

SRM VALLIAMMAI ENGINEERING COLLEGE

(An Autonomous Institution)

SRM Nagar, Kattankulathur – 603 203

DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING

QUESTION BANK



II YEAR - III SEMESTER

PCP401 – CYBER SECURITY

Regulation – 2023

Academic Year: 2026 – 2027 (ODD)

Prepared by,

Ms. S. Suma, Assistant Professor / CSE



SRM VALLIAMMAI ENGINEERING COLLEGE

SRM Nagar, Kattankulathur-603203

DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING



QUESTION BANK

SUBJECT : PCP401 - CYBER SECURITY

SEM / YEAR : III SEMESTER / II YEAR

UNIT I - OVERVIEW OF CYBER SECURITY

Introduction - Cyberspace - Cyber Crime - Nature of Threat - Cyber security - Policy, Mission and Vision of Cyber security Program. Cyber security management system - goals, technology categories - perimeter defense and encryption. Cyber security management framework.

UNIT –I [PART-A] – 2 Marks

Q.No	Question	Competence	Level
1	Define cybersecurity.	Remembering	BTL1
2	What is cyberspace?	Remembering	BTL1
3	Define cybercrime and provide one example.	Remembering	BTL1
4	Differentiate between a threat and a vulnerability.	Understanding	BTL2
5	Explain the CIA Triad and its significance in cybersecurity.	Understanding	BTL2
6	What is the primary goal of a cybersecurity program?	Understanding	BTL2
7	Define perimeter defense in the context of cybersecurity.	Remembering	BTL1
8	Explain the role of encryption in ensuring data security.	Understanding	BTL2
9	What are the three main technology categories in a cybersecurity management system?	Understanding	BTL2
10	Differentiate between authentication and authorization.	Understanding	BTL2
11	What is the purpose of a cybersecurity policy?	Understanding	BTL2
12	Define the term "risk" in cybersecurity.	Remembering	BTL1
13	Explain the concept of defense-in-depth.	Understanding	BTL2
14	What is the difference between a security policy and a security procedure?	Understanding	BTL2
15	Describe the role of the mission statement in a cybersecurity program.	Understanding	BTL2
16	What are the key components of a cybersecurity management framework?	Understanding	BTL2
17	Explain the concept of "perimeter defense" and list two perimeter defense technologies.	Understanding	BTL2
18	What is the significance of a vision statement in a cybersecurity program?	Understanding	BTL2
19	Differentiate between cybercrime and cyber-enabled crime.	Understanding	BTL2
20	Explain the nature of cyber threats in modern organizations.	Understanding	BTL2
21	What is the relationship between cybersecurity management and organizational governance?	Understanding	BTL2
22	Define the term "security breach."	Remembering	BTL1
23	Explain why perimeter defense alone is insufficient for comprehensive security.	Understanding	BTL2
24	What are the three pillars of cybersecurity management?	Remembering	BTL1

UNIT –I [PART-B] – 16 Marks

Q.No	Question	Marks	Competence	Level
1	Analyze the evolution of cyberspace and discuss the nature of cyber threats that have emerged, explaining how cybersecurity programs must adapt to address these challenges.	16	Analyzing	BTL4

