Programme Structure

Sharda School of Computing Science & Engineering

B.Tech. (CSE) with Specialization in Cyber Security & Forensics (CSF) in association with EC-Council

Programme Code:

Batch: 2026-2030

1.1 Vision, Mission and Core Values of the University

Vision of the University

To serve the society by being a global University of higher learning in pursuit of academic excellence, innovation and nurturing entrepreneurship.

Mission of the University

1. **Transformative educational experience**
2. **Enrichment by educational initiatives that encourage global outlook**
3. **Develop research, support disruptive innovations and accelerate entrepreneurship**
4. **Seeking beyond boundaries**

Core Values

- **Integrity**
- **Leadership**
- **Diversity**
- **Community**

Vision and Mission of the School

Vision of the School

To become a globally acclaimed institution of higher learning in engineering and technology promoting excellence in research, innovation and entrepreneurship

Mission of the School

1. **To impart quality education with strong industry & academic connectivity in the expanding fields of Engineering and Technology in a conductive and enriching learning environment.**
2. **To product technocrats equipped with technical & soft skills and experiential learning required to stay current with the modern tools in emerging technologies to fulfill professional responsibilities and uphold ethical values.**
3. **To inculcate a culture of interdisciplinary research, innovation and entrepreneurship to provide sustainable solutions to meet the growing challenges and societal needs.**
4. **To foster collaborative learning and to play adaptive leadership role in professional career and pursuit of higher education through effective mentoring and counseling.**

Core Values

- **Industry & Academic Connectivity**
- **Experiential learning**
- **Interdisciplinary research**
- **Global**

1.2 Vision and Mission of the Department

Vision of the Department

To be recognized as the fountainhead of excellence in technical knowledge and research in computer science and engineering to attract students and scholars across the globe

Mission of the Department

1. **To strengthen core competency of students to be successful, ethical, effective problem solver in Computer Science & Engineering through analytical learning.**
2. **To promote interdisciplinary research & innovation-based activities in emerging areas of technology globally**
3. **To facilitate and foster the industry-academia collaboration to enhance entrepreneurship skills and acquaintance with corporate culture.**
4. **To inculcate in them a higher degree of social consciousness and moral values towards solving interdisciplinary societal problems using industry-academia collaboration**

Core Values

- **Competency**
- **Global**
- **Entrepreneurship Skills**
- **Interdisciplinary research**

1.3 Programme Educational Objectives (PEO)

1.3.1 Writing Programme Educational Objectives (PEO)

Program educational objectives are broad statements that describe the career and professional accomplishments that the program is preparing graduates to achieve.

The Program Educational Objectives (PEOs) of UG Program in Computer Science & Engineering are:

PEO-1 The graduates will establish themselves as professionals by solving real-life problems using exploratory and analytical skills acquired in the field of Computer Science and Engineering.

PEO-2 The graduates will provide sustainable solutions to ever changing interdisciplinary global problems through their Research & Innovation capabilities.

PEO-3 The graduates will become employable, successful entrepreneur as an outcome of Industry-Academia collaboration.

PEO-4 The graduates will embrace professional code of ethics while providing solution to multidisciplinary social problems in industrial, entrepreneurial and research environment to demonstrate leadership qualities

Methods of Forming PEO's

STEP 1 : The needs of the Nation and society are identified through scientific publications, industry interaction and media.

STEP 2. Taking the above into consideration, the PEOs are established by the Coordination Committee of the department.

STEP 3. The PEOs are communicated to the alumni and their suggestions are obtained.

STEP 4. The PEOs are communicated to all the faculty members of the department and their feedback is obtained.

STEP 5. The PEOs are then put to the Board of Studies of the department for final approval.

1.3.2 Map PEOs with Mission Statements:

DEPARTMENT PEOs / DEPT OF CSE MISSION STATEMENTS	1. The graduates will establish themselves as professionals by solving real-life problems using exploratory and analytical skills acquired in the field of Computer Science and Engineering.	2. The graduates will be able to provide sustainable solutions to ever changing interdisciplinary global problems through their Research & Innovation capabilities.	3. The graduates will become employable, successful entrepreneur and innovator as an outcome of Industry-Academia collaboration.	4. The graduates will be able to embrace professional code of ethics while providing solution to multidisciplinary social problems in industrial, entrepreneurial and research environment to demonstrate leadership qualities.	
1. To strengthen core competency of students to be successful, ethical, effective problem solver in Computer Science & Engineering through analytical learning.	3	3	2	2	10/12
2. To promote interdisciplinary research & innovation based activities in emerging areas of technology globally.	2	3	2	2	9/12
3. To facilitate and foster the industry-academia collaboration to enhance entrepreneurship skills and acquaintance with corporate culture.	2	2	3	3	10/12
4: To inculcate in them a higher degree of social consciousness and moral values towards solving interdisciplinary societal problems using industry-academia collaboration	2	2	2	3	9/12
	9/12	10/12	9/12	10/12	83%

Enter correlation levels 1, 2, or 3 as defined below:

1. Slight (Low) 2. Moderate (Medium) 3. Substantial (High)

If there is no correlation, put "-"

1.3.3 Program Outcomes (PO's)

PO1:	**Engineering knowledge:**	Apply the knowledge of mathematics, science, engineering fundamentals, and an engineering specialization to the solution of complex engineering problems.
PO2:	**Problem analysis:**	Identify, formulate, review research literature, and analyze complex engineering problems reaching substantiated conclusions using first principles of mathematics, natural sciences, and engineering sciences.
PO3:	**Design/development of solutions:**	Design solutions for complex engineering problems and design system components or processes that meet the specified needs with appropriate consideration for the public health and safety, and the cultural, societal, and environmental considerations.
PO4:	**Conduct investigations of complex problems:**	Use research-based knowledge and research methods including design of experiments, analysis and interpretation of data, and synthesis of the information to provide valid conclusions.
PO5:	**Modern tool usage:**	Create, select, and apply appropriate techniques, resources, and modern engineering and IT tools including prediction and modeling to complex engineering activities with an understanding of the limitations.
PO6:	**The engineer and society:**	Apply reasoning informed by the contextual knowledge to assess societal, health, safety, legal and cultural issues and the consequent responsibilities relevant to the professional engineering practice.
PO7:	**Ethics:**	Apply ethical principles and commit to professional ethics and responsibilities and norms of the engineering practice.
PO8:	**Individual and team work:**	Function effectively as an individual, and as a member or leader in diverse teams, and in multidisciplinary settings.
PO9:	**Communication:**	Communicate effectively on complex engineering activities with the engineering community and with society at large, such as, being able to comprehend and write effective reports and design documentation, make effective presentations, and give and receive clear instructions.
PO10:	**Project management and finance:**	Demonstrate knowledge and understanding of the engineering and management principles and apply these to one's own work, as a member and leader in a team, to manage projects and in multidisciplinary environments.
PO11:	**Life-long learning:**	Recognize the need for, and have the preparation and ability to engage in independent and life-long learning in the broadest context of technological change.

PSO1:		Experiment and prepare programming concepts and provide new ideas and innovations towards research and societal issues.
PSO2:		Analyse and develop computer programs in the areas related to algorithms, system software, cloud computing, artificial intelligence & machine learning, bioinformatics, big data analytics, block chain, cyber security and networking for efficient design of computer-based systems of varying complexity.
PSO3:		Apply standard Software Engineering practices and strategies in software project development using open-source programming environment to deliver a quality product for business success.

1.3.4 Mapping of Program Outcome Vs Program Educational Objectives

Mapping	PEO1	PEO2	PEO3	PEO4
PO1	3	3	2	1
PO2	3	3	3	1
PO3	2	2	3	3
PO4	2	2	3	2
PO5	2	3	2	2
PO6	1	2	2	3
PO7	1	1	2	3
PO8	1	1	2	3
PO9	1	2	3	1
PO10	1	1	3	2
PO11	3	2	3	1
PSO1	2	3	1	3
PSO2	3	3	2	2
PSO3	3	3	2	2

1. Slight (Low) ***2. Moderate (Medium)*** ***3. Substantial***

B.Tech (CSE) with Specialization in Cyber Security & Forensics in Association with EC-Council

S. No	Course Type	Course Code	Course Name	Course Tyoe				L	T	P	C	SL	Offered in Term
					Max Marks								
					CA/ Lab	MSE/CE (Viva)	ESE						
1	**Introduction To Specialization**	CSCF 1101	Ethical Hacking Essentials	Theory	25	15	60	2	0	0	2	2	II
2	**Specialized Subject 1**	CSCF 2300	Digital Forensics	Theory +Practical	40	10	50	3	0	2	4	3	III
3	**Specialized Subject 2**	CSCF 2301	Ethical Hacking	Theory +Practical	40	10	50	3	0	2	4	3	IV
4	**Specialized Subject 3**	CSCF 3101	Security Threats Intelligence and Risk Management	Theory	25	15	60	3	0	0	3	3	V
5	**Specialized Subject 4**	CSCF 3302	Windows and Linux Hardening	Theory +Practical	40	10	50	3	0	2	4	3	VI
6	**Specialized Subject 5**	CSCF 3303	Cryptography and Network Defense	Theory +Practical	40	10	50	3	0	2	4	3	VI
7	**Specialized Subject 6**	CSCF 4101	Secure Internet of Things (IOT) systems	Theory	25	15	60	3	0	0	3	3	VII
			Total Credits to be taken								**24**		

