SRM VALLIAMMAI ENGINEERING COLLEGE
(An Autonomous Institution)

SRM Nagar, Kattankulathur–603203

DEPARTMENT OF CYBER SECURITY

QUESTION BANK

VII SEMESTER
1923708- SECURITY ASSESSMENT & RISK ANALYSIS
Regulation–2019
Academic Year 2025–2026(Odd Semester)

Prepared by
Mr.S. E.Rajkumar, A.P/CYS

1923708 - SECURITY ASSESSMENT & RISK ANALYSIS
SEM/ YEAR :VII SEMESTER / FOURTH YEAR

UNIT–I SECURITY BASICS

Advanced Linux Exploitation: Information Security (INFOSEC) Overview: critical information characteristics – availability information states processing security Countermeasures– education, training and awareness, critical information characteristics – confidentiality critical information characteristics – integrity, information states – storage, information states – transmission, security countermeasures–policy, procedures and practices, threats, Vulnerabilities.

UNIT–I [PART-A]

Q.No	Question	Competence	Level
1.	What is security?	Remembering	BTL1
2.	Where security has been used?	Remembering	BTL1
3.	What is information Security?	Remembering	BTL1
4.	What are the 3 Principles of Information Security?	Remembering	BTL1
5.	Discuss about integrity	Understanding	BTL2
6.	How will you protect the confidentiality of information	Analysing	BTL4
7.	List out Types of InfoSec	Understanding	BTL2
8.	Summarize about ISMS?	Understanding	BTL2
9.	Differentiate between active attacks and passive attacks	Understanding	BTL2
10.	Explain SETA	Evaluating	BTL5
11.	How will you implement Security Education, Training & Awarenes program?	Analysing	BTL4
12.	How SETA helps basic network security issues?	Analysing	BTL4
13.	What is mean by Information Assurance	Remembering	BTL1
14.	Explain Security Countermeasures	Applying	BTL3
15.	Discuss about Information States	Understanding	BTL2
16.	Discuss about Transmission state	Understanding	BTL2
17.	Name the information states	Understanding	BTL2
18.	Does Processing state defines time? Give Example	Analysing	BTL4
19.	Discover Critical Characteristics of Information	Applying	BTL3
20.	What is an Information Security Policy?	Remembering	BTL1
21.	How an Information Security Policy is Important?	Applying	BTL3
22.	What is Data Classification in Security Policy	Remembering	BTL1
23.	What is mean by threads?	Applying	BTL3
24.	What is mean by vulnerabilities?	Understanding	BTL2

UNIT–I[PART-B]

Q.No		Question	Marks	Competence	Level
1.	-	Describe about Information Security & Types.	13	Remembering	BTL1
2.	A	Summarize about Information Security Countermeasures.	13	Evaluating	BTL5
3.	-	Discuss in detail about Critical Characteristics of Information	13	Understanding	BTL2
4.		Analyze about Information Security Countermeasures	13	Analysing	BTL4
5.	-	Discuss about Security Education Training and Awareness (SETA)	13	Understanding	BTL2
6.	A	Analyse the Components of an Information System.	07	Analysing Remembering	BTL4
	B	Explain about types of attack	06		
7.	-	Analyze why security awareness training is important	13	Analysing	BTL4

8.		Describe about Information state in Assurance model	13	Remembering	BTL1
9.		Explain about security services in detail –		Remembering	BTL1
10.	-	Discuss in detail about security counter measures	06		
11	-	Summarize about Key Elements of an Information Security Policy	13	Understanding	BTL2
12	-	Illustrate about importance of Information Security Policy.	13	Applying	BTL3
13	-	Classify the pros and cons of Information Security Policy	13	Applying	BTL3
14	-	Discuss the difference between threats and Vulnerabilities.	13	Analysing	BTL4
15	-	Summarize about Vulnerabilities.	13	Understanding	BTL2
16	-	Analyse common network vulnerabilities	13	Analysing	BTL4
17	-	Explain about types of threads	13	Evaluating	BTL5
UNIT-I[PART-C]					
1		Discuss in detail Information Security and Principles of information security	15	Understanding	BTL2
2		Evaluate Information Assurance Model	15	Evaluating	BTL5
3		Analyze NSTISSC Security Model	15	Analysing	BTL4
4		Generalize in detail about Information Security Policy and Best Practices for Information Security Management?	15	Creating	BTL6
5		Analyze about threads and Types of Threats in security	15	Analysing	BTL4

