Course Code: 23CS1017 **R23**

SIDDHARTH INSTITUTE OF ENGINEERING & TECHNOLOGY:: PUTTUR
(AUTONOMOUS)
Siddharth Nagar, Narayanavanam Road – 517583

QUESTION BANK (DESCRIPTIVE)

Subject with Code: Information Security Management (23CS1017) **Regulation:** R23

Course & Branch: B. Tech. - CSE – CIC **Year & Sem. :** IV - I

UNIT –I

INTRODUCTION

1	a)	Define Information Security and state its primary objective.	[L1, CO1]	2M
	b)	List any two important events in the history of Information Security.	[L1, CO1]	2M
	c)	What are the critical characteristics of information? Mention any two.	[L1, CO1]	2M
	d)	What is the NSTISSC Security Model? Mention its purpose.	[L2, CO1]	2M
	e)	What is meant by balancing security and access in an information system?	[L2, CO1]	2M
2	a)	Explain the history and evolution of Information Security.	[L2, CO1]	5M
	b)	Describe the concept of Information Security and explain its importance in modern information systems.	[L2, CO1]	5M
3	a)	Explain the critical characteristics of information in detail with suitable examples.	[L2, CO1]	5M
	b)	Discuss the NSTISSC Security Model and explain its role in Information Security.	[L2, CO1]	5M
4	a)	Explain the different components of an Information System and their significance.	[L2, CO1]	5M
	b)	Illustrate the major components of an Information System with a suitable diagram.	[L3, CO1]	5M
5	a)	Discuss the security requirements associated with the different components of an Information System.	[L2, CO1]	5M
	b)	Explain how hardware, software, data, people, procedures, and networks can be secured	[L2, CO1]	5M
6	a)	Explain the concept of balancing security and access in an organization.	[L2, CO1]	5M
	b)	Analyze the trade-off between information security and accessibility with suitable examples.	[L4, CO1]	5M
7	a)	Define the System Development Life Cycle (SDLC) and explain its major phases.	[L2, CO1]	5M

	b)	Describe the importance of incorporating security into the System Development Life Cycle.	[L2, CO1]	5M
8	a)	Explain the Security System Development Life Cycle (Security SDLC) and its major phases.	[L2, CO1]	5M
	b)	Compare the conventional SDLC and Security SDLC with respect to security activities.	[L4, CO1]	5M
9	a)	Analyze the importance of information security in protecting organizational information assets.	[L4, CO1]	5M
	b)	Evaluate the need for integrating security throughout the system development process.	[L5, CO1]	5M
10	a)	Explain how the NSTISSC Security Model can be used to identify different dimensions of information security.	[L3, CO1]	5M
	b)	Analyze the relationship between information characteristics, security requirements, and information protection.	[L4, CO1]	5M
11	a)	Justify the need for a Security SDLC in developing secure information systems.	[L5, CO1]	5M
	b)	Design a basic Security SDLC framework for developing a secure organizational information system.	[L6, CO1]	5M

Course Code: 23CS1017 **R23**

UNIT –II

SECURITY INVESTIGATION

1	a)	Why is Information Security important for an organization?	[L1, CO2]	2M
	b)	List any two business needs for Information Security.	[L1, CO2]	2M
	c)	Define a security threat and a security attack.	[L1, CO2]	2M
	d)	What is an Access Control Matrix? Mention its purpose.	[L2, CO2]	2M
	e)	What is a confidentiality policy? Mention one objective.	[L2, CO2]	2M
2	a)	Explain the need for Information Security in an organization.	[L2, CO2]	5M
	b)	Describe the major business needs that influence the implementation of Information Security.	[L2, CO2]	5M
3	a)	Explain different types of security threats with suitable examples.	[L2, CO2]	5M
	b)	Describe various types of security attacks and their impact on information systems.	[L2, CO2]	5M
4	a)	Differentiate between security threats and security attacks with suitable examples.	[L4, CO2]	5M
	b)	Analyze how security threats and attacks affect the confidentiality, integrity, and availability of information.	[L4, CO2]	5M
5	a)	Explain the legal, ethical, and professional issues associated with Information Security.	[L2, CO2]	5M
	b)	Discuss the importance of ethical and professional responsibilities in Information Security.	[L2, CO2]	5M
6	a)	Explain the basic concepts and objectives of Computer Security.	[L2, CO2]	5M
	b)	Discuss the major components and requirements of a secure computer system.	[L2, CO2]	5M
7	a)	Define an Access Control Matrix and explain its structure with a suitable example.	[L2, CO2]	5M
	b)	Construct an Access Control Matrix for a simple organizational information system.	[L3, CO2]	5M
8	a)	Explain the concept of security policies and their importance in an organization.	[L2, CO2]	5M
	b)	Discuss the major objectives and characteristics of effective security policies.	[L2, CO2]	5M
9	a)	Explain confidentiality policies and their role in protecting organizational information.	[L2, CO2]	5M
	b)	Explain integrity policies and discuss their importance in maintaining	[L2, CO2]	5M

trustworthy information.

