SRM VALLIAMMAI ENGINEERING COLLEGE

(An Autonomous Institution)
SRM Nagar, Kattankulathur – 603 203

DEPARTMENT OF COMPUTER APPLICATIONS

QUESTION BANK

II SEMESTER M.C.A.

MC4264- CYBER SECURITY

Regulation – 2024

Academic Year 2024 – 2025(Even Semester)

Prepared by

Mr. M. Asan Nainar (AP Sel.G/M.C.A.)
Mr. N. Leo Bright Tennisson (AP Sr. G. / M.C.A.)

SRM VALLIAMMAI ENGINEERING COLLEGE

(An Autonomous Institution)
SRM Nagar, Kattankulathur-603 203
DEPARTMENT OF COMPUTER APPLICATIONS

QUESTION BANK

SUBJECT : MC4264 CYBER SECURITY
SEM/YEAR: II / I

UNIT - I: PLANNING FOR CYBER SECURITY
Best Practices-Standards and a plan of Action-Security Governance Principles, components and Approach-Information Risk Management-Asset Identification-Threat Identification-Vulnerability Identification-Risk Assessment Approaches-Likelihood and Impact Assessment-Risk Determination, Evaluation and Treatment-Security Management Function-Security Policy-Acceptable Use Policy- Security Management Best Practices - Security Models: Bell La Padula model, Biba Integrity Model - Chinese Wall model

UNIT - I: PART – A

Q. No	Question	BT Level	Competence	Course Outcome
1	**Define** cyberspace.	BTL-1	Remember	CO1
2	**List** the objectives of cyber security.	BTL-1	Remember	CO1
3	**Describe** cyber security.	BTL-1	Remember	CO1
4	**Identify** two related terms to cyber security.	BTL-1	Remember	CO1
5	**Examine** the general guidelines for evaluating risk.	BTL-1	Remember	CO1
6	**Tabulate** important Best Practices and Standards Documents.	BTL-1	Remember	CO1
7	**Name** the three principal activities of Standard of Good Practice for information security.	BTL-1	Remember	CO1
8	**What** is meant by integrity?	BTL-1	Remember	CO1
9	**What** is meant by Authenticity?	BTL-1	Remember	CO1
10	**What** is meant by non-repudiation?	BTL-1	Remember	CO1
11	**Describe** Risk Treatment.	BTL-1	Remember	CO1
12	**What** is meant by Risk Reduction?	BTL-1	Remember	CO1
13	**Describe** Risk Transfer.	BTL-1	Remember	CO1
14	**Summarize** Bell LaPadula model.	BTL-2	Understand	CO1
15	**Describe** Biba model.	BTL-2	Understand	CO1
16	**Contrast** User needs versus security implementation.	BTL-2	Understand	CO1
17	**Predict** areas of threat sources.	BTL-2	Understand	CO1
18	**Distinguish** Quantitative versus Qualitative risk assessment.	BTL-2	Understand	CO1

19	Is it easy or difficult to **estimate** the total cost of cybersecurity breaches? Express the fact.	BTL-2	Understand	CO1
20	**Differentiate** the terms threat and vulnerability	BTL-2	Understand	CO1
21	**Discuss** about Risk Retention.	BTL-2	Understand	CO1
22	**Give** an example for Asset Register.	BTL-2	Understand	CO1
23	**Express** the situation where you will choose Risk Avoidance technique.	BTL-2	Understand	CO1
24	**Give** an example of a worksheet to record and prioritize Information Types.	BTL-2	Understand	CO1
25	**What** is asset register?	BTL-1	Remember	CO1