List of Program Electives

S. No	Program Electives	Course Code	Course Name	Course Type				L	T	P	C	SL	Offered in Term
					Max Marks								
					CA/ Lab	MSE /CE (Viva)	ESE						
1	PE1	CSCF2302	Machine Learning for Cyber Security	Theory +Practical	25	15	60	3	0	2	4	3	IV
2		CSCF2303	Open source Tools for Cyber Security & Forensics	Theory +Practical	25	15	60	3	0	2	4	3	
3	PE2	CSCF3200	Disaster Recovery Management	Theory	25	15	60	3	0	0	3	3	V
4		CSCF3201	Mobile and Wireless Security	Theory	25	15	60	3	0	0	3	3	
6	PE3	CSCF3202	Web Application Security	Theory	25	15	60	3	0	0	3	3	VI
7		CSCF3203	Malware Analysis	Theory	25	15	60	3	0	0	3	3	
8	PE4	CSCF4200	Cloud Security	Theory	25	15	60	3	0	0	3	3	VII
9		CSCF4201	Penetration Testing	Theory	25	15	60	3	0	0	3	3	
10	PE5	CSCF4202	Exploit Writing	Theory	25	15	60	3	0	0	3	3	VII
11		CSCF4203	Risk Management	Theory	25	15	60	3	0	0	3	3	
13	PE6	CSCF4204	Digital Water Marking and Steganography	Theory	25	15	60	3	0	0	3	3	VII
14		CSCF4205	Information Security & Audit Monitoring	Theory	25	15	60	3	0	0	3	3	

SEMESTER II

COURSE PLAN

Ethical Hacking Essentials (CSCF1101)

Sharda School of Computing Science & Engineering | B.Tech CSE | Semester II | Batch 2026–2030

Theory-Only Course Plan — All 6 COs (CO1–CO6) | Theory Skill Dimensions TS1–TS6 | CA + MTE + ETE Assessment

PART I

COURSE SYLLABUS

Course Identification, Details, Outcomes, BTL Mapping & Lecture Plan

1. Course Identification

School:	SSCSE- Sharda School of Computing Science & Engineering	**Batch:**	2026 – 2030
Program:	B. Tech	**Current Academic Year:**	2026-27
Branch:	CSE	**Semester:**	II
Course Code:	**CSCF1101**	**Course Type:**	Core — Theory Only

2. Course Details

 THEORY-ONLY COURSE — All 6 COs (CO1–CO6) are assessed exclusively via Continuous Assessment (CA), MTE, and ETE. No laboratory component.

S.No	Attribute	Details
1	**Course Code**	**BECF201**
2	**Course Title**	**Ethical Hacking Essentials**
3	**Credits**	2

4	**Contact Hours (L-T-P-SL)**	2-0-0-2 (Theory: 30 hrs. Classroom + 30 hrs. Self-Learning = 60 hrs. total)
5	**Course Status**	**Core — Theory Only (No Laboratory Component)**
6	**Course Objectives**	1. To provide knowledge of legal and policy frameworks governing cybersecurity and ethical hacking. 2. To develop the ability to navigate international and Indian cyber laws and human rights in the digital age. 3. To familiarize students with offensive and defensive cybersecurity strategies within legal boundaries. 4. To enable students to investigate cybercrimes and understand the legal framework for cyber resilience.
7	**Course Outcomes (COs)**	**After successful completion of this course, students will be able to:** **CO1 (Apply/Analyze – L3/L4):** Identify security weaknesses in information systems and apply appropriate security mechanisms to mitigate them. **CO2 (Analyze – L4):** Analyze emerging computer security threats, attack trends, and corresponding defence mechanisms. **CO3 (Understand – L2):** Explain physical, logical, and operational security controls used in information systems protection. **CO4 (Analyze – L4):** Examine and assess the security posture of information systems through auditing and monitoring practices. **CO5 (Understand/Analyze – L2/L4):** Compare different types of computer viruses and their objectives in compromising information security. **CO6 (Evaluate – L5):** Evaluate various intrusion detection techniques and firewall design principles for securing organizational networks.
8	**Course Description**	This course provides an introduction to the fundamental concepts of ethical hacking, network security, and cyber law. Students will explore security threats, vulnerabilities, and cryptography, alongside essential management practices for information security. It covers legal frameworks addressing constitutional and human rights issues in cyberspace. Practical insights into cybercrime analysis, hacking methodologies, and digital forensics are integrated to prepare students for real-world cybersecurity challenges.
9	**Teaching & Learning Scheme**	Classroom Instructions (CI): 45 hrs. | Self Learning (SL): 45 hrs. | Total: 90 hrs.
10	**Mode of Examination**	**Theory Only. CAM: 20% | MTA: 10% | Quiz: 5% | Assignment: 15% | ETE: 50%**
11	**Textbook**	1. William Stallings and Lawrie Brown, *Computer Security: Principles and Practice*, Pearson, Latest Edition

		2. Mike Chapple, David Seidl, James Michael Stewart, CISSP Official Study Guide, Wiley. *(Excellent for security controls, auditing, risk management, IDS/firewalls, governance)* 3. David Kim and Michael G. Solomon, *Fundamentals of Information Systems Security*, Jones & Bartlett
12	**References**	1. Chris Davis, Mike Schiller, Kevin Wheeler, *IT Auditing Using Controls to Protect Information Assets*, McGraw Hill. 2. ISO/IEC 27001:2013 Information Security Management Systems. *(Strong Compliance reference)* 3. Nina Godbole & Sunit Belapure, *Cyber Security: Understanding Cyber Crimes, Computer Forensics and Legal Perspectives*, Wiley India

3. Outline Syllabus with CO Mapping

All CO mappings in this section refer to Theory COs (CO1–CO6). This is a theory-only course; all assessment is via CA, MTE, and ETE.

	Topic	CO Mapping
Unit 1	**Introduction to Information Security and Cyber Security**	
A	Introduction to Information Security, Cyber Security	**CO1, CO3**
B	Legal vs Illegal: Types of Hackers , Attack, Vulnerability, Risk	**CO3, CO4**
C	Ethical Hacking Fundamentals	**CO3, CO4**
Unit 2	**Traversing payloads**	
A	Payloads: Viruses, Worms , Trojan	**CO1, CO2, CO3**
B	Advanced Payloads: Spyware, Adware, Malware, Ransomware	**CO1, CO3, CO4**
C	Ethical Hacking Phases.	**CO2, CO3, CO4**
Unit 3	**Network and Windows OS as Defense**	
A	Networking basics : Types of Network, Introduction to Networking Devices	**CO2, CO3**

B	Defensive Overview: Firewall, Anti-Virus, Anti-Malware , UAC	CO2, CO3
C	Windows inbuilt Security, Window's Patch , Driver Update	CO3, CO4
Unit 4	**Cyber Crimes and Its Counter measures**	
A	Digital Arrest, Deep Fake, Phishing, Scammer based attacks, Cyber Bullying vs Cyber Stalking , Cyber Terrorism, Cyber Defamation	CO1, CO4
B	Fighting Cybercrimes: Cyber Awareness , Cyber Hygiene	CO2, CO5
C	Government Initiatives to fight against Cybercrime, Social Engineering Techniques and Countermeasures	CO4, CO6
Unit 5	**Cyber Law: Indian and International Perspectives**	
A	Overview of the Information Technology Act, 2000 and IT (Amendment) Act, 2008	CO4, CO5
B	Digital signatures, electronic records, and e-governance	CO4, CO5, CO6
C	Cybercrimes and legal provisions under Indian law, Overview of Digital Personal Data Protection (DPDP) Rules, 2025	CO5, CO6

4. Topic-wise Bloom's Taxonomy Level Mapping

S.No	Topic	L1 Remember	L2 Understand	L3 Apply	L4 Analyze	L5 Evaluate	L6 Create
1	1.A	□	□		□		
2	1.B		□	□	□		□
3	1.C	□	□		□	□	
4	2.A	□	□	□			
5	2.B	□	□	□	□		
6	2.C		□	□	□	□	
7	3.A	□	□	□			

8	3.B	□	□	□	□		
9	3.C		□	□	□	□	
10	4.A	□	□	□			
11	4.B	□	□	□	□		
12	4.C	□	□	□	□	□	
13	5.A	□	□		□		□
14	5.B		□	□	□	□	
15	5.C		□	□	□	□	□

5. CO vs Bloom's Taxonomy — All Three Domains

ℹ *Only strong/dominant alignments are mapped. This is a theory-only course; Psychomotor mapping is limited to Guided Response (P3) for algorithm implementation in CO3. Affective domain appears at A3 (Valuing) for efficiency analysis in CO4 and CO5.*

CO	Cognitive Domain (L1–L6)						Affective (A1–A5)					Psychomotor (P1–P7)						
CO	L1	L2	L3	L4	L5	L6	A1	A2	A3	A4	A5	P1	P2	P3	P4	P5	P6	P7
CO1	□	□					□											
CO2		□	□	□				□					□	□				
CO3		□	□	□			□						□	□				
CO4				□	□				□									
CO5			□	□	□	□			□					□	□			
CO6		□	□	□	□			□					□	□				

Legend: □ = Strong / Dominant mapping. Theory-only course: Cognitive domain is primary. Psychomotor (P3) limited to CO3 (algorithm implementation). Affective (A3) for CO4 and CO5 (valuing efficiency).

