

QUESTION BANK

SUBJECT : - INFORMATION SECURITY

SEM/YEAR : VIII/IV

UNIT I - INRODUCTION			
History, What is Information Security?, Critical Characteristics of Information, NSTISSC Security Model, Components of an Information System, Securing the Components, Balancing Security and Access, The SDLC, The Security SDLC			
PART-A			
Q.No	Questions	BT Level	Competence
1	How shall you interpret Information Security?	BTL 2	Understand
2	Name the multiple layers of security that a successful organization should have in its place to protect its operations..	BTL 4	Analyze
3	Define Information Security.	BTL 1	Remember
4	List the characteristics of CIA triangle.	BTL 1	Remember
5	Give the critical characteristics of Information.	BTL 2	Understand
6	Discuss the bottom up approach and top down approach.	BTL 2	Understand
7	Differentiate direct and indirect attacks.	BTL 4	Analyze
8	Give a short note on E-mail spoofing.	BTL 2	Understand
9	What are the measures required to protect confidentiality of information?	BTL 1	Remember
10	Show with the help of a diagram about the components of information Security.	BTL 3	Apply
11	How shall you design the computer as the subject and object of the attack?	BTL 6	Create
12	Assess the importance of a C.I.A triangle	BTL 5	Evaluate
13	Create a diagram for Information Security Implementation.	BTL 6	Create
14	State the responsibilities of Data Owners, Data custodians and Data users.	BTL 1	Remember
15	Examine if the C.I.A. triangle is incomplete, why is it so commonly used in security?	BTL 3	Apply
16	Describe a Security Team in an organization. Should the approach to	BTL 1	Remember

	security be technical or managerial?		
17	What is the use of methodology in the implementation of Information Security?	BTL 1	Remember
18	Compare Vulnerability and Exposure.	BTL 4	Analyze
19	Classify the three components of the C.I.A Triangle. What are they used for?	BTL 3	Apply
20	Information Security is which of the following: An Art or Science or both? Justify your answer.	BTL 5	Evaluate
PART B			
1	Evaluate the various components of Information Security that a successful organization must have. (13)	BTL 5	Evaluate
2	i) List the various components of an information system and tell about them. (8) ii) List the history of Information Security. (5)	BTL 1	Remember
3	i). What is NSTISSC Security Model? (8) ii). Describe in detail about the top down approach and the bottom up approach with the help of a diagram. (5)	BTL 1	Remember
4.	i). Identify the types of attacks in Information Security. (6) ii). Examine E-mail spoofing and phishing. (7)	BTL 1	Remember
5	i). Discuss about the need for confidentiality in Information Security. (7) ii). Explain the file hashing in the integrity of the information. (6)	BTL 2	Understand
6	i) Examine the critical characteristics of information security. (7) ii) Analyse in detail about the advantages and disadvantages of information security. (6)	BTL 4	Analyze
7	Illustrate briefly about SDLC waterfall methodology and its relation in respect to information security. (13)	BTL 3	Apply

8	Describe the Security Systems Development Life Cycle. (13)	BTL 2	Understand
9	i) Compose the roles of Information Security Project Team. (5) ii) Design the steps unique to the security systems development life cycle in all the phases of SSDLC model. (8)	BTL 6	Create
10	i) Illustrate the different types of instruction set architecture in detail. (7) ii) Examine the basic instruction types with examples. (6)	BTL 3	Apply
11	What are the six components of an information system? Which are most directly affected by the study of computer security? (13)	BTL 1	Remember
12	i) Infer about Information Security Project Team. (8) ii) Analyze the methodology important in the implementation of information security? How does a methodology improve the process? (5)	BTL 4	Analyze
13	Analyze the critical characteristics of information. How are they used in the study of computer security? (13)	BTL 4	Analyze
14	Discuss the steps common to both the systems development life cycle and the security systems life cycle. (13)	BTL 2	Understand
PART C			
1	Assess the importance of infrastructure protection (assuring the security of utility services) and how that is related to the enhancement of information security? (15)	BTL 5	Evaluate