UNIT - I: PART – B

CO1

Q. No	Question	Mark	BT Level	Competence	Course Outcome
1	**Apply** information security architecture reference model to an Enterprise Architecture reference model and explain the integration with block diagram.	16	BTL-3	Apply	CO1
2	**Demonstrate** various risk management process	16	BTL-3	Apply	CO1
3	**Examine** various basic security governance functions.	16	BTL-3	Apply	CO1
4	i. **Illustrate** Asset Identification. **i. Show** the content of Asset Register.	8 8	BTL-3	Apply	CO1
5	**i. Solve** risk analysis problem with simple risk analysis worksheet. **ii. Examine** factor analysis of information risk.	8 8	BTL-3	Apply	CO1
6	**Relate** Quantitative and Qualitative Risk Assessment.	16	BTL-3	Apply	CO1
7	**i. Classify** Threat Types. **ii. Experiment** vulnerability identification.	8 8	BTL-3	Apply	CO1
8	**Discover** risk assessment challenges.	16	BTL-3	Apply	CO1
9	i. **Analyze** likelihood assessment. ii. Estimate threat event frequency.	8 8	BTL-4	Analyze	CO1
10	**Explain** Impact Assessment.	16	BTL-4	Analyze	CO1
11	**Classify** various risk treatment options	16	BTL-4	Analyze	CO1
12	**i. Compare** various information security costs. **ii. Pointout** various documents related to security policy.	8 8	BTL-4	Analyze	CO1
13	**Differentiate** security governance and security management.	16	BTL-4	Apply	CO1
14	**Explain** security planning process with example.	16	BTL-5	Evaluate	CO1

15	**Summarize** various security models.	16	BTL-5	Evaluate	CO1
16	**Create** a table for Likelihood Assessment Scales.	16	BTL-6	Create	CO1
17	**Formulate** interactions between the security reference model and other reference models.	16	BTL-6	Create	CO1
18	**Summarize** the following. i) Bell La Padula ii) Biba integrity model iii) Chinese wall model	6 6 4	BTL-5	Evaluate	CO1

UNIT II SECURITY CONTROLS

People Management-Human Resource Security-Security Awareness and Education Information Management-Information Classification and handling-Privacy-Documents and Record Management- Physical Asset Management-Office Equipment-Industrial Control Systems-Mobile Device Security- System Development-Incorporating Security into SDLC - Disaster management and Incident response planning.

UNIT II PART – A

Q. No	Questions	BT Level	Competence	Course Outcome
1	**Define** the employment life cycle.	BTL-1	Remember	CO2
2	**List** all security aspects involving employees.	BTL-1	Remember	CO2
3	**Describe** security awareness.	BTL-1	Remember	CO2
4	**Identify** various information types.	BTL-1	Remember	CO2
5	**Examine** change management.	BTL-1	Remember	CO2
6	**Tabulate** average life cycle duration of common hardware.	BTL-1	Remember	CO2
7	**Name** the steps in document management life cycle.	BTL-1	Remember	CO2
8	**What** is meant by negligent behavior?	BTL-1	Remember	CO2
9	**What** is meant by accidental behavior?	BTL-1	Remember	CO2
10	**What** is meant by malicious behavior?	BTL-1	Remember	CO2
11	**Describe** hardware life cycle management.	BTL-1	Remember	CO2
12	**What** is multifactor authentication?	BTL-1	Remember	CO2
13	**Describe** hardware asset life cycle.	BTL-1	Remember	CO2
14	**Summarize** mobile device security strategy.	BTL-2	Understand	CO2
15	**Describe** golden record.	BTL-2	Understand	CO2
16	**Contrast** document management and records management.	BTL-2	Understand	CO2
17	**Predict** various vulnerabilities in mobile device security.	BTL-2	Understand	CO2
18	**Distinguish** rooting and sideloading.	BTL-2	Understand	CO2
19	**Estimate** various levels of risk in information security**.**	BTL-2	Understand	CO2
20	**Differentiate** critical information and sensitive information.	BTL-2	Understand	CO2

21	**Discuss** about application life cycle management.	BTL-2	Understand	CO2
22	**Give** the block diagram of document management life cycle.	BTL-2	Understand	CO2
23	**Express** about side-channel attacks.	BTL-2	Understand	CO2
24	**Give** the block diagram of records management functions.	BTL-2	Understand	CO2
25	**Give** the classification of information.	BTL-2	Understand	CO2