6. Lecture Plan Outline (Theory — 30 Lectures / 30Hours)

ℹ *Total classroom contact: 30 hours across 5 units. Self-Learning activities (30 hrs.) are structured separately in Section 11.*

Date	Topics to be Covered/Title	UNIT	Total Lectures
DD/MM/YYYY	Introduction to Information Security	Unit 1	6
DD/MM/YYYY	Introduction to Cyber Security		
DD/MM/YYYY	Types of Hackers		
DD/MM/YYYY	Attacks, Vulnerabilities, and Risk		
DD/MM/YYYY	Ethical Hacking Fundamentals		
DD/MM/YYYY	Legality, and ethics.		
DD/MM/YYYY	Introduction to Payloads	Unit 2	6
DD/MM/YYYY	Viruses, Worms, and Trojans		
DD/MM/YYYY	Life Cycle of Virus		
DD/MM/YYYY	Spyware, Adware		
DD/MM/YYYY	Malware and Ransomware		
DD/MM/YYYY	Ethical Hacking Phases		
DD/MM/YYYY	Networking Basics	Unit 3	6
DD/MM/YYYY	Networking Devices		
DD/MM/YYYY	Firewalls and Security Software		
DD/MM/YYYY	User Account Control (UAC) and Windows Security		
DD/MM/YYYY	Windows Updates and Driver Updates		
DD/MM/YYYY	Patch and its need		
DD/MM/YYYY	Digital Arrest, Deepfake, and Phishing	Unit 4	6
DD/MM/YYYY	Scam-based Attacks		
DD/MM/YYYY	Cyber Bullying, Cyber Stalking		

DD/MM/YYYY	Cyber Defamation, Cyber Terrorism		
DD/MM/YYYY	Cyber Awareness and Cyber Hygiene		
DD/MM/YYYY	Government Initiatives and Social Engineering		
DD/MM/YYYY	Information Technology Act, 2000	Unit 5	6
DD/MM/YYYY	IT (Amendment) Act, 2008		
DD/MM/YYYY	Digital Signatures, Electronic Records, and E-Governance		
DD/MM/YYYY	Cybercrimes under Indian Law		
DD/MM/YYYY	Overview of Digital Personal Data Protection (DPDP) Rules, 2025		
DD/MM/YYYY	Case Studies		

PART II

THEORY ASSESSMENT FRAMEWORK

Theory Skill Dimensions, CO × TS Mapping, CA / MTE / ETE Structure

7. Theory Skill Dimensions (TS1–TS6)

THEORY-ONLY COURSE — All 6 COs (CO1–CO6) are assessed exclusively via Continuous Assessment (CA), MTE, and ETE. No laboratory component.

Six Theory Skill Dimensions — one per Bloom's progression (L1–L4) — correspond directly to the six COs. They define precisely what competency is being measured in each section of the CA, MTE, and ETE, providing a clear NBA-auditable assessment rationale.

ID	Dimension	What is Measured	CO / BTL	Assessment
TS1	Cyber Security Fundamentals & Threat Identification	Understand information security concepts, identify cyber threats, vulnerabilities, risks, and distinguish different types of hackers and attacks.	**CO1 / CO6 | L1–L2**	CA | MTE Sec A | ETE Sec A
TS2	Malware Analysis & Ethical Hacking Fundamentals	Identify various types of malware and payloads, understand ethical hacking concepts and phases, and recommend appropriate security measures.	**CO2 / CO3 | L2–L4**	CA | MTE Sec A | ETE Sec A

TS3	Network & Operating System Security	Apply networking fundamentals and Windows security features including firewalls, antivirus, anti-malware, UAC, patches, and updates for system protection.	**CO1 / CO6 | L3**	CA | MTE Sec B | ETE Sec B
TS4	Cybercrime Awareness & Countermeasures	Analyze cybercrimes such as phishing, deepfakes, digital arrest scams, cyberbullying, cyberstalking, and recommend cyber hygiene and social engineering countermeasures.	**CO3 / CO6 | L3–L4**	MTE Sec B | ETE Sec B
TS5	Cyber Law & Data Protection	Explain the provisions of the IT Act 2000, IT Amendment Act 2008, digital signatures, e-governance, cybercrime laws, and DPDP Rules 2025.	**CO4 / CO6 | L4–L5**	ETE Sec B/C
TS6	Integrated Cyber Security Practices	Integrate cybersecurity concepts, legal compliance, defensive technologies, and awareness practices to address organizational security challenges through case studies and project work.	**CO5 / CO6 | L4–L5**	ETE Sec C

8. CO × Theory Skill Dimension Mapping (6 COs × 6 Dimensions)

ℹ *Each CO maps primarily to one TS dimension (H) with adjacent dimensions receiving secondary mapping (M), reflecting the progressive Bloom's structure of this course.*

CO	TS1 Conceptual Fundamentals	TS2 Process Interpretation	TS3 Security Applications	TS4 Cyber Law & Governance	TS5 Constitutional Rights	TS6 Cyber Crime Analysis
CO1	M	H	H	M		
CO2		H	M	M	M	
CO3	H	H	M			
CO4		M		H	M	M
CO5		H			H	
CO6		M	M	M	H	H

H = High / Primary alignment **M** = Medium / Secondary alignment *Blank = No direct alignment*

9. Continuous Assessment (CA) — 25 Marks

CA is formative and covers COs progressively as the syllabus is taught. It includes numerical-based assignments, a technical video learning report, and a real-world case study — mirroring TS1 through TS6.

9.1 CA Component Breakdown (Sample)

Component	Quantum	Marks	COs Assessed	Skill Dimensions
Assignments 1–5 (Ethical Hacking / Cyber Law / Rights / Cyber Crime Tasks)	5 Assignments	15	CO1, CO2, CO3, CO4	TS1, TS2, TS3, TS4
Technical Video Learning Report + Presentation	1 Report + Presentation	5	CO2, CO4, CO6	TS2, TS4, TS6
Real-World Security Audit / Incident Case Study Report	1 Report	5	CO4, CO5, CO6	TS4, TS5, TS6
TOTAL	—	25	CO1–CO6	TS1–TS6

9.2 Assignment-wise CO & TS Mapping

Item	Topic / Focus	COs	TS Dims	SL Hours	Evaluation Criteria
Assignment 1	Information security, cyber security, types of hackers, threats, vulnerabilities, risks, and ethical hacking fundamentals	CO1, CO3	TS1	5 hrs.	Conceptual clarity, networking terminology, threat identification accuracy.
Assignment 2	Malware and payloads: Viruses, worms, trojans, spyware, adware, malware, ransomware, and ethical hacking phases	CO2, CO3	TS2	5 hrs.	Threat analysis, control interpretation, comparative analysis of security controls

Assignment 3	Networking basics, networking devices, firewalls, antivirus, anti-malware, UAC, Windows security, patches, and driver updates	CO1, CO3	TS3	5 hrs.	Application of security mechanisms, cryptographic understanding, authentication implementation logic
Assignment 4	Cybercrimes: Digital arrest, deepfakes, phishing, scam-based attacks, cyber bullying, cyber stalking, cyber terrorism, cyber defamation, cyber hygiene, and social engineering countermeasures	CO4	TS4	5 hrs.	Audit assessment quality, log interpretation, analytical reasoning, compliance analysis
Assignment 5	IT Act 2000, IT (Amendment) Act 2008, digital signatures, electronic records, e-governance, cybercrime laws, and DPDP Rules 2025	CO5, CO6	TS5, TS6	5 hrs.	Threat evaluation, defense mechanism comparison, incident response reasoning, technical recommendations
Video Learning Report	Technical video on malware analysis, Windows security, network security, phishing prevention, cyber awareness, or cyber laws (minimum **3 hours**) with structured report and presentation	CO2, CO4, CO6	TS2, TS4, TS6	9 hrs.	Report on learning outcomes, threat interpretation, audit/monitoring understanding, self-reflection; Presentation (10 min)
Case Study Report	Real-world case study on ransomware, phishing campaigns, deepfake incidents, digital arrest scams, enterprise security breaches, or cyber law cases with detailed analysis	CO4, CO5, CO6	TS4, TS5, TS6	11 hrs.	Technical depth, factual analysis, security assessment, threat evaluation, incident handling recommendations