UNIT–II THREATS TO AND VULNERABILITIES OF SYSTEMS
Definition of terms (e.g., threats, vulnerabilities, risk), major categories of threats (e.g., fraud, Hostile Intelligence Service (HOIS), malicious logic, hackers, environmental and technological hazards, disgruntled employees, careless employees, HUMINT, and monitoring), threat impact areas, Counter measures: assessments (e.g., surveys, inspections). Concepts of Risk Management: consequences (e.g., corrective action, risk assessment)..

UNIT–II [PART-A]

Q.No	Question	Competence	Level
1.	What is mean by threads?	Remembering	BTL1
2.	List out Types of Threads	Understanding	BTL2
3.	Discuss about Vulnerability?	Understanding	BTL2
4.	What are the types of Vulnerability ?	Remembering	BTL1
5.	Discuss about Risk	Understanding	BTL2
6.	How risks can be defined?	Understanding	BTL2
7.	What is mean by Fraud	Understanding	BTL2
8.	Discuss about HIS?	Understanding	BTL2
9.	What are the objectives of HIS	Understanding	BTL2
10.	Explain Malicious Logic	Evaluating	BTL5
11.	List the types of malicious logic?	Analysing	BTL4
12.	What is Hacking?	Remembering	BTL1
13.	List the Types of Intruders	Remembering	BTL1
14.	Discuss what will Black Hat Hackers do?	Understanding	BTL2
15.	Discuss about DoS	Understanding	BTL2
16.	Discuss about DDoS Attack	Understanding	BTL2
17.	How will you Prevent from Getting Hacked?	Applying	BTL3

18.	List the thread impact areas	Remembering	BTL1
19.	What is mean by counter measures?	Remembering	BTL1
20.	In which areas common counter measures employed ?	Analysing	BTL4
21.	How survey assessment implemented in counter measures?	Applying	BTL3
22.	What is risk management	Remembering	BTL1
23.	Discuss the importance of risk management?	Analysing	BTL4
24.	List the risk management steps?	Understanding	BTL2

UNIT–II[PART-B]

Q.No		Question	Marks	Competence	Level
1.	-	Difference Between Threat, Vulnerability, and Risk.	13	Remembering	BTL1
2.		Analyze about types of threads	13	Evaluating	BTL5
3.	-	Discuss in detail about Risks	13	Understanding	BTL2
4.		Summarize about Types of fraud	13	Analysing	BTL4
5.	-	Discuss about Viruses and types of viruses	13	Understanding	BTL2
6.	A	Summarize the Causes of Vulnerabilities	07	Analysing	BTL4
	B	How to Find and Fix the Vulnerabilities?	06	Evaluating	BTL5
7.	-	Analyze about common network vulnerabilities	13	Analysing	BTL4
8.		Describe about Trojan and Common types of Trojan malware	13	Remembering	BTL1
9.	A	Explain about DoS –	07	Remembering	BTL1
	B	Discuss in detail about DDoS Attack	06	Remembering	BTL1
10.	-	Summarize about Intrusion & Intruders	13	Understanding	BTL2
11.		Analyze how will you Protect Yourself Against Hacking	13	Understanding	BTL2
12.	-	Discuss about hackers & types	13	Analysing	BTL4
13	-	Discuss about various Environmental Hazards and how will you overcome from hazards	13	Analysing	BTL4
14	-	Discuss about Disgruntled employees and Careless Employees.	13	Analysing	BTL4
15	-	Summarize about HUMINT Importance of Human Intelligence	13	Understanding	BTL2
16	-	Analyze the thread impact areas	13	Analysing	BTL4
17	-	Explain about Counter measures in security	13	Remembering	BTL1

UNIT-II[PART-C]

1	Discuss in detail about threads and Types of threads	15	Understanding	BTL2
2	Explain in detail about Hostile Intelligence Service (HIS) & summarize with Case study	15	Evaluating	BTL5
3	Analyze various Malicious Logic & Explain in Detail	15	Analysing	BTL4
4	Analyze about Environmental Hazards and technical hazard in security?	15	Creating	BTL6
5	Analyze risk management and discuss the importance of risk management	15	Analysing	BTL4

UNIT–III SECURITY PLANNING

Directives and procedures for policy mechanism, Risk Management: acceptance of risk (accreditation), corrective actions information identification, risk analysis and/or vulnerability assessment components, risk analysis results evaluation, roles and responsibilities of all the players in the risk analysis process, Contingency plan components, determination of backup requirements, development of plans for recovery actions after a disruptive event, development of procedures for offsite processing, emergency destruction procedures.

