8/36 **2411N821** Candidate's Seat No :_____

IMSc (CSF) Sem.-9 Examination

ICSF-502 (EA)

I.S.M.S.-I.S.O.

Time : 2-30 Hours] **November-2025** **[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. Discuss the role and importance of SoA in linking risk assessment and risk treatment and explain what justifications and documentation should accompany such exclusions to ensure audit readiness. Case: An e-commerce company is preparing its Statement of Applicability (SoA). During review, management decides to exclude teleworking controls, stating that "all employees work on-site." Evaluate this decision. 7Marks

OR

i. 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

ii. As the Chief Information Officer (CIO) of a financial institution, you have been tasked with overseeing the implementation of an ISMS. How would you, in line with Clause 4 and 5, demonstrate leadership and ensure the effective functioning of the ISMS within the organization? 7Marks

Question 2 Answer the following questions:

i. Explain the requirements for Information Security Communication (Clause 7.4) by detailing the five mandatory aspects an organization must define (What, When, With whom, How, and Who). Furthermore, describe the primary controls required by Clause 7.5.3 (Control of Documented Information) to protect critical documents and records throughout their lifecycle, covering key management activities such as distribution, retrieval, and disposition. 7Marks

ii. Explain the inter-relationship between Resources, Competence, and Awareness. Detail the two primary ways an organization must ensure competence and the two 7Marks

P.T.O

primary areas of information security awareness required for all personnel. Justify why insufficient resources directly undermine both competence and awareness initiatives.

OR

i. Outline the five key aspects 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. GlobalTech Inc., which completed its initial risk treatment six months ago, identified a high risk concerning uncontrolled administrator access to production servers. The risk treatment plan mandated the implementation of Multi-Factor Authentication (MFA) and quarterly review of all privileged accounts. An internal audit found that the MFA project was delayed and privileged accounts hadn't been reviewed in nine months, despite the documented plan. Analyze this scenario as a failure in Clause 8 (Operations). Explain sub-clauses GlobalTech Inc. is non-compliant with. Detail the corrective actions required to address both the failure to implement controls and the failure to retain evidence that the processes are being controlled. 7Marks

Question 3 Answer the following questions:

i. DataProtect Solutions conducted its last Internal Audit 18 months ago, despite a documented procedure requiring a 12-month interval. The audit covered only the IT department and ignored HR, Legal, and physical security, even though these areas handle sensitive PII. The audit report produced zero findings, but the subsequent external audit found 12 non-conformities related to staff training (HR) and supplier management (Legal). Analyze the scenario as a failure in Internal Audit. Explain the two primary ways DataProtect Solutions failed to comply with the Clause requirement for a proper internal audit program. Detail the corrective action required to bring the scope and interval of the audit program into compliance 7Marks

ii. Mention in detail all the steps required for Certification Preparation and Audit Readiness. 7Marks

OR

i. WebCorp Media reported an Incident Resolution Time metric of 98% compliance (achieving resolution within the 4-hour SLA) for the past quarter. However, the Management Review minutes (Clause 9.3) show that a system-wide network outage, which lasted 6 hours and was resolved only after external consultant intervention, was deliberately categorized as a "maintenance event" to keep the resolution time metric compliant. No actions were recorded regarding the high cost and reliance on the consultant. Analyse the scenario and explain in detail two mandatory outputs (actions or decisions) that Top Management should have documented in the review minutes, even if the incident was excluded from the metric, to ensure continual improvement of the ISMS. 7Marks

ii. 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

Questions 4 Answer the following questions:

i. Explain the role of Threat Intelligence as a new organizational control in ISO 27001:2022. How does it contribute to enhancing an organization's information security strategy? 7Marks

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

OR

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

ii. What are examples of technological control in smart devices and the IoT? How does employee monitoring use technological control? 7Marks

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

1. How do you check if a company is ISO 27001 certified?
2. What is the difference between clauses 0-3 and clauses 4-10 in ISO 27001:2022?
3. How do you assess the likelihood and impact of a risk?
4. How do you monitor and review the effectiveness of risk management?
5. What are the benefits of implementing an effective risk management process?
6. Explain the control of documented information.

7. What is the difference between physical, administrative, and technical controls?
8. Give example of technological control in governance and surveillance.
9. What is ISO 27001:2022?
10 If the company is certified under ISO 27001:2013, when will they have to comply with the newest version?
11 What is the Statement of Applicability (SoA)?
12 What are the four categories of Annex A controls?