10. Mid Term Examination (MTE) — 10 Marks (Units 1–3)

ℹ *MTE covers Units 1–3 (CO1, CO2, CO3). CO4, CO5 and CO6 are assessed in ETE and CA. MTE maps to TS1–TS4.*

Section	Marks	Theory Skill Dimensions	COs Assessed	Question Type & Guidance
Section A	**4**	TS1 — Information Security Fundamentals TS2 — Threat Analysis & Security Control Interpretation	CO1, CO2	Short-answer questions: information security concepts, IS audit fundamentals, governance, security controls, malware concepts, threat analysis, audit standards, access control principles
Section B	**6**	TS3 — Security Mechanism Application & Cryptography TS4 — Audit	CO1, CO3	Analytical/application questions: cryptographic applications, authentication mechanisms, audit lifecycle, audit assessment scenarios,

		Monitoring & Security Assessment Analysis		logging analysis, compliance evaluation, monitoring case-based questions
TOTAL	**10**	**TS1–TS4**	**CO1–CO3**	**Units 1–3 only. CO4, CO5 and CO6 assessed in ETE and CA.**

11. End Term Examination (ETE) — 50 Marks (All Units, All COs)

ℹ *ETE is comprehensive — all 5 units and all 6 COs (CO1–CO6). Minimum 24/60 required to pass.*

Section	Marks	Theory Skill Dimensions	COs Assessed	Question Type & Guidance
Section A	15	**TS1** — Cyber Security Fundamentals & Threat Identification **TS2** — Malware Analysis & Ethical Hacking Fundamentals	CO1, CO2, CO3	Short-answer questions (all units): definitions, information security, cyber security, hackers, attacks, vulnerabilities, malware, ethical hacking, networking basics, cyber awareness.
Section B	25	**TS3** — Network & Operating System Security **TS4** — Cybercrime Awareness & Countermeasures	CO3, CO4, CO5, CO6	Medium analytical questions: networking devices, firewalls, antivirus, Windows security, cybercrime analysis, phishing, deepfakes, digital arrest scams, social engineering, cyber hygiene, countermeasures.
Section C	10	**TS5** — Cyber Law & Data Protection **TS6** — Integrated Cyber Security Practices	CO5, CO6	Long/evaluation questions: IT Act 2000, IT (Amendment) Act 2008, digital signatures, DPDP Rules 2025, cyber law case studies, integrated security solutions, organizational cyber security strategies.
TOTAL	50	TS1–TS6 (all)	CO1–CO6	Scaled from 100-mark paper if needed. Minimum 20/50 to pass.

11.1 CO-wise Assessment Instrument Summary

CO	CO Statement (Short)	CA (25)	MTE (25)	ETE (50)	TS	PO Primary
CO1	Explain information security, cyber security concepts, identify threats, vulnerabilities, risks, and ethical hacking fundamentals.	✓	✓	✓	TS1 / TS3	PO1, PO2, PO3, PO5
CO2	Identify and analyze malware, payloads, and ethical hacking phases to recommend appropriate security measures.	✓	✓	✓	TS2	PO1, PO2, PO4
CO3	Apply networking concepts and Windows security mechanisms to protect systems and networks.	✓	✓	✓	TS1 / TS2 / TS3	PO1, PO2, PO5
CO4	Analyze cybercrimes, social engineering attacks, and implement cyber awareness and countermeasures.	✓	✓	✓	TS4 / TS6	PO2, PO4, PO5
CO5	Explain cyber laws, digital signatures, e-governance, and data protection regulations applicable to cyber security.	✓	—	✓	TS5	PO2, PO4
CO6	Integrate cyber security principles, legal compliance, and defensive practices to solve organizational security challenges.	✓	—	✓	TS5 / TS6	PO4, PO5, PSO3

CO5 and CO6 are NOT assessed in MTE (only Units 1–3 are covered at mid-semester). They are assessed in CA (self-learning activities) and ETE.

PART III

COMBINED MAPPINGS & REFERENCE

CO–PO Matrix, CO–PO Alignment, Self-Learning Activities, Bloom's Reference, Attendance & Pass/Fail

12. CO–PO and CO–PSO Mapping Matrix (Original Framework)

Strength Scale: 3 = Substantial (High) | 2 = Moderate | 1 = Slight (Low) | — = Not Applicable. Averages computed over non-zero entries only. PO framework as per the original course design.

CO	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PSO1	PSO2	PSO3
CO1	3	2	-	-	1	-	-	-	-	-	1	2	1	-
CO2	3	2	1	-	2	-	-	-	1	-	2	2	2	1
CO3	3	3	2	-	2	2	-	-	1	-	2	3	2	2
CO4	2	3	2	2	2	2	1	-	-	-	2	3	2	3
CO5	2	3	3	2	2	2	1	-	1	-	2	2	3	2
CO6	3	3	3	3	3	3	3	3	3	2	3	-	-	3
Avg	**2.67**	**2.67**	**2.20**	**2.00**	**2.00**	**2.00**	**1.33**	**2.00**	**1.00**	**1.00**	**2.00**	**2.33**	**2.33**	**2.00**

13. CO × PO Alignment Map (H/M Indicators — All 6 COs)

CO	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PSO1	PSO2	PSO3
CO1	H					M					H	H	H	
CO2	M				H	M		M			H	H	H	
CO3	H	H	H		H	M					M	M	H	
CO4	H	H	H	H		M	M	1	-	2	M			H
CO5	M	H	M		M	M	M						H	
CO6	3	3	3	2	3	2	2	2	1	1	3	3	3	3

= High / Primary alignment **M** = Medium / Secondary alignment *Blank = No direct alignment*

14. Self-Learning Activities (SL: 45 Hours)

S.No	Activity	Hours	COs / TS	Evaluation Criteria
1	Assignment Writing (5 assignments covering Networking, Security Management, Cyber Law, Rights, and Cyber Crime).	5 assignments × 5 hrs. each Total = 25 hrs.	CO1–CO6 TS1–TS6	Evaluated based on conceptual understanding, threat analysis, security mechanism application, audit assessment quality, technical correctness, analytical reasoning, and solution recommendations

2	Technical Video-Based Learning on hacking tools, cyber crime cases, and legal frameworks.	Video viewing: 3 hrs. Report preparation: 3 hrs. Presentation: 3 hrs. Total = 9 hrs.	CO2, CO4, CO6 TS2, TS4, TS6	Report + presentation based on learning outcomes, threat understanding, audit monitoring insights, security assessment observations, technical interpretation, and self-reflection
3	Real-World Case Study Analysis on Cyber Attacks, IT Act implementations, and Legal disputes.	Data collection / study: 4 hrs. Report preparation: 4 hrs. Presentation / discussion: 3 hrs. Total = 11 hrs.	CO4, CO5, CO6 TS4, TS5, TS6	Evaluated based on technical depth, factual investigation, security audit interpretation, defense mechanism evaluation, forensic reasoning, and mitigation recommendations
	TOTAL Self-Learning Hours	45 Hours	CO1–CO6	All activities are compulsory. Submission deadlines communicated at the start of the semester.

15. Bloom's Taxonomy — Domain Level Reference

Cognitive Domain (6 Levels)	Affective Domain (5 Levels)	Psychomotor Domain — Simpson (7 Levels)
L1 — Remember: Recall facts, definitions, basic concepts L2 — Understand: Explain ideas, concepts, and principles L3 — Apply: Use knowledge to solve problems in new situations L4 — Analyze: Break down information, examine relationships L5 — Evaluate: Judge, justify, assess, and make decisions L6 — Create: Design, develop, and produce new artefacts	A1 — Receiving: Awareness and willingness to attend A2 — Responding: Active participation and reaction A3 — Valuing: Commitment and assigning value to content A4 — Organizing: Integrating values into a personal system A5 — Characterizing: Internalized value system	P1 — Perception: Sensory cues guide motor activity P2 — Set: Mental, physical readiness to act P3 — Guided Response: Practice through imitation/trial P4 — Mechanism: Habitual correct performance P5 — Complex Overt Response: Skilled performance P6 — Adaptation: Modify skills for special situations P7 — Origination: Create new solution patterns

OBE Compliance Statement: This is a theory-only course. All 6 COs are mapped primarily to the Cognitive domain (L1–L5). Psychomotor domain (P3) appears only for CO3 (algorithm implementation as mental tracing). Affective domain (A3) appears for CO4 and CO5, reflecting valuing of algorithmic efficiency.

16. Attendance Policy & Pass / Fail Criteria

16.1 Attendance Policy

Component	Minimum	Applicable To	Consequence
Theory Classes	**75%**	All lecture sessions	Debarred from ETE if below threshold
Self-Learning / Assignment Submission	**All activities**	SL activities (45 hrs.)	Incomplete SL affects CA score directly

 Theory attendance must meet 75% minimum. Missing SL activities (assignments, video report, case study) directly impacts CA marks and is not compensable by exam performance.