UNIT II PART – B					
Q. No	**Question**	**Mark**	**BT Level**	**Competence**	**Course Outcome**
1	**Apply** various privacy controls to protect an organization to counter privacy threats and comply with government laws and regulations.	16	BTL-3	Apply	CO2
2	**Demonstrate** Security Categorization Process defined by NIST	16	BTL-3	Apply	CO2
3	**Examine** hardware life cycle management.	16	BTL-3	Apply	CO2
4	i. **Illustrate** the roles of Documents. ii. **Show** the differences between document management and record management.	8 8	BTL-3	Apply	CO2
5	i. **Illustrate** security governance approach. ii.**Examine** security governance evaluation.	8 8	BTL-3	Apply	CO2
6	**Relate** Information security and privacy.	16	BTL-3	Apply	CO2
7	**i. Classify** common mobile device threats. **ii. Experiment** with developing, testing and documenting security controls and features.	8 8	BTL-3	Apply	CO2
8	**Discover** DevOps Reference Arcitecture.	16	BTL-3	Apply	CO2
9	i.**Analyze** risk assessment concepts. ii. **Estimate** the level of risk in information secruity.	8 8	BTL-4	Analyze	CO2
10	**Explain** mobile Ecosystem.	16	BTL-4	Analyze	CO2
11	**Differentiate** IT Systems and Industrial Control Systems.	16	BTL-4	Analyze	CO2
12	i. **Compare** critical information and sensitive information. ii. **Point out** roles of documents with example.	6 10	BTL-4	Analyze	CO2
13	**Differentiate** document and records management.	16	BTL-4	Apply	CO2
14	**Explain** various security functions for IT systems and Industrial Control Systems.	16	BTL-5	Evaluate	CO2
15	**Summarize** typical security threats to Industrial Control	16	BTL-5	Evaluate	CO2

	Systems and key security measures for protecting Industrial Control Systems.				
16	**Create** a table that relates mobile ecosystem element and threats.	16	BTL-6	Create	CO2
17	**Formulate** App Vetting Process with a block diagram.	16	BTL-6	Create	CO2
18	**Formulate** Disaster management and incident response planning.	16	BTL-6	Create	CO2

UNIT – III CYBER SECURITY FOR BUSINESS APPLICATIONS AND NETWORKS				
Business Application Management-Corporate Business Application Security-End user Developed Applications-System Access- Authentication Mechanisms-Access Control System Management- Virtual Servers-Network Storage Systems-Network Management Concepts-Firewall-IP Security- Electronic Communications - Case study on OWASP vulnerabilities using OWASP ZAP tool.				
Q. No	**Questions**	**BT Level**	**Competence**	**Course Outcome**
UNIT III PART – A				
1	**Define** application management.	BTL-1	Remember	CO3
2	**List** key application management stakeholders.	BTL-1	Remember	CO3
3	**Describe** application portfolio management.	BTL-1	Remember	CO3
4	**Identify** the aim of web application security.	BTL-1	Remember	CO3
5	**Examine** application performance management.	BTL-1	Remember	CO3
6	**Tabulate** information to be included in a Business Application Register.	BTL-1	Remember	CO3
7	**Name** hosting options for Web Application Firewall.	BTL-1	Remember	CO3
8	**What** is reengineering?	BTL-1	Remember	CO3
9	**Differentiate** characteristics of High-Value Application and Low-Value Application.	BTL-2	Understand	CO3
10	**Give** the diagram for Application Life Cycle Management.	BTL-2	Understand	CO3
11	**Describe** authentication.	BTL-1	Remember	CO3
12	**What** is Authorization?	BTL-1	Remember	CO3
13	**Describe** Access control.	BTL-1	Remember	CO3
14	**Summarize** authentication factors in a table.	BTL-2	Understand	CO3
15	**Describe** authentication factor.	BTL-2	Understand	CO3
16	**Contrast** Biometric Verification and Biometric Identification with a diagram.	BTL-2	Understand	CO3
17	**Predict** Biometric System attack with a diagram**.**	BTL-2	Understand	CO3
18	**Distinguish** packet filtering firewall and stateful inspection firewall with a diagram.	BTL-2	Understand	CO3
19	**Estimate** cost versus accuracy of various biometric characteristics in User Authentication Schemes with a chart.	BTL-2	Understand	CO3
20	**What** is VoIP?	BTL-1	Remember	CO3
21	**What** is SAN?	BTL-1	Remember	CO3

