UNIT-1

1. How does the Software Development Life Cycle (SDLC) facilitate the systematic development of software, and how do the different phases of SDLC contribute to creating robust and reliable software solutions?
2. You are a cybersecurity consultant, and you have been asked by a medium-sized company to conduct a workshop on the critical characteristics of information. The company's employees come from diverse backgrounds and have varying levels of technical knowledge. Your task is to explain the critical characteristics of information in a clear and detailed manner to help them understand the importance of protecting sensitive information.
3. How do the various components of an information system interact and collaborate to support the efficient processing, storage, and retrieval of data, and how does this integration contribute to achieving organizational goals?

UNIT-2

1. How do ethical considerations impact the decision-making process and practices in information security?
2. Explain in detail the various Integrity models.
3. An employee, John, who holds a "Confidential" security clearance, has been attempting to access a file labeled "Top Secret" on the company's classified information system. The system has raised an access violation alert, indicating that John's access attempt is in violation of the Bell-LaPadula Model.

* What actions should you take in response to this security alert based on the Bell-LaPadula Model principles?
* How will you investigate the incident further to determine the nature and intent of John's access attempt?
* What are the possible consequences for John's access violation, and how will you ensure that similar incidents are prevented in the future while maintaining compliance with the Bell-LaPadula Model?

UNIT-3

* 1. How can organizations conduct a comprehensive risk assessment encompassing risk identification, analysis, evaluation and prioritization and effectively document the results to support informed decision making and risk management strategies?
  2. Explain in detail the Access Control Mechanisms that can be employed in securing the information.
  3. What are the fundamental principles that underlie the concept of information flow and confinement in computer security, and how do they relate to one another?

UNIT-4

1. What is Sphere of protection, Defense in Depth and Security perimeter? What are the key technological components used for security implementation?
2. Discuss in detail about NIST security models publications.
3. Explain how information security policy is implemented as procedure.

UNIT-5

1. Discuss in detail the cryptographic tools used for providing the security.
2. How Scanning and Analysis tools are useful in enforcing Information Security?
3. Explain in detail Physical Security, Security and Personnel.

Part-c

1. How do intrusion detection systems fit into the broader information security landscape, and what are their limitations in providing comprehensive protection for organizations' data and assets?
2. How can organizations ensure that their contingency plans for information security align with their overall business continuity strategy?
3. How does the Access Control Matrix Model address the complexities of modern information systems and data sharing, and what are the challenges and limitations of implementing this model in large-scale environments?

PART-A

1. Why C.I.A triangle is commonly used in information security?
2. When can a computer be a subject and an object of an attack respectively?
3. Why is information security a management problem?
4. Why is a methodology important in implementing the information security?
5. How can organizations effectively mitigate and respond to the ever-evolving landscape of Information Security threats?
6. What is policy? How it is different from law?
7. Distinguish between attack and threat.
8. What are the general categories of unethical and illegal behavior?
9. In risk management strategies, why does a periodic review have to be a part of process?
10. What do you mean by Confinement problem?

## What is the goal of documenting results of the risk assessment?

1. Write short notes on Ring-based Access Control.
2. Define policy and standards.
3. Mention the Drawbacks of ISO 17799/BS 7799.
4. What is firewall? How does it differ from gateway?
5. What are the resources available in web to assist an organization in developing best practices as part of security framework?
6. What are the advantages and disadvantages of using honey pot or padded cell approach?
7. Distinguish between symmetric and asymmetric encryption.
8. What are the seven major sources of physical loss?
9. What are Criteria for selecting information security personnel?