16.2 Pass / Fail Criteria

Condition	Threshold	Status	Remarks
ETE Score	≥ 24 / 60	**MANDATORY**	40% of ETE paper required; failing ETE means failing the course regardless of CA + MTE
Overall Total (CA + MTE + ETE)	≥ 40 / 100	**Must pass overall**	CA 25 + MTE 10 + ETE 50 + Other 15 = 100; 40% overall minimum required

CSCF1101 — MEASUREMENT ARCHITECTURE SUMMARY

Theory-Only Course | 6 COs (CO1–CO6) | 3 Assessment Instruments | 6 Theory Skill Dimensions (TS1–TS6)

CO1–CO2: Conceptual / Understand → TS1, TS2 → CA + MTE Sec A + ETE Sec A

CO3–CO4: Apply / Analyze → TS3, TS4 → CA + MTE Sec B + ETE Sec B

CO5–CO6: Analyze / Evaluate → TS5, TS6 → CA + ETE Sec B/C

CA 25 marks + MTE 10 marks + ETE 50 marks + Other 15 marks = Total 100 marks

SEMESTER III

COURSE PLAN

Digital Forensics

School of Computing Science & Engineering (SSCSE) | B.Tech CSE | Semester III | Batch 2026–2030

Integrated Course Plan — Theory COs (CO1–CO6) + Lab COs (CO7–CO10) | New AICTE 11-PO Framework | Full Skill Mapping

PART I

COURSE SYLLABUS

Course Identification, Details, Outcomes, BTL Mapping & Lecture/Lab Plans

1. Course Identification

School:	SSCSE	**Batch:**	2026–2030
Program:	B.Tech	**Current Academic Year:**	2026–27
Branch:	CSE	**Semester:**	III

2. Course Details

Integrated theory + laboratory model. 10 COs in two tiers: Theory COs (CO1–CO6) via MTE + ETE; Lab COs (CO7–CO10) via Laboratory Assessment only. No cross-evaluation.

S.No	Attribute	Details
1	**Course Code**	CSCF2300
2	**Course Title**	**Digital Forensics / Digital Forensics Lab**
3	**Credits**	4
4	**Contact Hours (L-T-P-SL)**	3-0-2-3

5	**Course Status**	Core
6	**Course Objective**	Hands-on labs and case-based simulations using industry-standard and open-source digital forensics tools to analyze disk images, network logs, and mobile data through complete investigations from acquisition to evidence presentation. Students develop investigative proficiency and prepare structured forensic reports aligned with real-world legal and professional practices.
7	**Course Outcomes (COs)**	**After successful completion of this course, the student will be able to:** **THEORY COs — Assessed via MTE + ETE:** CO1 (Remember – L1): Demonstrate the principles of Digital Forensics and how resultant evidence can be applied within legal cases. CO2 (Understand – L2): Illustrate their competence in recovering files, network forensics, password cracking CO3 (Apply – L3): Evaluate the effectiveness of available digital forensics tools and use them in a way that optimizes the efficiency and quality of digital forensics investigations. CO4 (Analyze – L4): Apply a solid foundational grounding in computer networks, operating systems, file systems, hardware, and mobile devices to digital investigations and to the protection of computer network resources from unauthorized activity CO5 (Evaluate – L5): Access and critically evaluate relevant technical and legal information and emerging industry trends CO6 (Create – L6): Adapt effectively the results of a computer, network, and/or data forensic analysis verbally, in writing, and in presentations to both technical and lay audiences. **LAB COs — Assessed via Laboratory Assessment only:** CO7 (Apply – L3): List potential security breaches of computer data that suggest violations of legal, ethical, moral, policy, and/or societal standards CO8 (Create – L5/L6): Prepare and present comprehensive digital forensic investigation reports and findings through written, verbal, and presentation formats for both technical and non-technical audiences. CO9 (Apply – L2/L3): Collaborate effectively with clients, management, and law enforcement agencies to support digital investigations and enhance the security of digital resources. CO10 (Apply – L3): Demonstrate professional and ethical conduct in digital forensic practices by ensuring impartiality, legal compliance, and protection of personal privacy.
8	**Teaching & Learning**	Classroom Instructions (CI) 45 hrs + Lab Instructions (LI) 30 hrs + Self Learning (SL) 45 hrs = 120 hrs
9	**Mode of Examination**	Lab (40 marks) + MTE (10 marks) + ETE (50 marks) = 100 marks. Theory COs: MTE + ETE only. Lab COs: Lab only.

10	**Self Learning (SL: 45 hrs)**	1. Install and explore Autopsy and Wireshark to analyze sample disk images and network traffic logs, identify digital evidence, and prepare a structured forensic report. 2. Perform a simulated end-to-end digital forensic investigation including evidence acquisition, file recovery, log analysis, timeline creation, and presentation of findings for a mock cybercrime case. 3. Study recent advancements such as cloud forensics, mobile forensics, IoT forensics, and anti-forensic techniques, and prepare a technical presentation and summary report discussing challenges and investigation methods.
11	**References**	1. Textbook: Behrouz A. Forouzan, "Cryptography And Network Security"- McGraw Hill. 2. Cryptography and Network Security: Principles and Practice Author: William Stallings Edition: 8th Edition (2024) 3. Introduction to Modern Cryptography Authors: Jonathan Katz, Yehuda Lindell Edition: 4th Edition (2025) 4. Cryptography: Theory and Practice Author: Douglas R. Stinson, Maura Paterson Edition: 4th Edition

3. Outline Syllabus — Theory Units with CO Mapping (CO1–CO6)

Unit CO mappings refer to Theory COs (CO1–CO6) only. Lab experiments reinforce these units but are assessed under Lab COs (CO7–CO10).

	Topic / Activity	CO Mapping
Unit 1	**Introduction To Computer Forensics: (8-0-0-6 = 14hrs)**	
A	History of Forensics – Computer Forensic Flaws and Risks	CO1, CO2, CO3
B	Rules of Computer Forensics – Legal issues – Digital Forensic Principles	
C	Digital Environments – Digital Forensic Methodologies	
Tools Used	NA	

Activities	**Objective:** • . Understand the evolution, concepts, risks, and challenges of computer forensics. • Apply legal, ethical, and procedural principles in digital forensic investigations. • Analyze digital forensic environments, methodologies, and investigation processes.	
Unit 2	**An Overview of Digital Forensics Investigation: (10-0-0-9= 19 hrs)**	
A	Live forensics and investigation –digital evidence	CO1, CO2,CO3,CO5
B	seizure methodology factors limiting the whole sale seizure of hardware- Demystifying computer/ cyber crime	
C	explosion of networking – explosion of wireless networks – interpersonal communication	
Tools Used	Wireshark, Autopsy,	
Activities	**Objective:** • Collection and analysis of volatile digital evidence from active systems. • Procedures and limitations in acquiring and preserving digital evidence. • Impact of networking, wireless systems, and communication technologies on cybercrime growth.	
Unit 3	**Data Forensics (9-0-0-10 = 19 hrs)**	
A	Recovering deleted files and deleted partitions – deleted file recovery tools –	CO2, CO3, CO4, CO5, CO6
B	Deleted partitioned recovery tools – data acquisition and duplication	
C	Data acquisition tools – hardware tools – backing up and duplicating data.	
Tools Used	FTK Imager	

Activities	**Objective:** • Recover deleted files and partitions using forensic recovery tools and techniques. • Perform data acquisition, duplication, backup, and preservation of digital evidence. • Explore hardware and software tools used for forensic data acquisition and recovery.	
Unit 4	**Router Forensics And Network Forensics (9-0-0-10 = 19 hrs)**	
A	Overview of Routers – Hacking Routers – Investigating Routers	CO3, CO4, CO5
B	Investigating Wireless Attacks – Basics of wireless - Wireless Penetration Testing	
C	Direct Connections to Wireless Access Point – Wireless Connect to a Wireless Access Point.	
Tools Used	Wireshark, Nmap, tcpdump , Netcat	
Activities	**Objective:** • Understand router architecture, router hacking techniques, and forensic investigation of routers. • Analyze wireless attacks and perform basic wireless penetration testing techniques. • Study methods of connecting and investigating wireless access points and wireless networks.	
Unit 5	**E-Mail Forensics and Steganography (9-0-0-10 = 19 hrs)**	
A	Forensics Acquisition – Processing Local mail archives –	CO2, CO3, CO4, CO5, CO6
B	Processing server level archives – classification of steganography	
C	categories of steganography in Forensics – Types of password cracking.	

Tools Used	John the Ripper, The Sleuth Kit	
Activities	**Objective:** • Understand e-mail forensic acquisition and analysis of local and server-level mail archives. • Classify steganography techniques and their applications in digital forensics investigations. • Explore password cracking methods and forensic techniques for credential recovery.	