22	**Discuss** the threats involved in use of VoIP.	BTL-2	Understand	CO3
23	**Express** multifactor authentication.	BTL-2	Understand	CO3
24	**Give** the diagram for SAN and NAS configuration.	BTL-2	Understand	CO3
25	**What** is OWASP?	BTL-1	Remember	CO3

UNIT III PART – B					
Q. No	**Question**	**Mark**	**BT Level**	**Competence**	**Course Outcome**
1	**Apply** best practices for Application portfolio management.	16	BTL-3	Apply	CO3
2	**Demonstrate** application performance management steps.	16	BTL-3	Apply	CO3
3	**Examine** corporate business application security.	16	BTL-3	Apply	CO3
4	i. **Illustrate** Open Web Application Security Project OWASP Top 10 Application Security Risks. **ii. Show** a web application firewall with diagram.	8 8	BTL-3	Apply	CO3
5	**i. Illustrate** benefits of EUDAs. **ii. Examine** risks of EUDAs.	8 8	BTL-3	Apply	CO3
6	**Explain** EUDA Security Framework.	16	BTL-4	Analyze	CO3
7	**Differentiate** characteristics of High-Value Application and Low-Value Application and High-cost/High-Risk and Low-Cost/Low Risk Application.	16	BTL-4	Analyze	CO3
8	**Summarize** business application management best practices.	16	BTL-5	Evaluate	CO3
9	**Create** a model for Electronic User Authentication.	16	BTL-6	Create	CO3
10	**Relate** Electronic Functions and Data for eID cards in a table.	16	BTL-3	Apply	CO3
11	i) **Classify** criteria for Biometric Characteristics. ii) **Experiment** physical characteristics used in Biometric Applications.	8 8	BTL-3	Apply	CO3
12	**Discover** operation of a Biometric Authentication System.	16	BTL-3	Apply	CO3
13	i. **Analyze** firewall characteristics. ii. **Estimate** Backup and Recovery guidelines with a table.	8 8	BTL-4	Analyze	CO3
14	**i. Compare** Type1 and Type2 Hypervisors. **ii. Point out** Virtualization Security Issues.	6 10	BTL-4	Analyze	CO3
15	**Differentiate** Application proxy firewall and Circuit-level proxy firewall with a diagram and explain.	16	BTL-4	Apply	CO3
16	**Explain** Elements of System Management.	16	BTL-5	Evaluate	CO3
17	**Formulate** Authenticator Assurance Levels with table for Assurance Level determined by Estimated impact level.	16	BTL-6	Create	CO3
18	**Formulate** a case study on OWASP vulnerabilities using OWASP ZAP tool	16	BTL-6	Create	CO3

