1. Explain Seven Domains of a Typical IT Infrastructure in detail with examples.
2. Note down the ways to maximize the CIA triad within the LAN domain compliance?
3. Explain in detail steps to identify security incident?
4. Note down the ways to maximize the CIA triad within the Workstation domain compliance?
5. Write case study related to cyber incidence explaining incidence response plan.
6. What are the critical steps involved in identifying corporate risks during pre-incident preparation, and why are they significant?
7. What is a Live Response and why it is Preferred for Malware Detection and Containment?
8. Explain COBIT , ISO/IEC 27001, and why is it important?
9. Explain Goals of Incident Response.
10. What are the key functions of CERTs (Computer Emergency Response Teams)?
11. Explain Containment and Eradication.
12. Why is creating a structured lessons-learned document essential after a major remediation effort? What elements should it include to support future incident handling?
13. How Does Incident Response Support Legal, Regulatory, and Strategic Goals?
14. How do confidentiality, integrity, and availability (CIA triad) relate to information security?
15. Discuss System/Application Domain from IT Domains.
16. What is PCIDSS and HIPAA and Explain it with organization security scenario.
17. Explain in detail Precursor and Indicators with Signs of an Incident
18. How can periodic penetration testing and continuous intelligence updates improve an organization’s ability to mitigate future risks? Provide specific examples of their benefits.
19. Explain compliance law requirements and business drivers in workstation domain?
20. Explain pros and cons of performing a live response evidence collection versus a forensic disk image. Why is a live response the most common method of evidence preservation during an IR?
21. What are the different approaches to remediation, such as immediate, delayed, and combined actions? Under what circumstances should each be implemented?
22. Explain Incident Reporting and Incident Analysis.
23. How Does Incident Response Minimize Damage and Downtime?
24. How to implement network-based and host-based solutions for IOC creation and searching
25. Explain Disaster Recovery & planning of DR.

26. How vulnerability, threat and attack effects the IT security audit?

27. During an investigation, you discover evidence of malware that is running on a system. explain how you would respond and why?

28. Explain Incident Prioritization with example.

29. What are the high-level goals of incident reporting, and how do they align with effective risk communication to both technical and non-technical stakeholders?

30. Elaborate and list the classification of critical control requirements for an IT infrastructure audit.

31. What is Business Continuity Planning (BCP), and how does it integrate with incident response and organizational resilience?

32. What is adjudication under the IT Act?

33. Explain the role of critical assets such as corporate reputation, confidential business information, and payment account data in risk identification. How should exposures to these assets be assessed and prioritized?

34. Explain Types of Computer Security Incidents.

35. Describe the process of combining asset criticality, exposure, and exploit-ability factors to prioritize risks. Provide an example scenario illustrating this process.

36. Elaborate and list the classification of critical control requirements for an IT infrastructure audit.

37. What standards and practices should be followed when documenting metadata and findings in risk reports? Provide examples of format and content organization.

38. What is COBIT and GDPR and Explain it with organization security scenario.

39. Prepare a detailed audit and compliance report for an IT firm specializing in managing digital intellectual properties (IPs).

40. How do cyber espionage and information warfare intersect?

41. What is Section 43A of the IT Act about?

42. Explain how asset criticality and operational dependencies influence the selection of BCP strategies.

43. What are vulnerable resources? Explain with Example.

44. Discuss the role of executive leadership in advocating for and supporting

45. BCP initiatives. How does leadership involvement affect the BCP's success?