2	Explain the CIA Triad in detail. How does each component contribute to a comprehensive cybersecurity strategy? Discuss real-world examples where each component has been compromised.	16	Understanding	BTL2
3	Discuss the key components of a cybersecurity management framework. Explain how policy, mission, and vision statements guide the development and implementation of such a framework.	16	Understanding	BTL2
4	Analyze the relationship between cybersecurity goals and technology categories. Explain how perimeter defense and encryption technologies work together to protect organizational assets.	16	Analyzing	BTL4
5	Evaluate the importance of a cybersecurity management system in modern organizations. Discuss the challenges organizations face in implementing such systems and propose strategies to overcome them.	16	Evaluating	BTL5
6	Describe the various categories of cybersecurity technology. How do these technologies support the CIA Triad and contribute to an organization's overall security posture?	16	Understanding	BTL2
7	Analyze the nature of cyber threats facing organizations today. Discuss the factors that contribute to the increasing sophistication of these threats and their impact on cybersecurity management.	16	Analyzing	BTL4
8	Explain the concept of perimeter defense in detail. Discuss its strengths and limitations in the context of modern cybersecurity challenges, including insider threats and cloud computing.	16	Understanding	BTL2
9	Compare and contrast different cybersecurity management frameworks. Discuss the factors organizations should consider when selecting and implementing a framework.	16	Analyzing	BTL4
10	Evaluate the role of encryption in a comprehensive cybersecurity program. Discuss its applications in ensuring confidentiality, integrity, and availability of data.	16	Evaluating	BTL5
11	Discuss the importance of developing a clear vision, mission, and policy for a cybersecurity program. How do these elements influence the program's effectiveness and organizational buy-in?	16	Analyzing	BTL4
12	Create a comprehensive cybersecurity management framework for a medium-sized organization. Justify your selection of components, technologies, and policies.	16	Creating	BTL6
13	Compare the effectiveness of different perimeter defense technologies. Discuss scenarios where each technology would be most appropriate and their limitations.	16	Analyzing	BTL4
14	Explain how cybersecurity goals are translated into technical controls and policies. Provide examples of how specific goals drive the selection of specific security technologies.	16	Understanding	BTL2
15	Analyze the challenges organizations face in implementing cybersecurity management systems in complex, interconnected environments. Propose solutions to address these challenges.	16	Analyzing	BTL4
16	Evaluate the effectiveness of the CIA Triad as a framework for cybersecurity. Discuss whether additional principles should be added to address modern security challenges.	16	Evaluating	BTL5
17	Discuss the role of organizational culture in the success of cybersecurity programs. How can management frameworks help shape security-conscious organizational behavior?	16	Analyzing	BTL4

UNIT – II : ATTACKS AND COUNTERMEASURES

Malicious Attacks, Threats, and Vulnerabilities - Scope of cyber-attacks - Tools used to attack computer systems - security breach - Risks, vulnerabilities and threats. Malware - malicious software attack - social engineering attack - wireless network attack – web application attack - Countermeasures- Types of Network Security Devices -Firewalls, Intrusion Detection Systems, Content Filtering, Virtual Private Networks – Encryption.

UNIT-II [PART-A]- 2 Marks

Q.No	Question	Competence	Level
1	Define malware and provide three examples of malware types.	Remembering	BTL1
2	Differentiate between a vulnerability and an exploit, providing examples for each.	Understanding	BTL2
3	Explain the concept of SQL injection and how it can be prevented.	Understanding	BTL2
4	Define Cross-Site Scripting (XSS) and explain how it can be exploited.	Understanding	BTL2
5	What are the three main categories of security threats?	Remembering	BTL1
6	Explain the term "zero-day exploit" and why it poses a significant threat to cybersecurity.	Understanding	BTL2
7	Define Denial of Service (DoS) attack and Distributed Denial of Service (DDoS) attack, highlighting the difference between them.	Understanding	BTL2
8	Describe the role of social engineering in cyber-attacks and provide two examples of social engineering techniques.	Understanding	BTL2
9	What is ransomware and describe two common methods used to infect systems.	Understanding	BTL2
10	Differentiate between adware and spyware, providing examples of each.	Understanding	BTL2
11	Explain the term "trojan horse" and how it differs from a virus.	Understanding	BTL2
12	Discuss the role of a botnet in cyber-attacks.	Understanding	BTL2
13	Define the term "rootkit" and explain its purpose.	Understanding	BTL2
14	Describe the characteristics of a Man-in-the-Middle (MitM) attack and provide examples of scenarios where MitM attacks can occur.	Understanding	BTL2
15	Explain the term "supply chain attack" and discuss its significance in cybersecurity.	Understanding	BTL2
16	What is spear phishing and why is it often more effective than traditional phishing attacks?	Understanding	BTL2
17	Define wireless network attacks and provide two examples.	Remembering	BTL1
18	What is a web application attack and provide two common types.	Understanding	BTL2
19	Explain the function of a firewall in network security.	Understanding	BTL2
20	Describe the role of an Intrusion Detection System (IDS).	Understanding	BTL2
21	What is content filtering and how does it enhance security?	Understanding	BTL2
22	Explain the purpose of a Virtual Private Network (VPN).	Understanding	BTL2
23	Differentiate between a firewall and an intrusion prevention system (IPS).	Understanding	BTL2
24	What is the difference between active and passive attacks?	Understanding	BTL2