UNIT – IV TECHNICAL SECURITY				
Supply Chain Management-Cloud Security-Security Architecture-Malware Protection Intrusion Detection-Digital Rights Management-Cryptographic Techniques-Threat and Incident Management- Vulnerability Management-Security Event Management-Forensic Investigations-Local Environment Management-Business Continuity.				
Q. No	**Questions**	**BT Level**	**Competence**	**Course Outcome**
UNIT IV PART – A				
1	**Define** information and communications technology (ICT).	BTL-1	Remember	CO4
2	**List** types of flows associated with a supply chain.	BTL-1	Remember	CO4
3	**Describe** Supply Chain Management.	BTL-1	Remember	CO4
4	**Identify** Supply Chain risk areas.	BTL-1	Remember	CO4
5	**Examine** Tier 3 supply chain threat considerations.	BTL-1	Remember	CO4
6	**Tabulate** requirements for a Cryptographic Hash Function H.	BTL-1	Remember	CO4
7	**Name** supply chain security controls.	BTL-1	Remember	CO4
8	**What** is cloud computing?	BTL-1	Remember	CO4
9	**What** is malware?	BTL-1	Remember	CO4
10	**What** is brute-force attacks?	BTL-1	Remember	CO4
11	**Describe** product/service flow.	BTL-1	Remember	CO4
12	**What** is information flow in supply chain flows?	BTL-1	Remember	CO4
13	**Describe** money flow in supply chain flows.	BTL-1	Remember	CO4
14	**Summarize** cloud computing.	BTL-2	Understand	CO4
15	**Describe** rule-based data recognition.	BTL-2	Understand	CO4
16	**Contrast** security event and security incident.	BTL-2	Understand	CO4
17	**Predict** exact file matching.	BTL-2	Understand	CO4
18	**Distinguish** data at rest and data in motion.	BTL-2	Understand	CO4
19	**Estimate** cryptoperiod.	BTL-2	Understand	CO4
20	**Differentiate** passive monitoring and active monitoring.	BTL-2	Understand	CO4
21	**Discuss** patch management.	BTL-2	Understand	CO4
22	**Give** block diagram of Public-Key encryption/decryption.	BTL-2	Understand	CO4
23	**Express** cryptosystem.	BTL-2	Understand	CO4
24	**Give** block diagram for digital signature using public-key encryption.	BTL-2	Understand	CO4
25	**Describe** business continuity.	BTL-2	Understand	CO4

UNIT IV PART – B					
Q. No	**Question**	**Mark**	**BT Level**	**Competence**	**Course Outcome**
1	**Apply** supply chain best practices for an organization.	16	BTL-3	Apply	CO4
2	**Demonstrate** supply chain management concepts.	16	BTL-3	Apply	CO4
3	**Examine** supply chain flows.	16	BTL-3	Apply	CO4
4	iii. **Illustrate** supply chain management. **iv. Show** a typical sequence of elements involved in supply chain management with a diagram.	8 8	BTL-3	Apply	CO4

5	**iii.Illustrate** Multi-tiered Organization wide Risk Management. **iv. Examine** supply chain risk areas.	8 8	BTL-3	Apply	CO4
6	**Relate** information security incident management and an information security management system (ISMS).	16	BTL-3	Apply	CO4
7	**i. Classify** incident categories and severity classes. **ii. Experiment** phases of digital forensics process.	8 8	BTL-3	Apply	CO4
8	**Discover** NIST cloud computing reference architecture.	16	BTL-3	Apply	CO4
9	i. **Analyze** cloud security. ii. **Estimate** threats for cloud service users.	8 8	BTL-4	Analyze	CO4
10	**Explain** security architecture.	16	BTL-4	Analyze	CO4
11	**Explain** forensic investigations.	16	BTL-4	Analyze	CO4
12	i. **Compare** patch management techiques. **ii. Pointout** three patch management techniques.	6 10	BTL-4	Analyze	CO4
13	**Differentiate** aversarial threats and accidental threats.	16	BTL-4	Apply	CO4
14	**Explain** malware protection activities.	16	BTL-5	Evaluate	CO4
15	**Summarize** identity and access management.	16	BTL-5	Evaluate	CO4
16	**Create** malware system entity relationship diagram and explain practical malware protection.	16	BTL-6	Create	CO4
17	**Formulate** capabilities of malware protection software.	16	BTL-6	Create	CO4
18	**Explain** business continuity with a diagram.	16	BTL-4	Analyze	CO4