10	a)	Compare confidentiality policies and integrity policies with suitable examples.	[L4, CO2]	5M
	b)	Analyze how security policies can be used to address both confidentiality and integrity requirements.	[L4, CO2]	5M
11	a)	Explain hybrid policies and discuss their significance in Information Security.	[L2, CO2]	5M
	b)	Design a suitable hybrid security policy that addresses both confidentiality and integrity requirements of an organization.	[L6, CO2]	5M

Course Code: 23CS1017 **R23**

UNIT –III

SECURITY ANALYSIS

1	a)	Define Risk Management in Information Security.	[L1, CO4]	2M
	b)	What is meant by risk identification? Mention any two sources of security risk.	[L1, CO4]	2M
	c)	Define risk assessment and state its purpose.	[L1, CO4]	2M
	d)	What is an Access Control Mechanism? Mention any two examples.	[L2, CO3]	2M
	e)	What is the Information Flow Problem?	[L4, CO3]	2M
2	a)	Explain the concept of Risk Management and its importance in Information Security.	[L2, CO4]	5M
	b)	Describe the major steps involved in the Risk Management process.	[L2, CO4]	5M
3	a)	Explain the process of identifying security risks in an organization.	[L2, CO4]	5M
	b)	Describe various sources and types of risks that affect information systems.	[L2, CO4]	5M
4	a)	Explain the process of assessing risks in an information system.	[L2, CO4]	5M
	b)	Analyze the factors that should be considered while assessing security risks.	[L4, CO4]	5M
5	a)	Explain the different approaches used for assessing information security risks.	[L2, CO4]	5M
	b)	Evaluate the importance of risk assessment in protecting organizational information assets.	[L5, CO4]	5M
6	a)	Explain the process of controlling identified security risks.	[L2, CO4]	5M
	b)	Discuss different strategies used to control or mitigate information security risks.	[L2, CO4]	5M
7	a)	Explain the concept of Access Control Mechanisms and their role in information security.	[L2, CO3]	5M
	b)	Describe different types of Access Control Mechanisms with suitable examples.	[L2, CO3]	5M
8	a)	Compare different access control mechanisms based on their characteristics and applications.	[L4, CO3]	5M
	b)	Analyze how access control mechanisms help protect information resources from unauthorized access.	[L4, CO3]	5M
9	a)	Explain the Information Flow Problem in information security systems.	[L2, CO3]	5M
	b)	Describe the significance of controlling information flow between different security levels.	[L2, CO3]	5M

10	a)	Explain the Confinement Problem and its significance in secure information systems.	[L2, CO3]	5M
	b)	Analyze the challenges involved in preventing unauthorized information leakage through information flows.	[L4, CO3]	5M
11	a)	Evaluate the relationship between risk assessment, access control, and information flow control in an information security system.	[L5, CO4]	5M
	b)	Design a basic risk-control framework incorporating suitable access control mechanisms for an organizational information system.	[L6, CO3]	5M