UNIT -II [PART-B]- 16 Marks

Q.No	Question	Marks	Competence	Level
1	Discuss the various types of malicious attacks commonly encountered in cybersecurity. Categorize them and explain the impact of each type on organizations.	16	Analyzing	BTL4
2	Explain the concept of threat, vulnerability, and risk in the context of cybersecurity, illustrating with relevant examples. How do these concepts interrelate?	16	Understanding	BTL2

3	Analyze the scope of cyber-attacks in today's interconnected world, considering motives, targets, and potential impact. Discuss how the scope has evolved over time.	16	Analyzing	BTL4
4	Compare and contrast different types of malware, highlighting their functionalities, infection methods, and potential impact on systems and data.	16	Analyzing	BTL4
5	Describe common attack vectors used by cybercriminals to exploit vulnerabilities in computer systems and networks. Provide countermeasures for each vector.	16	Applying	BTL3
6	Discuss the role of social engineering in cybersecurity attacks, providing examples of common techniques. Analyze why social engineering is often more successful than technical attacks.	16	Analyzing	BTL4
7	Explain the concept of wireless network attacks and discuss common strategies employed by attackers. Describe the countermeasures organizations can implement.	16	Understanding	BTL2
8	Outline the various tools and techniques used for conducting web application attacks. Explain how vulnerabilities like SQL injection and XSS are exploited and prevented.	16	Understanding	BTL2
9	Evaluate the impact of a security breach on an organization's reputation and financial stability, considering both short-term and long-term effects. Provide real-world examples.	16	Evaluating	BTL5
10	Discuss the importance of implementing countermeasures to mitigate cyber-attack risks. Explain the role of firewalls, IDS, VPNs, and encryption in a comprehensive security strategy.	16	Analyzing	BTL4
11	Compare and contrast different types of network security devices. Discuss how they work together to provide defense-in-depth.	16	Analyzing	BTL4
12	Analyze the strengths and limitations of encryption as a countermeasure. Discuss different encryption techniques and their appropriate applications.	16	Analyzing	BTL4
13	Describe the steps involved in conducting a security risk assessment. How does a risk assessment help in selecting appropriate countermeasures?	16	Applying	BTL3
14	Discuss the challenges associated with securing IoT devices against cyber-attacks. Propose strategies and countermeasures to address these challenges.	16	Analyzing	BTL4
15	Explain the concept of zero-day vulnerabilities and their significance. Discuss strategies for mitigating risks associated with unknown vulnerabilities.	16	Understanding	BTL2
16	Evaluate the effectiveness of different types of firewalls in various network configurations. Discuss scenarios where each type would be most appropriate.	16	Evaluating	BTL5
17	Compare the role of Intrusion Detection Systems and Intrusion Prevention Systems. Analyze how these systems complement each other in a comprehensive security architecture.	16	Analyzing	BTL4

UNIT – III : STRATEGIES FOR CYBER SECURITY

Creating a Secure Cyber, Types of Attacks, Comparison of Attacks, Creating an Assurance Framework, Encouraging Open Standards, Strengthening the Regulatory framework, Creating Mechanisms for IT Security, Securing E-Governance Services, and Protecting Critical Information Infrastructure. Areas for Intervention - Legal Responses - Harmonization of Legislation - Criminalization of Cyber Offences - National Security and issues related to Privacy and Freedom of Expression - Investigation Procedures - International Cooperation - Electronic Evidence - Liability of ISPs-Recommendations