4. Topic-wise Bloom's Taxonomy Level Mapping (Theory)

S.No	Topic	L1	L2	L3	L4	L5	L6
1	1.A	□	□				
2	1.B		□	□			
3	1.C		□	□			
4	2.A			□			
5	2.B			□			
6	2.C			□	□		
7	3.A			□	□		□
8	3.B		□	□		□	
9	3.C			□	□		
10	4.A			□	□		
11	4.B			□	□	□	
12	4.C			□			
13	5.A		□	□		□	□

14	5.B			□	□		□
15	5.C			□	□	□	□

5. CO vs Bloom's Taxonomy — All Three Domains (Updated for 10 COs)

□ *Only strong/dominant alignments are mapped. Lab COs (CO7–CO10) extend into Psychomotor and Affective domains, reflecting the skill-based nature of lab and project work.*

CO	Cognitive Domain (L1–L6)						Affective (A1–A5)					Psychomotor (P1–P7)						
CO	L1	L2	L3	L4	L5	L6	A1	A2	A3	A4	A5	P1	P2	P3	P4	P5	P6	P7
CO1	□																	
CO2		□																
CO3			□											□				
CO4				□											□			
CO5					□											□		
CO6						□			□							□	□	
CO7			□					□						□	□			
CO8					□	□			□						□	□	□	
CO9			□							□	□							
CO10			□					□			□			□				

Legend: □ = Strong / Dominant mapping only. Theory COs: primarily Cognitive. Lab COs: span all three domains.

6. Lecture Plan Outline (Theory — 45 Lectures)

Date	Topics to be Covered	Unit	Total Lectures
DD/MM/YY	History of Forensics	**UNIT-1**	**8**

DD/MM/YY	Computer Forensic Flaws		
DD/MM/YY	Computer Forensic Risks		
DD/MM/YY	Rules of Computer Forensics		
DD/MM/YY	Legal issues		
DD/MM/YY	Digital Forensic Principles		
DD/MM/YY	Digital Environments		
DD/MM/YY	Digital Forensic Methodologies		
DD/MM/YY	Live forensics and investigation	**UNIT-2**	**10**
DD/MM/YY	Digital evidence		
DD/MM/YY	Seizure methodology		
DD/MM/YY	Factors limiting wholesale seizure of hardware		
DD/MM/YY	Demystifying computer/cyber crime		
DD/MM/YY	Explosion of networking		
DD/MM/YY	Explosion of wireless networks		
DD/MM/YY	Explosion of wireless networks		
DD/MM/YY	Interpersonal communication		
DD/MM/YY	Network-based cybercrime evolution, Wireless communication impact on cybercrime		
DD/MM/YY	Recovering deleted files	**UNIT-3**	**9**
DD/MM/YY	Recovering deleted partitions		
DD/MM/YY	Deleted file recovery tools		
DD/MM/YY	Deleted partition recovery tools		
DD/MM/YY	Data acquisition		
DD/MM/YY	Data duplication		
DD/MM/YY	Data acquisition tools		
DD/MM/YY	Hardware tools		
DD/MM/YY	Backing up data, Duplicating data		
DD/MM/YY	Overview of Routers	**UNIT-4**	**9**
DD/MM/YY	Hacking Routers		

DD/MM/YY	Investigating Routers		
DD/MM/YY	Investigating Wireless Attacks		
DD/MM/YY	Basics of Wireless		
DD/MM/YY	Wireless Penetration Testing		
DD/MM/YY	Direct Connections to Wireless Access Point		
DD/MM/YY	Wireless Connection		
DD/MM/YY	Wireless Connection to a Wireless Access Point		
DD/MM/YY	Forensics Acquisition	**UNIT-5**	**9**
DD/MM/YY	Processing Local Mail Archives		
DD/MM/YY	Processing Server-Level Archives		
DD/MM/YY	Classification of Steganography		
DD/MM/YY	Categories of Steganography in Forensics		
DD/MM/YY	Types of Password Cracking		
DD/MM/YY	Email Evidence Collection		
DD/MM/YY	Email Forensic Analysis		
DD/MM/YY	Steganography Detection Techniques, Password Recovery Methods in Forensics		

7. Lab Session Plan — List of Experiments (Updated CO7–CO10)

W1–W12: All experiments develop CO7 skills (professional implementation, tool usage, documentation). W13–W15 (teal rows): CO8 (design/real-world), CO9 (ethics/reflection), CO10 (teamwork/presentation). Theory knowledge is applied but NOT re-evaluated in lab.

Week	Session	Experiment	Lab CO	Marks
W1	S-1	Learn to install wine / virtual box or any other equivalent software on the host os	**CO7**	3.0

W2	S-2	Perform an experiment to grab a banner with telnet and perform the task using netcat utility	**CO7**	3.0
W3	S-3	Perform an experiment for port scanning with nmap, superscan or any other software.	**CO7**	3.0
W4	S-4	Using nmap1)find open ports on a system 2) find the machines which are active	**CO7**	3.0
W5	S-5	Using nmap 1)find the version of remote os on other systems 2)find the version of s/w installed on other system	**CO7**	3.0
W6	S-6	Perform an experiment on active and passive finger printing using xprobe2 and nmap.	**CO7**	3.0
W7	S-7	Performa an experiment to demonstrate how to sniff for router traffic by using the tool wireshark	**CO7**	3.0
W8	S-8	Perform an experiment how to use dumpsec	**CO8/CO9**	3.0
W9	S-9	Perform an wireless audit of an access point / router and decrypt wep and wpa.	**CO8/CO10**	3.0

W10	S-10	Perform an experiment to sniff traffic using arp poisoning.	**CO9/CO10**	3.0
W11	S-11	Install ipcop on a linux system and learn all the function available on the software	**CO7**	3.0
W12	S-12	Install jcrypt tool (or any other equivalent) and demonstrate asymmetric crypto algorithm.	**CO7**	3.0
W13	S-13	Install jcrypt tool (or any other equivalent) and demonstrate symmetric crypto algorithm.	**CO8**	3.0
W14	S-14	Install jcrypt tool (or any other equivalent) and demonstrate hash	**CO8/CO9**	3.0
W15	S-15	Install jcrypt tool (or any other equivalent) and demonstrate digital/pki signatures	**CO8/CO9**	3.0

Instructions: Write C programs, compile, execute and test with suitable test cases. Lab record (aim, algorithm, code, output, result) must be submitted before the next session.

PART II
THEORY ASSESSMENT FRAMEWORK
Theory Skill Dimensions, MTE & ETE Structure for Theory COs (CO1–CO6)

8. Theory Skill Dimensions (TS1–TS6) — CO1 through CO6

THEORY COs (CO1–CO6) — Assessed exclusively via MTE and ETE only

Six theory skill dimensions — one per Bloom's level L1–L6 — correspond directly to CO1–CO6. They define the competency measured in each section of MTE and ETE, providing a clear NBA-auditable assessment rationale.

ID	Dimension	What is Measured	CO / BTL	Assessment
TS1	**Digital Forensics Fundamentals & Evidence Recognition**	Recall digital forensics terminology, legal principles, forensic methodologies, evidence types, networking basics, steganography concepts, and password cracking terminology	CO1 | L1–L2	MTE Sec A | ETE Sec A
TS2	**Forensic Investigation Process & Conceptual Interpretation**	Explain forensic investigation procedures, legal considerations, evidence acquisition methods, wireless/network attacks, and interpret digital forensic workflows logically	CO2 | L2	MTE Sec A | ETE Sec A
TS3	**Digital Evidence Acquisition & Forensic Tool Application**	Apply forensic tools and techniques for deleted file recovery, partition recovery, data acquisition, wireless penetration testing, and email investigation	CO3 | L3	MTE Sec B | ETE Sec B
TS4	**Cyber Incident Analysis & Forensic Reasoning**	Analyze digital evidence, trace cyber incidents, assess router/network attack scenarios, evaluate correctness of forensic findings, and explain investigative outcomes	CO4 | L4	MTE Sec B | ETE Sec B
TS5	**Comparative Evaluation of Forensic Techniques & Evidence Validation**	Compare forensic tools and methodologies, evaluate efficiency and reliability of investigative approaches, assess legal/technical evidence, and justify conclusions with evidence	CO5 | L5	ETE Sec B/C
TS6	**Design of Complete Forensic Investigation Procedures, Professional Reporting & Legal-Ethical Integration**	Design complete forensic investigation procedures, prepare professional forensic reports, present findings for technical and non-technical audiences, and integrate tools with legal/ethical practices	CO6 | L6	ETE Sec C

9. Theory Assessment Structure — MTE and ETE

9.1 Mid Term Examination (MTE) — 10 Marks (CO1–CO4 only)

Section	Marks	Skill Dimensions	COs	Question Type
Sec A	**4**	TS1 — Digital Forensics Fundamentals & Evidence Recognition TS2 — Forensic Investigation Process & Conceptual Interpretation	**CO1, CO2**	Short-answer: definitions.
Sec B	**6**	TS3 — Digital Evidence Acquisition & Forensic Tool Application TS4 — Cyber Incident Analysis & Forensic Reasoning	**CO3, CO4**	Long and descriptive answers
TOTAL	**10**	TS1–TS4	**CO1–CO4**	Units 1–3 covered; CO5 and CO6 assessed only in ETE

9.2 End Term Examination (ETE) — 100 Marks (Scaled to 50) (CO1–CO6)

Section	Marks	Skill Dimensions	COs	Question Type
Sec A	**25**	TS1 — Digital Forensics Fundamentals & Evidence Recognition TS2 — Forensic Investigation Process & Conceptual Interpretation	**CO1, CO2**	Short questions: definitions.
Sec B	**50**	TS3 — Digital Evidence Acquisition & Forensic Tool Application	**CO3, CO4, CO5**	Medium questions: Comparison, Tools and Techniques

		TS4 — Cyber Incident Analysis & Forensic Reasoning TS5 — Comparative Evaluation of Forensic Techniques & Evidence Validation		
Sec C	**25**	TS5 — Comparative Evaluation of Forensic Techniques & Evidence Validation TS6 — Design of Complete Forensic Investigation Procedures	**CO5, CO6**	Long/design questions: Applications, working principles/
TOTAL	**100**	TS1–TS6 (all)	**CO1–CO6**	Scaled to 50 marks. Minimum 20/50 required to pass.

