2111E754

Candidate's Seat No :_____

M.Sc Sem-3 Examination

502

Cyber Security & Forensic (EA) ISMS-ISO

November-2024

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

Question 1 Answer the following questions:

i. Explain the PDCA model in the context of ISMS and how each phase contributes to continual improvement. 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 5, demonstrate leadership and ensure the effective functioning of the ISMS within the organization? 7Marks

OR

i. What are the three guiding principles of ISO 27001? 7Marks

ii. Explain the steps an organization should take to determine the context in which its Information Security Management System (ISMS) operates as per Clause 4 of ISO 27001. How do internal and external factors influence this context? 7Marks

Question 2 Answer the following questions:

i. Clause 6.1 of ISO 27001 emphasizes the importance of addressing risks and opportunities in the context of ISMS. Explain the steps an organization should take when planning actions to address risks and opportunities. How does this clause help in achieving continual improvement and preventing undesired effects? 7Marks

ii. Discuss how an organization can ensure that the personnel responsible for information security are competent according to Clause 7.2 of ISO 27001. What methods can be used to evaluate and maintain competence? 7Marks

OR

i. Describe the role of effective communication in supporting the ISMS, as required by Clause 7.4 of ISO 27001. How should an organization structure its internal and external communications? 7Marks

ii. Describe the key components of the risk assessment process outlined in Clause 8.2 of ISO 27001. How does systematic documentation and regular review contribute to effective risk management? 7Marks

Question 3 Answer the following questions:

i. Discuss the role of internal audits in the performance evaluation of an ISMS as per Clause 9 of ISO 27001. How should organizations plan and conduct internal audits to ensure they are effective and provide valuable insights? 7Marks

ii. What steps should an organization take to prepare for an ISO 27001 certification audit regarding monitoring, review, and continuous improvement? Discuss the importance of management reviews in this preparation process. 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

(P.T.O)

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. 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. Name new controls that have been added to the ISO 27001 document. 7Marks

OR

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. 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

Questions 5 Attempt any Seven out of Twelve. 14Marks

1. What are mandatory documents for ISO 27001 certification?
2. List two methods an organization can use to raise awareness about information security among its employees, as suggested by Clause 7.3 of ISO 27001.
3. What is the primary focus of operational planning and control as outlined in Clause 8.1 of ISO 27001?
4. What factors influence the frequency of management reviews for the ISMS as per Clause 9.1 of ISO 27001?
5. How does measuring differ from monitoring in the context of Clause 9.1 of ISO 27001?
6. Differentiate between major and minor non-conformities in an ISMS, providing one example of each.
7. Why is it essential to conduct awareness programs as part of ISO 27001:2022 compliance?
8. What was the change in the number of controls in Annex A of ISO 27001 from the previous version to the 2022 update?
9. Which of the following is a new focus area in ISO 27001:2022 compared to previous versions?
   A. Increased emphasis on IT hardware
   B. Greater focus on human aspects of security and supply chain
   C. Emphasis on document control practices
   D. Exclusively technical controls
10. What is the definition of information security according to ISO/IEC 27000?
11. Which document is necessary to demonstrate that an organization has an established ISMS in ISO 27001:2022?
    A. Business Continuity Plan
    B. Risk Management Plan
    C. Information Security Policy
    D. Supplier Management Policy
12. What is the difference between clauses 0-3 and clauses 4-10 in ISO 27001:2022?

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