DSS address penetration testing differently from the external and internal vulnerability assessments? Who performs penetration testing?
10. We only do e-commerce. Which SAQ should we use?
11. Explain different merchant levels.
12. My business has multiple locations. Is each location required to validate PCI compliance?

.....X.....X.....

E1187-7

M.Sc. Cybersecurity and Forensic, Semester- 3 (Final Examination -2025)

CSF 502 EC – ISMS - PIMS

Duration: 2hr 30min **Total Max. 70**

Question 1 Answer the following questions:

i. Describe the Privacy Information Management System based on the ISO/IEC 27701 standard. Discuss its key clauses and how the PIMS framework extends the core principles of an ISMS. 7Marks

ii. Discuss the role of data subject rights as mandated by regulations like the GDPR. How does a PIMS provide the necessary controls and processes to effectively manage and fulfil these rights within an organization? 7Marks

OR

i. Explain the concept of data flow mapping and inventory in a PIMS. Describe the steps involved in creating an accurate data inventory, and justify why this is the foundational first step for any privacy compliance program. 7Marks

ii. Describe the Information Security Management System. Discuss its key components and explain why an organization should implement ISMS. 7Marks

Question 2 Answer the following questions:

i. What is the purpose of privacy monitoring and continuous improvement in the PIMS lifecycle? Explain the role of privacy audits and compliance reviews in maintaining the ongoing effectiveness and adherence to regulatory mandates. 7Marks

ii. Explain the concept of privacy risk assessment within the PIMS framework. Describe the steps involved in identifying, analysing, and evaluating risks to the rights and freedoms of data subjects. 7Marks

OR

i. Describe the essential documentation and records required by a PIMS, such as the Statement of Applicability (SoA) and the Record of Processing Activities. Explain how these documents are critical for demonstrating regulatory compliance and accountability. 7Marks

ii. What is the purpose of monitoring and continuous improvement in the ISMS lifecycle? Explain the role of audits and reviews in maintaining the effectiveness of an ISMS. 7Marks

Question 3 Answer the following questions:

i. Define pseudonymization and the Right to Erasure. How does the implementation of pseudonymization aid in managing this specific data subject right, and what are the technical and legal challenges organizations must overcome to ensure effective erasure? 7Marks

ii. Discuss the key components and considerations for establishing a comprehensive Third-Party Risk Management program within a PIMS. What are the specific contractual and audit measures required to hold data processors accountable for the privacy of data subject information? 7Marks

OR

i. Define the concepts of a Privacy Incident and a Personal Data Breach. How do 7Marks

the processes for breach detection and internal reporting differ from the procedure for notification to supervisory authorities and data subjects under PIMS?

ii. Describe the role of encryption and breach notification in PIMS. Why are these controls essential for maintaining data privacy, especially when dealing with third party data processors? 7Marks

Questions 4 Answer the following questions:

i. Evaluate the influence of Big Data analytics and Machine Learning on PIMS compliance. What are the unique privacy risks introduced by the large-scale collection and processing of personal data for profiling, and how should organizations integrate de-identification and differential privacy to manage these risks? 7Marks

ii. Describe a case study on PIMS adoption in the AdTech or e-commerce industry. Discuss the main challenges faced regarding cookie consent, cross-border data transfer, and targeted advertising, and the technical and policy strategies used to address them. 7Marks

OR

i. Evaluate the influence of Artificial Intelligence (AI) on ISMS and PIMS. What are the potential benefits and risks, and how should organizations adopt their security and privacy measures to account for AI integration? 7Marks

ii. Explain the impact of cloud security on ISMS. How do cloud-specific challenges influence information security policies and practices within an organization? 7Marks

Questions 5: Attempt any Seven out of Twelve. 14 Marks

1. Which ISO standard specifies the requirements for a PIMS?
2. Name one principle of Privacy by Design.
3. What is the main output of a DPIA?
4. Give an example of a data subject right.
5. What is the primary goal of the "Right to Erasure" under GDPR?
6. Which ISO standard specifically addresses Privacy Information Management?
7. Name one key domain in ISMS controls.
8. Give an example of a risk treatment strategy.
9. Which ISMS process focuses on identifying and analyzing risks?
10. What is the primary goal of a Privacy Impact Assessment (PIA)?
11. Name one key control in PIMS designed to protect personal data.
12. Which control focuses on informing individuals about data breaches?

.....X.....X.....