PART III

LABORATORY ASSESSMENT FRAMEWORK

Evaluation Scheme, CA Rubric, Mini Project Rubric, Skill Dimensions for Lab COs (CO7–CO10)

10. Evaluation Scheme — Overview

Component	Weightage	Marks	COs Assessed
Laboratory Assessment	40%	**40**	Lab COs only: CA experiments
Mid Semester Examination (MTE)	10%	**10**	Theory COs only: CO1, CO2, CO3, CO4
End Semester Examination (ETE)	50%	**50**	Theory COs only: CO1, CO2, CO3, CO4, CO5, CO6
TOTAL	**100%**	**100**	Strict separation — no cross-assessment

11. Laboratory Assessment (40 Marks)

 LAB COs (CO7–CO10) — Assessed exclusively via Laboratory Assessment only (CA)

11.1 Component Breakdown

Sub-Component	Quantum	Marks	Remarks
Lab Experiments (CA)	Best 10 of 12	**30**	3.0 marks each — assesses CO7, CO8, CO9
Mini Project/Case Study	1 Project	**10**	Design, implementation, demo & reflection — all 4 Lab COs (CO7–CO10)
TOTAL	—	**40**	

11.2 Per-Experiment CA Rubric (3.0 Marks each — Assesses CO7, CO8, CO9)

Criterion	Marks	CA Skill Dimensions Covered	Marking Guide	Lab CO
Problem Definition & Experimental Design	**1.0**	CA1 — Problem identification, forensic objective, scope definition CA2 — Investigation planning, tool/environment selection CA7 — Methodology, workflow, attack/defense analysis plan	1.0: Well-defined with design | 0.5: Partial | 0: Missing	CO7, CO8
Code Execution & Computational Efficiency	**1.0**	CA3 — Correct execution of scanning/sniffing/auditing/crypto tasks CA4 — Efficient and optimized use of tools/scripts	1.0: Correct & efficient | 0.5: Correct, not optimized | 0: Fails	CO7
Output Analysis, Outcome & Lab Documentation	**0.75**	CA5 — Packet/log/result analysis and interpretation CA6 — Evidence validation, screenshots, observations and conclusion documentation	0.75: Thorough | 0.5: Adequate | 0.25: Partial | 0: Absent	CO8, CO9
Professional Attitude & Ethical Conduct	**0.25**	CA6 — Structured report, screenshots, references, conclusion CA8 — Viva-voce understanding and communication	0.25: Consistent | 0.10: Occasional | 0: Absent	CO9

		PO7/CO9 — Ethical and responsible cybersecurity practices		
Total	**3.0**	All 8 CA skill dimensions covered		

11.3 Best-10-of-N Scoring Scheme

Conducted	Best N Counted	Max Score	Note
> (10 + x)	Best 10	**30 Marks**	x worst dropped
10	All 10	**30 Marks**	No drop
< 10	All	**≤ 30 Marks**	Deficit = zero

11.4 Mini Project Evaluation Rubric (10 Marks — All 4 Lab COs)

Criterion	Marks	Project Skill Dimensions	Marking Guide	Lab CO / PO
SDG Alignment & Problem Scoping	**1.5**	P1 — SDG mapping; societal relevance P2 — Problem scope and stakeholder requirements P4 — Innovative solution proposal with alternatives	1.5: Comprehensive | 1.0: Adequate | 0.5: Partial | 0: Absent	CO8 / PO3, PO6
Project Planning & Financial Awareness	**1.5**	P2 — Timeline, milestones, resource planning P11 — Financial feasibility and cost estimation	1.5: Detailed | 1.0: Adequate | 0.5: Basic | 0: Absent	CO10 / PO10
End-to-End Implementation & System Operation	**2.0**	P5 — Professional toolchain selection P6 — Complete project build and integration P7 — System commissioning and operational testing	2: Fully operational | 1–1.5: Partial | 0–0.5: Non-functional	CO7, CO8 / PO3, PO5
Impact Assessment & Critical Reporting	**2.0**	P8 — Measurable outcome vs stated goals P9 — Statistical/comparative analysis; technical report	2: Rigorous | 1.5: Good | 1: Basic | 0: Absent	CO8, CO10 / PO6

Communication, Presentation & Teamwork	**2.0**	P3 — Communication plan and testing strategy P10 — Professional presentation quality and delivery	2: Excellent | 1.5: Good | 1: Adequate | 0: Poor	CO10 / PO8, PO9
Skill Reflection, Ethics & Professional Attitudes	**1.0**	P12 — Skill growth mapping (pre/post project) P13 — Professional attitudes and ethical conduct	1.0: Reflective & honest | 0.5: Partial | 0: Absent	CO9 / PO7, PO11
Total	**10**	All 13 Project skill dimensions; all 4 Lab COs (CO7–CO10)		

12. CA Skill Dimensions (8 Dimensions — Lab COs only)

ID	Dimension	What is Measured	Lab CO Anchor
CA1	**Problem Definition & Metrics**	Define forensic/security problem; identify measurable attributes, attack indicators, objectives, scope, and success criteria	CO7, CO8
CA2	**Experimental Design & Tool Setup**	Plan experiment/investigation; configure tools and environments such as VirtualBox, Wine, Nmap, Wireshark, IPCop, cryptographic utilities, Linux CLI, and network settings	CO7
CA3	**Code Implementation & Execution**	Correctly execute scanning, sniffing, auditing, fingerprinting, firewall, and cryptographic experiments to obtain expected outputs	CO7
CA4	**Computational Efficiency & Optimization**	Analyze efficiency of scans/captures/configurations; identify bottlenecks, security gaps, and optimization techniques	CO7
CA5	**Output Analysis & Result Interpretation**	Analyze captured packets, logs, scans, fingerprints, and cryptographic outputs; explain findings and derive evidence-based conclusions	CO8
CA6	**Documented Outcome with Verification**	Record experiment results formally with screenshots/logs/output verification and validate against objectives	CO7, CO8
CA7	**Algorithmic Design & Solution Planning**	Design investigation workflow/steps; prepare procedures, attack-defense methodology, flowcharts, or security audit plans before execution	CO7, CO8

CA8	**Lab Record Maintenance & Viva-Voce**	Maintain complete lab records, observations, ethical practices, and demonstrate conceptual understanding during viva	CO7, CO9

13. Project Skill Dimensions (13 Dimensions — Lab COs only)

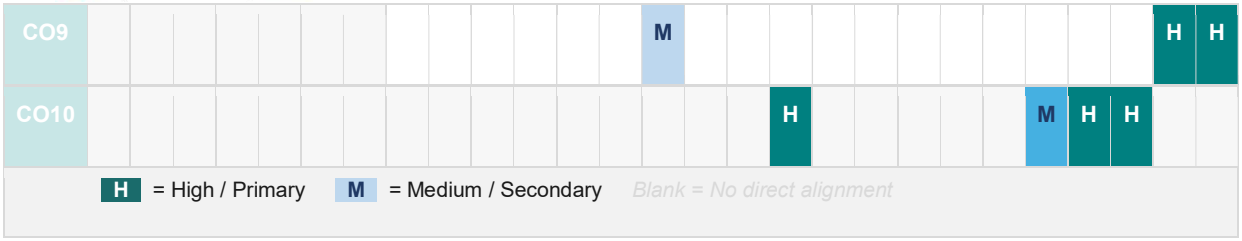
ID	Dimension	What is Measured	Lab CO / PO Anchor
P1	**SDG Alignment & Social Relevance**	Map project to relevant SDGs; articulate societal value and intended impact	CO8 | PO6
P2	**Problem Scoping & Requirements**	Define boundaries; produce formal problem statement with measurable goals	CO8 | PO2
P3	**Communication & Testing Strategy**	Develop communication plan; design testing strategy; coordinate group activities	CO10 | PO9
P4	**Innovative Solution Proposal**	Propose solution with alternatives; justify selection using design criteria	CO8 | PO3
P5	**Professional Toolchain**	Select and justify development tools; configure professional project environment	CO7 | PO5
P6	**End-to-End Implementation**	Build complete integrated solution incorporating at least 3 syllabus topics	CO7, CO8 | PO3
P7	**System Commissioning & Testing**	Deploy and operate system; conduct edge-case and stress tests	CO7, CO8 | PO5
P8	**Measurable Impact & Outcome**	Evaluate actual outcomes against goals; quantify impact using defined metrics	CO8 | PO6
P9	**Critical Analysis & Reporting**	Perform comparative/statistical analysis; produce structured technical report	CO8, CO10 | PO2, PO4
P10	**Professional Presentation & Teamwork**	Deliver professional presentation; evidence team collaboration and role differentiation	CO10 | PO8, PO9
P11	**Financial Feasibility & Planning**	Estimate project cost; justify resource allocation; discuss cost-effectiveness	CO10 | PO10
P12	**Individual Skill Growth Mapping**	Document pre/post skill gaps; map personal contributions to project dimensions	CO9 | PO11