UNIT-III [PART-A]- 2 Marks

Q.No	Question	Competence	Level
1	What is an assurance framework in cybersecurity?	Understanding	BTL2
2	Explain the importance of open standards in cybersecurity.	Understanding	BTL2
3	Why is strengthening the regulatory framework important for cybersecurity?	Understanding	BTL2
4	Define E-Governance and explain the security challenges associated with it.	Understanding	BTL2
5	What is Critical Information Infrastructure (CII)?	Remembering	BTL1
6	Explain the concept of harmonization of legislation in the context of cybercrime.	Understanding	BTL2
7	Why is the criminalization of cyber offences important?	Understanding	BTL2
8	Describe the tension between national security and privacy in cyberspace.	Understanding	BTL2
9	What is the role of international cooperation in combating cybercrime?	Understanding	BTL2
10	Define electronic evidence and explain its importance in cybercrime investigations.	Understanding	BTL2
11	What is the liability of Internet Service Providers (ISPs) in cybersecurity?	Understanding	BTL2
12	Explain the purpose of investigation procedures in cybercrime cases.	Understanding	BTL2
13	What is the relationship between freedom of expression and cybersecurity regulations?	Understanding	BTL2
14	Define the term "cyber sovereignty."	Remembering	BTL1
15	What are the key areas for intervention in cybersecurity strategy?	Understanding	BTL2
16	Explain the concept of mechanisms for IT security.	Understanding	BTL2
17	Why is securing E-Governance services a priority for governments?	Understanding	BTL2
18	What are the challenges in protecting Critical Information Infrastructure?	Understanding	BTL2
19	Define the term "cybercrime investigation."	Remembering	BTL1
20	Explain the significance of international conventions on cybercrime.	Understanding	BTL2
21	What are the key components of an assurance framework?	Understanding	BTL2
22	How do legal responses to cybercrime vary across jurisdictions?	Understanding	BTL2
23	What is the role of evidence collection in cybercrime investigations?	Understanding	BTL2
24	Explain the concept of "digital evidence admissibility."	Understanding	BTL2

UNIT -III [PART-B]- 16 Marks

Q.No	Question	Marks	Competence	Level
1	Analyze the key strategies for creating a secure cyber environment. Discuss the importance of assurance frameworks, open standards, and regulatory strengthening.	16	Analyzing	BTL4
2	Compare different types of cyber attacks and their impact on organizations and nations. Propose strategies to counter each type of attack.	16	Analyzing	BTL4

3	Explain the process of creating an assurance framework for cybersecurity. Discuss the components of such a framework and how it enhances organizational security.	16	Understanding	BTL2
4	Discuss the importance of strengthening the regulatory framework for cybersecurity. Evaluate the effectiveness of different regulatory approaches globally.	16	Analyzing	BTL4
5	Analyze the challenges in securing E-Governance services. Propose strategies to protect these services from cyber threats while maintaining accessibility and efficiency.	16	Analyzing	BTL4
6	Explain the concept of Critical Information Infrastructure and its protection. Discuss the unique challenges in protecting CII and propose solutions.	16	Understanding	BTL2
7	Evaluate the legal responses to cybercrime internationally. Discuss the need for harmonization of legislation and the challenges in achieving it.	16	Evaluating	BTL5
8	Discuss the importance of criminalizing cyber offences. Analyze the effectiveness of existing legal frameworks and propose improvements.	16	Analyzing	BTL4
9	Analyze the tension between national security and privacy/freedom of expression in cyberspace. Discuss how governments can balance these competing interests.	16	Analyzing	BTL4
10	Explain the investigation procedures for cybercrime cases. Discuss the role of electronic evidence and the challenges in collecting and preserving it.	16	Understanding	BTL2
11	Discuss the importance of international cooperation in combating cybercrime. Analyze the challenges in international cooperation and propose solutions.	16	Analyzing	BTL4
12	Evaluate the liability of ISPs in cybersecurity matters. Discuss the balance between ISP responsibilities and the need for an open internet.	16	Evaluating	BTL5
13	Create a comprehensive set of recommendations for a national cybersecurity strategy. Justify each recommendation based on best practices and current threats.	16	Creating	BTL6
14	Analyze the role of open standards in enhancing cybersecurity. Discuss the benefits and challenges of adopting open standards in critical sectors.	16	Analyzing	BTL4
15	Compare different approaches to cybersecurity assurance frameworks. Evaluate their effectiveness in various organizational contexts.	16	Analyzing	BTL4
16	Discuss the challenges in securing E-Governance services while maintaining citizen trust. Propose strategies to enhance both security and service delivery.	16	Analyzing	BTL4
17	Evaluate the effectiveness of international conventions on cybercrime. Discuss their impact on national legislation and international cooperation.	16	Evaluating	BTL5