12	Formulate which management groups are responsible for implementing information security to protect the organization's ability to function.		BTL 6	Create
13	Evaluate the measures that individuals can take to protect themselves from shoulder surfing.		BTL 5	Evaluate
14	Define the meaning of the term 'Electronic Theft'.		BTL 1	Remember
15	Express about the password attacks.		BTL 2	Understand
16	State are the various types of malware? How do worms differ from viruses? Do Trojan horses carry viruses or worms?		BTL 1	Remember
17	Interpret the following terms: Macro Virus & Boot Virus.		BTL 2	Understand
18	Analyze about commonplace security principles.		BTL-4	Analyze
19	List any five attacks that is used against controlled systems.		BTL 1	Remember
20	What is the difference between a denial-of-service attack and a distributed denial-of-service attack? Which is more dangerous? Why?		BTL 5	Evaluate
PART-B				
1	i). Discuss about the threats. (6)		BTL 2	Understand
	ii). Express about five criterias for a policy to become enforceable. (7)			
2	Illustrate the methods does a social engineering hacker use to gain information about a user's login id and password? How would this method differ if it were targeted towards an administrator's assistant versus a data-entry clerk? (13)		BTL 3	Apply
3	Describe about the types of Laws and Ethics in Information Security. (13)		BTL 1	Remember
4	How will you develop management groups that are responsible for implementing information security to protect the organization's ability to function ? (13)		BTL 6	Create
5	i) State the types of password attacks. (6)		BTL 1	Remember
	ii) Tell the three ways in which an authorization can be handled. (7)			
6	i) Express in detail about : (2)		BTL 2	Understand
	(a) Protecting the functionality of an organization (2)			
	(b) Enabling the safe operations of Applications (2)			
	(c) Protecting data that organizations collect and use (2)			
	(d) Safeguarding Technology Assets in organizations (2)			
	ii) Discuss in detail about worms. (5)			

7	Analyze in detail about Ethics and Information Security. (13)	BTL 4	Analyze
8	i) Examine in detail about Access control list. (8) ii) Give an example of Systems-specific policy. (5)	BTL 1	Remember
9	i) List the Computer Security Hybrid Policies. (7) ii) Describe the types of Computer Security. (6)	BTL 1	Remember
10	i) Quote the confidentiality policies. (7) ii) Discuss in detail about the types of security policies. (6)	BTL 2	Understand
11	i) Explain Integrity Policies. (6) ii) Assess the Secure Software Development. (7)	BTL 5	Evaluate
12	Analyze whether information security a management problem? What can management do that technology cannot? (13)	BTL 4	Analyze
13	Point out why data the most important asset an organization possesses? (13) What other assets in the organization require protection?	BTL 4	Analyze
14	Illustrate which management groups are responsible for implementing information security to protect the organization's ability to function. (13)	BTL 3	Apply

PART C

1	How has the perception of the hacker changed over recent years? (15) Compose the profile of a hacker today.	BTL 6	Create
2.	Evaluate which management groups are responsible for implementing information security to protect the organization's ability to function? (15)	BTL 5	Evaluate
3	Summarize how does technological obsolescence constitute a threat to information security? How can an organization protect against it? (15)	BTL 5	Evaluate
4	Generalize how the intellectual property owned by an organization usually have value? If so, how can attackers threaten that value? (15)	BTL 6	Create

UNIT III- SECURITY ANALYSIS

Risk Management: Identifying and Assessing Risk, Assessing and Controlling Risk – Systems: Access Control Mechanisms, Information Flow and Confinement Problem

PART-A

Q.No	Questions	BT Level	Competence
1	Express the role of Risk Management in Information Security.	BTL 2	Understand
2	Define the four communities of interest responsible for addressing all levels of risk.	BTL 2	Understand
3	Define Risk Identification.	BTL 1	Remember

4	List the Risk Management categorization subdivisions.		BTL 1	Remember
5	Express the Data Asset Attributes.		BTL 2	Understand
6	Distinguish between asset's ability to generate revenue and its ability to generate profit.		BTL 2	Understand
7	Name the types of Information classification.		BTL 1	Remember
8	Evaluate the strategies for controlling risk.		BTL 5	Evaluate
9	State the vulnerabilities in Risk Management.		BTL 1	Remember
10	Design a table to list the threats and their related examples.		BTL 6	Create
11	Classify the Quantitative and Qualitative Risk Control Practices.		BTL 4	Analyze
12	Show with relevant examples show Microsoft follows best practices for Risk Management.		BTL 3	Apply
13	Assess the metric based measures used in benchmarking.		BTL 5	Evaluate
14	Tell the Ten Immutable Laws of Security offered by the Microsoft.		BTL 1	Remember
15	Show the Risk Management.		BTL 3	Apply
16	Point out the significance of Residual Risk.		BTL 4	Analyze
17	Define Mitigate Strategy.		BTL 1	Remember
18	Show the three common methods used to defend control strategy.		BTL 3	Apply
19	Classify the information contained in the computer or personal digital assistant. Based on the potential for misuse, what information would be confidential, sensitive, unclassified for public release?		BTL 4	Analyze
20	Generalize the strategies for controlling risk.		BTL 6	Create
PART-B				
1	Discuss in detail about Risk Management.	(13)	BTL 2	Understand
2	Describe and draw the components of Risk Identification.	(13)	BTL 1	Remember
3	i) Define Information Classification Scheme. ii) Describe the threats that represent danger to organization's information.	(3) (10)	BTL 1	Remember
4	Design and develop Risk Assessment using sample TVA spreadsheet.	(13)	BTL 6	Create
5	i) Design Risk control strategies. ii) Examine Risk Handling Decision points.	(8) (5)	BTL 1	Remember
6	i). Summarize Cost Benefit Analysis. ii). Distinguish the Defend control strategy and Transfer control strategy.	(9) (4)	BTL 2	Understand
7	i). Discuss in detail about Benchmarking.	(7)	BTL 4	Analyze