UNIT–III [PART-A]

Q.No	Question	Competence	Level
1.	What is mean by Policy mechanisms?	Remembering	BTL1
2.	Discuss about Risk management	Understanding	BTL2
3.	Will Traditional risk management harm organizations?Give Reasons	Analyzing	BTL4
4.	What is mean by enterprise risk management ?	Remembering	BTL1
5.	What is a corrective action?	Understanding	BTL2
6.	How Risk Prioritization is essential?	Analyzing	BTL4
7.	Discuss Root Cause Analysis	Understanding	BTL2
8.	Expand SMART Criteria?	Remembering	BTL1
9.	Why Is Risk Analysis Important?	Analyzing	BTL4
10.	What Is Risk Analysis?	Remembering	BTL1
11.	Discuss about vulnerability assessment?	Analyzing	BTL4
12.	What is Risk Evaluation?	Remembering	BTL1
13.	What is Employers' roles and responsibilities in Risk Management	Remembering	BTL1
14.	Discuss what will Contingency plans do?	Understanding	BTL2
15.	What is Data Custodians	Understanding	BTL2
16.	Discuss about disaster recovery plan	Understanding	BTL2
17.	How does disaster recovery plan works ?	Applying	BTL3
18.	List the key steps of a disaster recovery (DR) plan?	Remembering	BTL1
19.	What is mean by DR Plan?	Remembering	BTL1
20.	What is Disaster Management Plan?	Analyzing	BTL4
21.	What are the Physical hazards?	Applying	BTL3
22.	What is risk assessment and disaster management plan	Remembering	BTL1
23.	Discuss the importance of Security planning?	Analyzing	BTL4
24.	What are the emergency risk management procedures?	Understanding	BTL2

UNIT–III[PART-B]

Q.No		Question	Marks	Competence	Level
1.	-	Discuss in detail policy mechanism.	13	Remembering	BTL1
2.		Analyze the difference between Traditional risk management and enterprise risk management	13	Evaluating	BTL5
3.	-	Discuss in detail about risk response strategies	13	Understanding	BTL2
4.		Analyze the Pros and cons of Risk Analysis	13	Analyzing	BTL4
5.	-	Discuss about vulnerability assessment components	13	Understanding	BTL2
6.	A	Summarize about Risk evaluation	07	Analyzing	BTL4
	B	How and who should do risk assessments?	06	Evaluating	BTL5
7.	-	Analyze about contingency plan components	13	Analyzing	BTL4
8.		Elaborate How are organizations using disaster recovery plans?	13	Analyzing	BTL4
9.	A	Analyze the Workers' roles and responsibilities in Risk	07	Analyzing	BTL4

		management			
	B	Explain the role of The role of the Risk Manager	06	Understanding	BTL2
10.	-	Summarize about determination of backup requirements	13	Understanding	BTL2
11.	-	Discuss about DR plan importance	13	Understanding	BTL2
12.		Explain in detail about Types of Risk Analysis		Understanding	BTL2
13	-	Discuss about step-by-step guide to developing procedures for offsite processing in risk management	13	Analyzing	BTL4
14	-	Discuss the scope and objective of Disaster Management Plan.	13	Analyzing	BTL4
15	-	Summarize about disaster management and emergency preparedness plan	13	Understanding	BTL2
16	-	Explain about Physical hazards and how to prevent from physical hazards	13	Understanding	BTL2
17	-	Explain about security planning in detail	13	Remembering	BTL1
UNIT-III[PART-C]					
1		Discuss in detail about essential directives and procedures for policy mechanisms in security planning	15	Understanding	BTL2
2		Why is risk management important? Explain in Detail about risk management process.	15	Analyzing	BTL5
3		Explain the steps involved in identifying corrective actions	15	Analyzing	BTL4
4		Explain about Risk analysis and Types of Risk Analysis	15	Creating	BTL6
5		Analyze key steps of a disaster recovery (DR) plan?	15	Analyzing	BTL4