UNIT – IV : POLICIES TO MITIGATE CYBER RISK

Promotion of R&D in Cyber security - Reducing Supply Chain Risks - Mitigate Risks through Human Resource Development - Creating Cyber security Awareness- Information sharing - Implementing a Cyber security Framework. Signatures- Digital Signature, Electronic Signature

UNIT-IV [PART-A]- 2 Marks

Q.No	Question	Competence	Level
1	Why is promoting R&D important for cybersecurity?	Understanding	BTL2
2	Define supply chain risk in the context of cybersecurity.	Understanding	BTL2
3	Explain how human resource development helps mitigate cybersecurity risks.	Understanding	BTL2
4	What is the importance of cybersecurity awareness?	Understanding	BTL2
5	Define information sharing in cybersecurity and explain its benefits.	Understanding	BTL2
6	What is a cybersecurity framework and why is it important?	Understanding	BTL2
7	Define a digital signature and explain its purpose.	Remembering	BTL1
8	Differentiate between a digital signature and an electronic signature.	Understanding	BTL2
9	What are the key components of supply chain risk management?	Understanding	BTL2
10	Explain the role of training in cybersecurity risk mitigation.	Understanding	BTL2
11	How does cybersecurity awareness help in reducing organizational risk?	Understanding	BTL2
12	What are the benefits of implementing a cybersecurity framework?	Understanding	BTL2
13	Define cryptography and its role in digital signatures.	Understanding	BTL2
14	What is Public Key Infrastructure (PKI)?	Understanding	BTL2
15	Explain the concept of non-repudiation and its relationship to digital signatures.	Understanding	BTL2
16	Why is information sharing between organizations important for cybersecurity?	Understanding	BTL2
17	What are the challenges in implementing cybersecurity frameworks?	Understanding	BTL2
18	Define supply chain attacks and provide an example.	Remembering	BTL1
19	How can organizations reduce supply chain risks?	Understanding	BTL2
20	What is the role of certification in cybersecurity awareness?	Understanding	BTL2
21	Explain the difference between a hash function and encryption.	Understanding	BTL2
22	What is the purpose of a Certificate Authority (CA)?	Understanding	BTL2
23	How does information sharing help in threat intelligence?	Understanding	BTL2
24	Define security awareness training and its objectives.	Understanding	BTL2

UNIT -IV [PART-B]- 16 Marks

Q.No	Question	Marks	Competence	Level
1	Discuss the importance of promoting R&D in cybersecurity. Analyze how research and development contributes to addressing emerging cyber threats.	16	Analyzing	BTL4
2	Explain the concept of supply chain risks in cybersecurity. Discuss strategies for identifying, assessing, and mitigating these risks.	16	Understanding	BTL2
3	Analyze how human resource development can mitigate cybersecurity risks. Discuss the role of training, certification, and career	16	Analyzing	BTL4