	ii). Explain with an example about the best practices followed in an organization. (6)		
8	Assess the reasons to why the periodic review be a part of the process in risk management strategies. (13)	BTL 5	Evaluate
9	Examine as to how Risk appetite varies from organization to organization. (13)	BTL 3	Apply
10	i) Analyze which is more important to the systems components classification scheme. (7) ii) Describe Incidence Reponse Plan. (6)	BTL 4	Analyze
11	Express the Security Incident Handling. (13)	BTL 2	Understand
12	i) Explain in detail about Information Flow. (7) ii). Pointout the Confinement Problem. (6)	BTL 4	Analyze
13	i) Define Access Control List. (8) ii) Differentiate between various Feasibility Studies for organization's strategic objectives. (5)	BTL 1	Remember
14	With a suitable diagram . examine about the Risk Management. (13)	BTL 3	Apply

PART C

1	Formulate the points for Hardware , Software and Network Asset Identification. (15)	BTL6	Create
2	Explain in detail about System Access control Mechanism. (15)	BTL 5	Evaluate
3	Evaluate with a proper example about the Risk Identification in detail. (15)	BTL 5	Evaluate
4	Develop necessary points with any example for Assets Identification and valuation. (15)	BTL 6	Creating

UNIT IV-LOGICAL DESIGN

Blueprint for Security, Information Security Policy, Standards and Practices, ISO 17799/BS 7799, NIST Models, VISA International Security Model, Design of Security Architecture, Planning for Continuity

PART-A

Q.No	Questions	BT Level	Competence
1	Distinguish between Physical Design and Logical Design.	BTL 2	Understand
2	Express significant points in Information Security Blueprint.	BTL 1	Remember
3	Give the five goals of Information Security Governernance.	BTL 2	Understand
4	Pointout the five criteriasfor a policy to be effective and thus legally enforceable.	BTL 4	Analyze

5	What are the two areas in which Enterprise Security Policy typically addresses compliance?		BTL 1	Remember
6	Define Issue Specific Security Policy.		BTL 1	Remember
7	State the types of Policies.		BTL 1	Remember
8	Assess the drawbacks of ISO 17799/BS 7799.		BTL 5	Evaluate
9	Formulate the significant points in the scope of NIST SP 800-14.		BTL 6	Create
10	Analyze the name of NIST documents that can assist in the design of a security framework.		BTL 4	Analyze
11	Generalize the security plans using NIST SP 800-18 that can be used as the foundation for a comprehensive security blueprint and framework.		BTL 6	Create
12	State two important documents in a VISA International Security Model.		BTL 1	Remember
13	Assess the Defence in Depth Policy.		BTL 2	Understand
14	Quote the important types of controls in VISA International Security Model.		BTL 1	Remember
15	Point out the components of Contingency Planning.		BTL 4	Analyze
16	Examine using the diagram for spheres of security.		BTL 3	Apply
17	Show the different stages in the Business Impact Analysis step.		BTL 3	Apply
18	Assess the commonly accepted Security Principles.		BTL 5	Evaluate
19	Differentiate		BTL 2	Understand
20	Examine the five testing strategies of Incident Planning.		BTL 3	Apply
PART-B				
1	i) List the 3 types of security policies. (8) ii) Identify the components of ISSP. (5)		BTL 1	Remember
2	Elaborate briefly about Information Security Blueprint. (13)		BTL 1	Remember
3	i) Give the details of the types of policies in Information Security. (4) ii) Identify the inherent problems with ISO 17799. (9)		BTL 2	Understand
4	Express in detail about ISO 17799/BS 7799. (13)		BTL 2	Understand
5	Explain in detail about NIST security Models. (13)		BTL 4	Analyze