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

2411N821

Candidate's Seat No :_____

IMSc (CSF) Sem.-9 Examination
ICSF-502 (EB)
I.S.M.S.-P.C.I.-D.S.S.
November-2025

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

Question 1 Answer the following questions:

i. What are the levels of merchants and services providers? What is the significance of the different levels? 7Marks

ii. Explain the primary objective of PCI DSS Requirement 1 in securing the Cardholder Data Environment (CDE). Describe the critical function of network segmentation and how it relates to firewall rules. Detail three specific requirements related to firewall implementation that must be met to achieve compliance with PCI DSS Requirement 1. 7Marks

OR

i. Analyse this incident with respect to compliance failures in the PCI DSS and explain how strict adherence to Requirement would have acted as compensating controls to prevent or severely limit the scope of this breach. The Target Data Breach (2013) occurred when attackers gained access to Target's network through a compromised account belonging to a third-party HVAC vendor. The attackers then exploited inadequate firewall segmentation to move laterally from the vendor's access point to the Point-of-Sale (POS) systems within the Cardholder Data Environment (CDE), where they stole over 40 million card details. 7Marks

ii. Explain the steps involved in implementing a firewall configuration that complies with PCI DSS requirements. 7Marks

Question 2 Answer the following questions:

i. Analyze the scenario as a failure in PCI DSS. Identify and explain the violation. Detail the two immediate corrective actions that TravelQuick Inc. must be taken. TravelQuick Inc., a travel booking company, stores all necessary payment data in an encrypted database (compliant with Req. 3). However, during an internal audit, it was discovered that a development server backup contained unencrypted, full Primary Account Numbers (PANs) from three years ago. The development team was unaware that the backup process captured this sensitive data, and the data had exceeded the company's documented 90-day retention period 7Marks

P.T.O

ii. SmallBiz Payments, a new merchant, allows its customer service team to communicate payment authorization forms containing full Primary Account Numbers (PANs) to clients via standard, unencrypted email. Furthermore, the point-of-sale (POS) terminal in the office uses a WPA2-PSK wireless network to connect to the CDE, but the network key has not been changed in five years, and the wireless network is not segmented from the corporate network. Identify and explain the violation. 7Marks

OR

i. E-Comm Store, an online retailer, had anti-malware software installed on all servers, but the configuration was flawed. An internal audit found that the signature files on 20% of the servers were over six months old. Furthermore, the daily log review failed to notice that the anti-malware service had been disabled on a key point-of-sale (POS) server for three weeks. This dormant state allowed a sophisticated piece of malware to infect the POS system and start collecting Cardholder Data. Analyze this incident as a critical failure of PCI DSS. Identify and explain the violation and detail the two immediate corrective actions for the same. 7Marks

ii. ABC system implemented a new feature in its payment processing application. The single lead developer (who wrote, tested, and approved the code) used a centralized console to deploy the new code directly to the production server. A vulnerability was later discovered in the new code, allowing an attacker to bypass a control and access payment data. The vulnerability was a known flaw that a mandated security code review should have identified. Identify and explain the violation of Requirement and detail the corrective actions required for the organization to establish a proper change control process that prevents any single person from unilaterally deploying vulnerable code to the production CDE. 7Marks

Question 3 Answer the following questions:

i. Describe the Principle of Least Privilege and how it forms the foundational concept for both requirements. Detail the necessary documented information an organization must maintain to demonstrate that user access rights are strictly aligned with their job function and business necessity. Explain the requirement in establishing strong access control measures. 7Marks

ii. Identify and explain the violation Need-to-Know and the principle of Least Privilege and. Detail the two specific documented procedures that DataSecure Corp. should implement. DataSecure Corp. hired an external consultant to optimize its database (DB) performance within the Cardholder Data Environment (CDE). The IT manager, for simplicity, granted the consultant full administrative privileges on the database server, including the ability to view, modify, and delete all customer payment records. The consultant's actual business need was only read-only access to performance metrics. After the work was completed, the consultant's account was deactivated, but no review of the excessive permissions granted was ever performed. 7Marks

OR

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

ii. Detail the mandatory pieces of information regarding the quality of log data and log management infrastructure. Justify why centralizing security logs is critical for effective monitoring and forensic analysis, emphasizing the need for synchronized system time. 7Marks

Questions 4 Answer the following questions:

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

ii. What are the primary objectives of a PCI DSS audit, how do they enhance the security of cardholder data, and what preparation steps, including necessary documentation, should organizations take before the audit? 7Marks

OR

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

ii. Detail the difference between the external vulnerability scan and the internal vulnerability scan. justify why both must be performed at least quarterly and after any significant change to the network. Furthermore, describe the mandatory requirement for addressing high-risk vulnerabilities and providing evidence of remediation. 7Marks

P.T.O

N 821-8

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

1. What is the definition of 'merchant'?
2. What is the difference between SAQ and RoC?
3. Are debit card transactions in scope for PCI? Explain.
4. Do a user needs vulnerability scanning to validate compliance?
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. We only do e-commerce. Which SAQ should we use?
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.....