UNIT –IV

LOGICAL DESIGN

1	a)	What is meant by a Blueprint for Security? State its purpose.	[L1, CO5]	2M
	b)	Define an Information Security Policy and mention its importance.	[L1, CO5]	2M
	c)	What are security standards and practices? Mention any two examples.	[L2, CO5]	2M
	d)	What is ISO 17799/BS 7799? State its purpose in Information Security.	[L2, CO5]	2M
	e)	What is the purpose of planning for continuity in Information Security?	[L2, CO5]	2M
2	a)	Explain the concept of a Blueprint for Security and discuss its major components.	[L2, CO5]	5M
	b)	Describe the importance of a security blueprint in designing an organization's Information Security program.	[L1, CO5]	5M
3	a)	Explain the purpose, objectives, and components of an Information Security Policy.	[L2, CO5]	5M
	b)	Discuss the role of Information Security Policies in establishing organizational security requirements.	[L2, CO5]	5M
4	a)	Explain the importance of security standards and practices in Information Security management.	[L2, CO5]	5M
	b)	Differentiate between security policies, standards, and practices with suitable examples.	[L4, CO5]	5M
5	a)	Explain ISO 17799/BS 7799 and discuss its significance in Information Security management.	[L2, CO5]	5M
	b)	Describe the major security management principles addressed by ISO 17799/BS 7799.	[L2, CO5]	5M
6	a)	Explain the NIST models and their role in developing effective Information Security measures.	[L2, CO5]	5M
	b)	Analyze the importance of NIST security models in establishing and managing organizational security controls.	[L4, CO5]	5M
7	a)	Explain the VISA International Security Model and its major components.	[L2, CO5]	5M
	b)	Discuss how the VISA International Security Model can be used to strengthen security in financial transactions.	[L2, CO5]	5M
8	a)	Explain the principals involved in designing a secure Information Security architecture.	[L2, CO5]	5M
	b)	Illustrate the major components of a security architecture with a suitable diagram.	[L3, CO5]	5M
9	a)	Analyze the factors that should be considered while designing a security	[L4, CO5]	5M

architecture for an organization.

	b)	Evaluate the importance of integrating security policies, standards, and controls into the security architecture.	[L5, CO5]	5M
10	a)	Explain the concept of continuity planning and its importance to Information Security.	[L2, CO5]	5M
	b)	Describe the major activities involved in planning for continuity of organizational operations.	[L2, CO5]	5M
11	a)	Evaluate the role of security standards and models in developing a comprehensive logical security design.	[L5, CO5]	5M
	b)	Design a basic logical security architecture for an organization incorporating security policies, standards, security controls, and continuity planning.	[L6, CO5]	5M

Course Code: 23CS1017 **R23**

UNIT –V

PHYSICAL DESIGN

1	a)	What is Security Technology? Mention any two security technologies used in an organization.	[L1, CO6]	2M
	b)	Define Intrusion Detection System (IDS). State its primary purpose.	[L1, CO6]	2M
	c)	What is meant by security scanning? Mention any two scanning or analysis tools.	[L1, CO6]	2M
	d)	Define Cryptography and mention its role in Information Security.	[L2, CO6]	2M
	e)	What is Physical Security? Mention any two physical security measures.	[L1, CO6]	2M
2	a)	Explain the role of security technology in protecting organizational information systems.	[L2, CO6]	5M
	b)	Describe the major categories of security technologies used to protect information assets.	[L2, CO6]	5M
3	a)	Explain the concept, objectives, and working of an Intrusion Detection System (IDS).	[L2, CO6]	5M
	b)	Describe the different types of IDS and their applications in Information Security.	[L2, CO6]	5M
4	a)	Explain the process of security scanning and analysis in an information system.	[L2, CO6]	5M
	b)	Discuss the role of scanning and analysis tools in identifying security vulnerabilities.	[L2, CO6]	5M
5	a)	Compare different types of Intrusion Detection Systems based on their characteristics and deployment.	[L4, CO6]	5M
	b)	Analyze how IDS and security scanning tools can work together to identify and respond to security threats.	[L4, CO6]	5M
6	a)	Explain the fundamental concepts of Cryptography and its importance in Information Security.	[L2, CO6]	5M
	b)	Describe the different types of cryptographic techniques used for protecting information.	[L2, CO6]	5M
7	a)	Explain the role of encryption and decryption in securing information.	[L2, CO6]	5M
	b)	Compare symmetric and asymmetric cryptographic techniques with suitable examples	[L4, CO6]	5M
8	a)	Explain different types of Access Control Devices used for protecting physical and logical resources.	[L2, CO6]	5M
	b)	Discuss the role of access control devices in preventing unauthorized access to organizational resources.	[L2, CO6]	5M

9	a)	Explain the major components and measures of Physical Security in an organization.	[L2, CO6]	5M
	b)	Analyze the importance of physical security in protecting information systems and infrastructure.	[L4, CO6]	5M
10	a)	Explain the role of security and personnel in maintaining an effective Information Security environment.	[L2, CO6]	5M
	b)	Discuss various personnel-related security measures used to reduce security risks in an organization.	[L2, CO6]	5M
11	a)	Evaluate the importance of integrating security technology, cryptography, access control, physical security, and personnel security in an organization.	[L5, CO6]	5M
	b)	Design a comprehensive physical security framework for an organization incorporating suitable security technologies, IDS, access control devices, physical security measures, and personnel controls.	[L6, CO6]	5M

Prepared by – Dr. P. Karthikeyan, Associate Professor, CSE Department