6	i) Define information security governance. Who in the organization should plan for it? (5) ii) Examine how can a security framework assist in the design and implementation of a security infrastructure? (8)	BTL 1	Remember
7	i) Demonstrate with a diagram about the guidelines, purposes used to achieve using ISO/IEC 17799. (8) ii) Illustrate where can a security administrator find information on established security frameworks? (5)	BTL 3	Apply
8	i) Evaluate VISA International Security Model. (5) ii) Summarize planning for Continuity. (8)	BTL 5	Evaluate
9	Design Security Architecture and explain the goals used for achieving it. (13)	BTL 6	Create
10	Analyze what Web resources can aid an organization in developing best practices as part of a security framework? (13)	BTL 4	Analyze
11	Point out management, operational, and technical controls, and explain when each would be applied as part of a security framework. (13)	BTL 4	Analyze
12	Describe contingency planning? How is it different from routine management planning? What are the components of contingency planning (13)	BTL 1	Remember
13	Discuss briefly about policy, a standard, and a practices with any example. (13)	BTL 2	Understand
14	Illustrate briefly about Incident Response Methodology. (13)	BTL 3	Apply
PART C			
1	How shall you create framework and blueprint for Information Security ? (15) Design diagrams and with suitable examples.	BTL 6	Create
2	Explain Information Security Continuity for ISO 27001. Also tell about its security considerations. (15)	BTL 6	Evaluate
3	Evaluate the Ten Sections mentioned ISO/IEC 17799 . (15)	BTL 5	Evaluate
4	Summarize SETA (Security, Education, Training, Awareness) and its elements. (15)	BTL 5	Evaluate
UNIT V-PHYSICAL DESIGN			
Security Technology, IDS, Scanning and Analysis Tools, Cryptography, Access Control Devices, Physical Security, Security and Personnel.			
PART-A			
Q.No	Questions	BT Level	Competence
1	Give the mechanisms that access control relies on.	BTL 2	Understand
2	Show the advantages of the intrusion detection systems.	BTL 3	Apply

3	List the three ways in which Authorization can be handled.	BTL 1	Remember
4	Analyze the primary disadvantage of application-level firewalls.	BTL 4	Analyze
5	Quote the different types of Firewalls that are characterized by its structure..	BTL1	Remember
6	Define Hybrid Firewall.	BTL1	Remember
7	Express five generations of Firewalls. Which generations are still common in use?	BTL 2	Understand
8	State Honey Pots.	BTL 1	Remember
9	Differentiate signature-based IDPS and behavior-based IDPS.	BTL 2	Understand
10	Show the use of scanning and Analysis Tools.	BTL 3	Apply
11	Compare Cryptography and Steganography.	BTL 5	Evaluate
12	Define Cryptography.	BTL 1	Remember
13	Create the factors for selecting the right firewalls.	BTL 6	Create
14	Assess the controls of protecting the secure facility.	BTL 5	Evaluate
15	Quote the signature based IDS.	BTL 1	Remember
16	Express the information security function that can be placed within any one of the following functions.	BTL 2	Understand
17	Formulate the best practices such that the information security function can be placed within any of the following organizational functions.	BTL 6	Create
18	Categorize IDPS Detection Methods.	BTL 4	Analyze
19	Differentiate Honey pots and Honey Nets	BTL 4	Analyze
20	Classify IDPS.	BTL 3	Apply

PART-B

1	i) Define Scanning and Analysis tools. (8)	BTL 1	Remember
	ii) List and explain the cryptographic algorithms. (5)		
2	i) Give the names of firewalls categorized by processing mode. (4)	BTL 2	Understand
	ii) Summarize IDPS Terminology. (9)		
3	Express IDPS Response Options.. (13)	BTL 2	Understand
4	Examine Strengths and Limitations of IDPs. (13)	BTL 3	Apply
5	List the Biometric Access Controls. (13)	BTL 1	Remember
6	i) Pointout the tools used in cryptography. (7)	BTL 4	Analyze
	ii) Explain Man-in-the middle attack. (6)		
7	i) Evaluate Honey pots, Honeynets, Padded cells. (6)	BTL 5	Evaluate
	ii) Assess the dictionary attack, Timing attacks and Defending against attacks. (7)		

8	i) Classify architectural implementation of firewalls. (9) ii) Analyze typical relationship among the untrusted network, the firewall, and the trusted network?. (4)	BTL 4	Analyze
9	Formulate configuring and managing firewalls. (13)	BTL 6	Create
10	Elaborate vulnerability scanners. (13)	BTL 1	Remember
11	Explain about Symmetric and Asymmetric Encryption with examples. (13)	BTL 4	Analyze
12	i) Describe cipher methods. (8) ii) Discuss about protocols for secure communications. (5)	BTL 1	Remember
13	Illustrate briefly about the credentials of Information Security Professionals. (13)	BTL 3	Apply
14	Discuss about Employment Policies and Practices. (13)	BTL 2	Understand
PART C			
1	Explain how does screened host architectures for firewalls differ from screened subnet firewall architectures? Which of these offers more security for the information assets that remain on the entrusted network? (15)	BTL 6	Create
2	Evaluate how does a network-based IDPS differ from a host-based IDPS? (15)	BTL 5	Evaluate
3	Formulate in detail about the importance of Physical Security. (15)	BTL 6	Create
4	Create the options available for the location of the information security functions within the organization. Discuss the advantages and disadvantages of each option. (15)	BTL 6	Create