2411N822

Candidate's Seat No :_____

IMBA (CSM) Sem.-9 Examination
CSM-MBA-502 (EA)
I.S.M.S.-I.S.O.
November-2025

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

Question 1 Answer the following questions:

i. 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

ii. Case Study: GreenMed Pvt. Ltd. is a healthcare organization storing patient data across its local servers and a cloud platform. While preparing for ISO 27001:2022 certification, the audit consultant asks the company to clearly define the scope of its ISMS. The management is uncertain whether to include third-party cloud services and branch offices within the scope. Explain the purpose and importance of Context of the Organization in ISO/IEC 27001:2022. How does it contribute to the effectiveness of an ISMS? 7Marks

OR

i. 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

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 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

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. 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

ii. 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

N822-3

OR

i. Mention in detail all the steps required for Certification Preparation and Audit Readiness. 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. What is organizational control? How does the organizational control process work? Explain all the types of organisational control. 7Marks

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

OR

i. 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

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.....