	development in building security capabilities.			
4	Discuss the importance of creating cybersecurity awareness. Design a comprehensive awareness program for an organization and evaluate its potential effectiveness.	16	Creating	BTL6
5	Evaluate the importance of information sharing in cybersecurity. Discuss the challenges and benefits of sharing threat intelligence among organizations.	16	Evaluating	BTL5
6	Explain the process of implementing a cybersecurity framework. Discuss the factors organizations should consider and the benefits of framework adoption.	16	Understanding	BTL2
7	Compare digital signatures and electronic signatures. Discuss their applications, legal status, and role in ensuring data integrity and authentication.	16	Analyzing	BTL4
8	Analyze the role of policies in mitigating cyber risk. Propose a comprehensive policy framework that addresses R&D, supply chain, HR, and awareness.	16	Analyzing	BTL4
9	Discuss the challenges organizations face in reducing supply chain risks. Propose strategies to address these challenges in the context of global supply chains.	16	Analyzing	BTL4
10	Evaluate the effectiveness of different approaches to cybersecurity awareness. Compare training methods and their impact on reducing security incidents.	16	Evaluating	BTL5
11	Explain the technical and legal aspects of digital signatures. Discuss how they provide authentication, integrity, and non-repudiation.	16	Understanding	BTL2
12	Analyze the role of cybersecurity frameworks in mitigating risk. Compare different frameworks and discuss their applicability in various organizational contexts.	16	Analyzing	BTL4
13	Propose a cybersecurity framework for a small to medium enterprise. Justify the selection of components and discuss implementation challenges.	16	Creating	BTL6
14	Discuss the importance of information sharing in national cybersecurity strategies. Analyze the role of public-private partnerships in threat intelligence sharing.	16	Analyzing	BTL4
15	Evaluate the challenges in implementing digital signature infrastructure. Discuss the role of PKI and the challenges in its adoption.	16	Evaluating	BTL5
16	Discuss the relationship between cybersecurity awareness and organizational culture. Propose strategies to embed security awareness in organizational values.	16	Analyzing	BTL4
17	Analyze the role of R&D in developing innovative cybersecurity solutions. Discuss how research addresses emerging threats and contributes to competitive advantage.	16	Analyzing	BTL4

UNIT – V : CRITICAL INFORMATION INFRASTRUCTURE PROTECTION

National Security - Information Sharing and Coordination - Innovation In Regulatory Approach - Innovation in Security Programs - Proactive Threat and Vulnerability Management - Promoting Best Practices in Critical Infrastructure Sectors - Assessing and Monitoring Security Preparedness of Sectors (Security Index) - Security in Information Technology Supply Chain -Taking Leadership and Participating in International Efforts - Capacity Building in Security Skills and training and Awareness. The Indian Cyberspace- Cyber Threats - Need for a Comprehensive Cyber Security Policy - Need for a Nodal Authority - Need for an International Convention on Cyberspace - Cyber War - Fifth Domain of Warfare - Meeting the Cyber Warfare Challenges.

