Roll No. | | | | | | | | | |

(190) SET-I

COER University

END SEMESTER EXAMINATION, EVEN SEMESTER, 2023-24

Time : 3 hour **Semester** : VI **Total Marks : 100**
Program Name : B.Tech **Branch/Specialization** : Cyber Security
Course Code : SOC336 **Course Name** : Information Security Management

Note: All questions are compulsory. No student is allowed to leave the examination hall before the completion of thetime.

Q. No 1	Attempt Any Four Parts. Each Question Carries 5 Marks.	CO	BL
(a)	Explain the difference between the key elements and logical elements of a Network . How do these elements contribute to information security?	CO 1	2
(b)	Describe the three critical characteristics of information (CIA). Why are these characteristics important for understanding information security?	CO 1	2
(c)	Summarize the concept of information states. How does information transition between different states impact its security?	CO 1	2
(d)	Compare between threats and attack vectors. Provide an example of each.	CO 1	2
(e)	Briefly explain the concept of Common Vulnerabilities and Exposures (CVE).How does identifying CVEs help organizations improve their security posture?	CO 1	2

Q. No 2	Attempt Any Four Parts. Each Question Carries 5 Marks.	CO	BL
(a)	Explain the role of the ISO 27000 series in information security management. Briefly compare ISO 27001 and ISO 27002 in terms of their focus.	CO 2	2
(b)	Describe the Plan-Do-Check-Act (PDCA) model and its application within the context of information security management.	CO 2	2
(c)	Outline the key steps involved in a typical incident response plan.	CO 2	3
(d)	Briefly explain the role of digital forensics and investigations in information security. How do they differ from traditional incident response?	CO 2	2
(e)	Explain the steps to which organizations can leverage methodologies and frameworks like those discussed to achieve better information security posture?	CO 2	2

Q. No 3	Attempt Any Four Parts. Each Question Carries 5 Marks.	CO	BL
(a)	Describe the role of contingency planning in ensuring business continuity in the face of security incidents.	CO 3	2
(b)	Discuss two legal or regulatory drivers that influence information security practices in organizations	CO 3	3
(c)	Briefly explain the concept of security certifications in the context of information security management. What are some benefits of obtaining certifications?	CO 3	2
(d)	Summarize with facts that why security awareness training crucial for employees? Explain two key elements that should be included in such training programs.	CO 3	3
(e)	Discuss various practical considerations organizations should address when implementing security frameworks. How can they ensure the frameworks remain effective against current and future threats?	CO 3	3

Q. No 4	Attempt Any Two Parts. Each Question Carries 10 Marks.	CO	BL
(a)	Justify the necessity of having documented information security policies and procedures within an organization. Explain the key elements that a comprehensive information security policy should address.	CO 4	3
(b)	Discuss the role of governance structures in developing and enforcing information security policies. How can organizations ensure effective implementation of these policies across different departments and personnel?	CO 4	2

(c)	Differentiate between security standards, guidelines, and frameworks used in information security management. Provide an example of each and explain how they relate to policies and procedures.	CO 4	3

Q. No 5	Attempt Any Two Parts. Each Question Carries 10 Marks.	CO	BL
(a)	Discuss the concept of accountability in information security management. How can organizations establish a culture of shared responsibility for security across different departments and personnel?	CO 5	4
(b)	Describe the importance of effective teamwork during an information security incident. Outline the key roles and responsibilities of different team members within an incident response plan.	CO 5	3
(c)	Present a hypothetical information security scenario (e.g., data breach, malware attack). Analyze the scenario by identifying the potential security roles involved and their corresponding responsibilities in responding to the situation.	CO 5	4

----------**End of Paper**----------