UNIT – V SECURITY ASSESSMENT				
Security Monitoring and Improvement-Security Audit-Security Performance-Information Risk Reporting-Information Security Compliance Monitoring-Security Monitoring and Improvement Best practices.				
Q. No	**Questions**	**BT Level**	**Competence**	**Course Outcome**
UNIT V PART – A				
1	**Define** security audit.	BTL-1	Remember	CO5
2	**List** the objectives of security audit.	BTL-1	Remember	CO5
3	**Describe** security audit trail.	BTL-1	Remember	CO5
4	**Identify** data to collect for auditing.	BTL-1	Remember	CO5
5	**Examine** system-level audit trails.	BTL-1	Remember	CO5
6	**Tabulate** security performance metrics for information security.	BTL-1	Remember	CO5
7	**Name** security-related events.	BTL-1	Remember	CO5
8	**What** is system-level audit trails?	BTL-1	Remember	CO5
9	**What** is application-level audit trails?	BTL-1	Remember	CO5
10	**What** is user-level audit trails?	BTL-1	Remember	CO5
11	**Describe** objectives of an internal security audit.	BTL-1	Remember	CO5
12	**What** is physical access audit trails?	BTL-1	Remember	CO5
13	**Describe** objectives of the external security.	BTL-1	Remember	CO5
14	**Summarize** security performance.	BTL-2	Understand	CO5
15	**Describe** security performance metric.	BTL-2	Understand	CO5

16	**Contrast** goal and metrics of System of internal control.	BTL-2	Understand	CO5
17	**Predict** alternate audit capability.	BTL-2	Understand	CO5
18	**Distinguish** goal and metrics of performance and conformance.	BTL-2	Understand	CO5
19	**Estimate** audit storage capacity.	BTL-2	Understand	CO5
20	**Differentiate** internal and external audit.	BTL-2	Understand	CO5
21	**Discuss** about audit generation.	BTL-2	Understand	CO5
22	**Give** examples for security performance metrics.	BTL-2	Understand	CO5
23	**Express** cross-organizational audit.	BTL-2	Understand	CO5
24	**Give** main uses of security metrics.	BTL-2	Understand	CO5
25	**Give** the objectives of information risk reporting.	BTL-2	Understand	CO5

UNIT V PART – B					
Q. No	**Question**	**Mark**	**BT Level**	**Competence**	**Course Outcome**
1	**Apply** security using security audit and alarm model.	16	BTL-3	Apply	CO5
2	**Demonstrate** internal and external audit.	16	BTL-3	Apply	CO5
3	**Examine** security audit controls.	16	BTL-3	Apply	CO5
4	i. **Illustrate** security performance. **ii. Show** sources of security metrics.	8 8	BTL-3	Apply	CO5
5	**i. Illustrate** security performance measurement. **ii. Examine** security performance metrics.	8 8	BTL-3	Apply	CO5
6	**Relate** area and metric with examples of security performance metrics.	16	BTL-3	Apply	CO5
7	**i. Classify** audit log metric with low, moderate and higher risk threshold. **ii. Experiment** Information Security Metric Development Process.	8 8	BTL-3	Apply	CO5
8	**Discover**	16	BTL-3	Apply	CO5
9	i. **Analyze** information risk reporting. ii. **Estimate** risk reporting goals and metrics.	8 8	BTL-4	Analyze	CO5
10	**Explain** information security metrics program implementation process.	16	BTL-4	Analyze	CO5
11	**Explain** about auditable events.	16	BTL-4	Analyze	CO5
12	**i. Explain** audit generation. **ii. Point out** sources of security metrics.	6 10	BTL-4	Analyze	CO5
13	**Explain** security performance measurement.	16	BTL-4	Apply	CO5
14	**Explain** various level of audit trails.	16	BTL-5	Evaluate	CO5
15	**Summarize** information security compliance monitoring**.**	16	BTL-5	Evaluate	CO5
16	**Create** steps for providing technical or automated protection of audit information. enhancements.	16	BTL-6	Create	CO5
17	**Formulate** security monitoring and improvement best practices.	16	BTL-6	Create	CO5
18	**Summarize** security monitoring and reporting.	16	BTL-5	Evaluate	CO5