UNIT-V [PART-A]- 2 Marks

Q.No	Question	Competence	Level
1	What is Critical Information Infrastructure (CII) and why is it important for national security?	Understanding	BTL2
2	Define the term "Security Index" in the context of critical infrastructure.	Understanding	BTL2
3	Explain the importance of information sharing and coordination in protecting CII.	Understanding	BTL2
4	What is meant by proactive threat and vulnerability management?	Understanding	BTL2
5	Why is innovation in regulatory approach important for CII protection?	Understanding	BTL2
6	Define cyber war and explain the concept of the "Fifth Domain of Warfare."	Understanding	BTL2
7	What is a nodal authority and why is it needed in cyberspace governance?	Understanding	BTL2
8	Explain the need for an International Convention on Cyberspace.	Understanding	BTL2
9	What are the key components of security preparedness assessment for critical infrastructure sectors?	Understanding	BTL2
10	Describe the concept of security skills capacity building.	Understanding	BTL2
11	Why is the IT supply chain considered a security concern for critical infrastructure?	Understanding	BTL2
12	What are the characteristics of a comprehensive cyber security policy?	Understanding	BTL2
13	Explain the role of international participation in CII protection.	Understanding	BTL2
14	Define the term "cyber deterrence."	Remembering	BTL1
15	What are the main cyber threats to Indian cyberspace?	Understanding	BTL2
16	Explain the concept of cyber resilience.	Understanding	BTL2
17	What is the significance of best practices in critical infrastructure sectors?	Understanding	BTL2
18	Define incident response in the context of CII.	Remembering	BTL1
19	Explain the importance of proactive vulnerability management.	Understanding	BTL2
20	What is the role of government in CII protection?	Understanding	BTL2
21	Define cyber warfare and differentiate it from traditional warfare.	Understanding	BTL2
22	What are the challenges in meeting cyber warfare challenges?	Understanding	BTL2
23	Explain the concept of information sharing in CII protection.	Understanding	BTL2
24	What is the importance of security awareness in critical infrastructure sectors?	Understanding	BTL2

UNIT -V [PART-B]- 16 Marks

Q.No	Question	Marks	Competence	Level
1	Discuss the relationship between Critical Information Infrastructure Protection and National Security. Analyze the threats to CII and propose comprehensive protection strategies.	16	Analyzing	BTL4
2	Explain the importance of information sharing and coordination in protecting CII. Analyze the challenges in establishing effective	16	Understanding	BTL2

	information sharing mechanisms.			
3	Analyze the need for innovation in regulatory approaches for CII protection. Propose regulatory innovations that could enhance security without hindering innovation.	16	Analyzing	BTL4
4	Discuss the concept of innovation in security programs for CII protection. Evaluate the role of new technologies and approaches in enhancing CII security.	16	Analyzing	BTL4
5	Explain the principles of proactive threat and vulnerability management. Design a proactive vulnerability management program for a critical infrastructure sector.	16	Understanding	BTL2
6	Discuss the importance of promoting best practices in critical infrastructure sectors. Analyze how best practices can be disseminated and adopted across sectors.	16	Analyzing	BTL4
7	Explain the concept of a Security Index for assessing sector preparedness. Evaluate the effectiveness of different assessment methodologies and propose improvements.	16	Understanding	BTL2
8	Analyze the challenges in ensuring security in the IT supply chain. Propose strategies to enhance supply chain security for critical infrastructure.	16	Analyzing	BTL4
9	Discuss the importance of taking leadership and participating in international efforts for CII protection. Evaluate the effectiveness of international cooperation in enhancing CII security.	16	Analyzing	BTL4
10	Explain the concept of capacity building in security skills and awareness. Design a comprehensive capacity building program for critical infrastructure workforce.	16	Understanding	BTL2
11	Analyze the state of Indian cyberspace and its cyber threats. Propose a comprehensive cybersecurity policy for India addressing these threats.	16	Analyzing	BTL4
12	Discuss the need for a Nodal Authority for cybersecurity in India. Propose the structure, functions, and powers of such an authority.	16	Analyzing	BTL4
13	Evaluate the need for an International Convention on Cyberspace. Discuss the challenges in developing such a convention and propose solutions.	16	Evaluating	BTL5
14	Explain the concept of cyber war as the Fifth Domain of Warfare. Analyze the challenges in meeting cyber warfare challenges and propose strategies for cyber deterrence.	16	Understanding	BTL2
15	Analyze the specific challenges in protecting critical information infrastructure in India. Propose sector-specific strategies for sectors like energy, finance, and transportation.	16	Analyzing	BTL4
16	Create a comprehensive framework for assessing and monitoring security preparedness of critical infrastructure sectors. Include metrics, methodology, and implementation guidance.	16	Creating	BTL6
17	Evaluate the role of public-private partnerships in CII protection. Analyze the benefits and challenges of such partnerships and propose models for effective collaboration.	16	Evaluating	BTL5