UNIT–IV: POLICIES AND PROCEDURES		
Physical Security Measures: alarms, building construction, cabling, communications centre, environmental controls (humidity and air conditioning), filtered power, physical access control systems (key cards, locks and alarms) Personnel Security Practices and Procedures: access authorization/verification (need–to–know), contractors, employee clearances, position sensitivity, security training and awareness, systems maintenance personnel, Administrative Security Procedural Controls: attribution, copyright protection and licensing		
UNIT–IV [PART-A]		
Q.No	Question	Competence	Level
1.	What is mean by Policy and procedures?	Remembering	BTL1
2.	What is a security policy?	Remembering	BTL1
3.	How security policy is important?Give Reasons	Analyzing	BTL4
4.	What are the three types of security policies ?	Remembering	BTL1
5.	What is physical security?	Understanding	BTL2
6.	List some multiple elements and measures of physical security?	Understanding	BTL2
7.	What are the levels of Levels of physical security	Remembering	BTL1
8.	What is Cabling?	Remembering	BTL1
9.	What is mean by Data center?	Remembering	BTL1
10.	Discuss about Physical security controls?	Remembering	BTL1
11.	Draw the Data center tiers?	Remembering	BTL1
12.	What are Physical and Environmental Controls?	Remembering	BTL1
13.	What is Personnel Security ?	Remembering	BTL1
14.	Discuss Procedures in physical security?	Understanding	BTL2

15.	What is mean by access authorization	Understanding	BTL2
16.	What is Multi-factor authentication (MFA)	Understanding	BTL2
17.	Discuss about Public Key Infrastructure (PKI)?	Remembering	BTL1
18.	What is mean by Authorization?	Remembering	BTL1
19.	Discuss about Biometric Authentication?	Understanding	BTL2
20.	What is mean by contractors?	Remembering	BTL1
21.	Differentiate Security Guard Services and Cyber security Contractors?	Understanding	BTL2
22.	What is mean by Phishing Awareness?	Remembering	BTL1
23.	Discuss the importance Continuous Training and Reinforcement?	Analyzing	BTL4
24.	What are the Procedural Controls?	Understanding	BTL2

UNIT–IV[PART-B]

Q.No		Question	Marks	Competence	Level
1.	-	Discuss in detail about types of security policies	13	Remembering	BTL1
2.		Analyze the Physical security measures and methods	13	Analyzing	BTL4
3.	-	Discuss in detail about the common physical security measures that rely on cabling	13	Understanding	BTL2
4.		Analyze how organization monitor the safety and security of the data center?	13	Analyzing	BTL4
5.	-	Explain about Data center infrastructure	13	Understanding	BTL2
6.	A	Explain the Levels of physical security	07	Analyzing	BTL4
	B	What are the methods to identify physical security threats?	06	Evaluating	BTL5
7.	-	Discuss about the Data center tiers	13	Understanding	BTL2
8.		Analyze about Physical and Environmental Controls	13	Analyzing	BTL4
9.		Analyze about position sensitivity	13	Analyzing	BTL4
10.	-	Summarize about personnel security practices and procedures	13	Understanding	BTL2
11.		Explain about employee clearances	13		
12.	-	Discuss about access authorization in security	13	Understanding	BTL2
13	-	Discuss about step-by-step guide to develop systems maintenance personnel	13	Analyzing	BTL4
14	-	Discuss in detail about Administrative Security.	13	Analyzing	BTL4
15	-	Summarize about the Procedural Controls	13	Understanding	BTL2
16	-	Explain about attribution in Procedural Controls	13	Understanding	BTL2
17	-	Explain about copyright protection and licensingin detail	13	Remembering	BTL1

UNIT-IV[PART-C]

1	Discuss in detail about security policy and Seven elements of an effective security policy	15	Understanding	BTL2
2	Explain in detail about Physical security control technology and Physical security planning	15	Analyzing	BTL5
3	Analyze and Explain the Layers in data center Security	15	Analyzing	BTL4
4	Explain about several types of security contractors	15	Creating	BTL6
5	Analyze various aspects to consider when implementing security training and awareness programs?	15	Analyzing	BTL4

UNIT–V: OPERATIONS SECURITY

OPSEC surveys/OPSEC planning INFOSEC: computer security – audit, cryptography–encryption (e.g., point–to–point, network, link), cryptography–key management (to include electronic key), Cryptography–strength (e.g., complexity, secrecy, characteristics of the key). Case study of threat and vulnerability assessment.

UNIT–V [PART-A]

Q.No	Question	Competence	Level
1.	What is Operational Security?	Remembering	BTL1
2.	What are the steps in OPSEC?	Remembering	BTL1
3.	How OPSEC is important?Give Reasons?	Analyzing	BTL4
4.	Discuss about OPSEC Survey	Remembering	BTL1
5.	Discuss the Characteristics of OPSEC?	Understanding	BTL2
6.	List some Types of Surveys?	Understanding	BTL2
7.	What is critical information (CI)?	Remembering	BTL1
8.	Discuss the role of OPSEC Program Manager?	Understanding	BTL2
9.	What Is Information Security?	Remembering	BTL1
10.	What is an information security management system (ISMS)?	Remembering	BTL1
11.	What is the General Data Protection Regulation (GDPR)?	Remembering	BTL1
12.	What is Computer Security?	Remembering	BTL1
13.	List the Types of Computer Security?	Remembering	BTL1
14.	How computer security is important to Society?	Analyzing	BTL4
15.	What is mean by Computer Society threads	Understanding	BTL2
16.	What is a Cyber security Audit	Understanding	BTL2
17.	Discuss How it is Helpful for Your Business?	Remembering	BTL1
18.	What are the Significant benefits of IT security audits?	Remembering	BTL1
19.	Discuss the Scope of a Cybersecurity Audit?	Understanding	BTL2
20.	What is mean by cryptography?	Remembering	BTL1
21.	List the types of Cryptography in detail?	Understanding	BTL2
22.	What is encryption?	Remembering	BTL1
23.	What is an encryption algorithm?	Remembering	BTL1
24.	What are the key management?	Understanding	BTL2

UNIT–V[PART-B]

Q.No		Question	Marks	Competence	Level
1.	-	Discuss in detail about procedures for OPSEC surveys	13	Remembering	BTL1
2.		Explain in detail about role OPSEC Program Manager and OPSEC Coordinators	13	Analyzing	BTL4
3.	-	Discuss in detail about the Types of Information security	13	Understanding	BTL2
4.		Explain about computer Society and types of computer society?	13	Analyzing	BTL4
5.	-	Explain in detail about security audit	13	Understanding	BTL2
6.	A	Differentiate between symmetric and asymmetric cryptography?	07	Analyzing	BTL4 BTL5
	B	Discuss about What type of problems does cryptography solve?	06	Evaluating	
7.	-	Explain about Cryptography in detail	13	Understanding	BTL2
8.		Explain about types of Cryptography in detail	13	Analyzing	BTL4
9.	A	How does encryption work?	07	Analyzing	BTL4

	B	Explain about the importance of encryption?	06	Understanding	BTL2
10.	-	Summarize about Distribution of Public Key	13	Understanding	BTL2
11.	-	Discuss about access authorization in security	13	Understanding	BTL2
12.	-	Discuss about point–to–point encryption in detail	13	Analyzing	BTL4
13.	-	Discuss in detail Cryptographic Key Management.	13	Analyzing	BTL4
14.	-	Explain in detail about complexity in cryptography	13	Understanding	BTL2
15.	-	Discuss about characteristics of the key	13	Understanding	BTL2
16.	-	Explain about OPSEC program structure	13	Remembering	BTL1
17.		Explain in detail about encrypting a network	13	Understanding	BTL2
UNIT-V[PART-C]					
1		Discuss in detail about Operational security, importance and steps in operational security	15	Understanding	BTL2
2		Discuss in detail about OPSEC Program structure and Draw program structure for your organization	15	Analyzing	BTL5
3		Explain about Information security and Types of Information security	15	Understanding	BTL2
4		Explain about Encryption and types of encryption	15	Understanding	BTL2
5		Analyze Key Management in Cryptography and discuss about The public key distribution?	15	Analyzing	BTL4