P13	**Professional Attitude, Ethics & Responsibility**	Demonstrate integrity, ethical conduct, and responsible use of tools/data throughout	CO9 | PO7

14. CO × Skill Dimensions Mapping (10 COs × [6 Theory+ 8 CA + 13 Project Dimensions])

- *Theory COs (CO1–CO6) are fully mapped. Lab COs (CO7–CO10) intentionally have no TS mapping — confirming strict assessment separation.*
- *Theory COs (CO1–CO6) have NO CA alignment — confirms they are NOT evaluated in lab. All CA alignments confined to Lab COs (CO7–CO10).*
- *Theory COs (CO1–CO6) have NO project alignment — confirms strict lab-only assessment. All 13 Project dimensions anchored exclusively to Lab COs (CO7–CO10).*

CO	Theory Skill Dimensions						CA Skill Dimensions								Project Skill Dimensions												
	TS1 Factual Recall	TS2 Conceptual Expl.	TS3 Procedural App.	TS4 Analytical Rsng	TS5 Compar. Eval.	TS6 Synthesis & Design	CA1 :Prob.Def.	CA2 Exp.Setup	CA3 Execution	CA4 Efficiency	CA5 Output Anal.	CA6 Doc.Outcome	CA7 Algo.Design	CA8 Lab Rec./Viva	P1 SDG	P2 Scoping	P3 Comm.	P4 Solution	P5 Tools	P6 Impl.	P7 Sys.Op.	P8 Impact	P9 Analysis	P10 Present.	P11 Financial	P12 Skill Map	P13 Attitude
CO1	H	M																									
CO2	M	H	M																								
CO3		M	H	M																							
CO4			M	H	M																						
CO5				M	H	M																					
CO6			M		M	H																					
CO7							H	H	H	M		M	M	H					H	M	H						
CO8							M		M		H	H	H		H	H		H	M	H	M	H	M				



PART IV

COMBINED MAPPINGS & REFERENCE

CO–PO Matrix, SDG Mapping, Bloom's Taxonomy Reference, Attendance & Pass/Fail

15. CO–PO and CO–PSO Mapping Matrix (All 10 COs)

Strength Scale: 3 = Substantial (High) | 2 = Moderate | 1 = Slight (Low) | – = Not Applicable. Column averages computed over non-zero entries only.

CO/PO	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PSO1	PSO2	PSO3
CO1	3	2	-	2	2	2	3	1	1	1	2	3	2	2
CO2	3	3	2	2	3	-	2	2	-	1	2	3	3	2
CO3	2	3	3	3	3	-	2	-	-	1	2	3	3	3
CO4	3	2	2	3	3	-	2	-	1	-	2	3	3	2
CO5	2	3	-	2	2	2	2	-	1	2	3	2	3	2
CO6	2	2	-	-	-	1	-	-	3	2	2	2	2	2
CO7	–	–	1	–	3	1	–	–	–	–	–	2	3	3
CO8	–	1	3	1	2	3	–	–	–	–	–	2	3	3
CO9	–	–	–	–	–	–	3	–	–	–	3	–	1	2
CO10	–	–	–	–	–	1	–	3	3	3	2	2	2	2

Avg	2.50	2.29	2.20	2.17	2.57	1.67	2.33	2.00	1.80	1.67	2.25	2.44	2.50	2.30

PO7 (Ethics) now receives mapping from CO9 (strength 3). PO11 (Life-Long Learning) is addressed by both Theory COs and CO9. Lab COs (CO7–CO10) extend coverage to POs 3, 5, 6, 7, 8, 9, 10, 11.

16. CO × PO Alignment Map (H/M Indicators — All 10 COs × 11 POs)

CO	PO1 Eng.Know.	PO2 Prob.Analysis	PO3 Design	PO4 Investigation	PO5 Tool Usage	PO6 Engineer & World	PO7 Ethics	PO8 Teamwork	PO9 Comm.	PO10 Proj.Mgmt	PO11 Lifelong
CO1	H	M	-	M	M	M	H				M
CO2	H	H	M	M	H	-	M	M	-		M
CO3	M	H	H	H	H	-	M	-	-		M
CO4	H	M	M	H	H	-	M	-		-	M
CO5	M	H	-	M	M	M	M	-		M	H
CO6	M	M	-	-	-		-	-	H	M	M
CO7	–	–		–	H		–	–	–	–	–
CO8	–		H		M	H	–	–	–	–	–
CO9	–	–	–	–	–	–	H	–	–	–	H
CO10	–	–	–	–	–		–	H	H	H	M

H = High / Primary **M** = Medium / Secondary *Blank = No direct alignment*

17. Course-to-SDG Mapping Matrix

SDG Goal	Description	Mapping	Justification
SDG 4	Quality Education	3 (High)	Builds strong foundation in computational thinking and structured programming; aligned with lifelong learning (CO1–CO6, CO9).
SDG 8	Decent Work & Economic Growth	3 (High)	Develops industry-relevant programming and professional tool skills (CO7) directly applicable to employment in technology sectors.
SDG 9	Industry, Innovation & Infrastructure	3 (High)	Enables development of efficient software solutions; fosters innovation through real-world application design (CO6, CO8) and team-based projects (CO10).
SDG 12	Responsible Consumption & Production	2 (Moderate)	Promotes efficient, optimized coding; encourages ethical coding and responsible use of computational resources (CO9, CO7).

18. Bloom's Taxonomy — Domain Level Reference

Cognitive Domain (6 Levels)	Affective Domain (5 Levels)	Psychomotor Domain — Simpson (7 Levels)
L1 — Remember: Recall facts, definitions, basic concepts L2 — Understand: Explain ideas, concepts, principles L3 — Apply: Use knowledge to solve new problems L4 — Analyze: Break down information, examine patterns L5 — Evaluate: Judge, justify, assess, make decisions L6 — Create: Design, develop, produce new solutions	A1 — Receiving: Awareness, willingness to attend A2 — Responding: Active participation and reaction A3 — Valuing: Showing commitment, assigning value A4 — Organizing: Integrating values into personal system A5 — Characterizing: Internalized value system	P1 — Perception: Sensory cues guide motor activity P2 — Set: Mental, physical readiness to act P3 — Guided Response: Basic practice through imitation P4 — Mechanism: Habitual correct performance P5 — Complex Overt Response: Skilled performance P6 — Adaptation: Modify skills for special situations P7 — Origination: Create new solution patterns

OBE Compliance Statement: Theory COs (CO1–CO6) are primarily mapped to the Cognitive domain (L1–L6). Lab COs (CO7–CO10) span all three domains — Cognitive (L2–L6), Psychomotor (P3–P7), and Affective (A2–A5) — reflecting the skill-based nature of laboratory and project assessment.

19. Attendance Policy & Pass/Fail Criteria

19.1 Attendance Policy

Component	Minimum	Applicable To	Consequence
Theory Classes	**70%**	All lecture sessions	Debarred from ETE
Practical / Lab	**70%**	All lab sessions	Debarred from ETE
Combined (Theory + Lab)	**75%**	Combined sessions	Debarred from ETE

Both theory and practical attendance must independently meet 70%. The combined must be 75%. Satisfying one does NOT compensate for a shortfall in the other.

19.2 Pass / Fail Criteria

Condition	Threshold	Status	Remarks
ETE Score (scaled)	**≥ 20 / 50**	**MANDATORY**	40% of ETE; equivalent to ≥ 40/100 on the full paper
Overall Total	**≥ 40 / 100**	**Must pass overall**	Lab 40 + MTE 10 + ETE 50 = 100; 40% overall minimum required

PPS INTEGRATED COURSE PLAN — MEASUREMENT ARCHITECTURE

11 AICTE Programme Outcomes → 10 COs (6 Theory + 4 Lab) → 3 Assessment Instruments → 27 Skill Dimensions (6 TS + 8 CA + 13 Project)

Theory Tier CO1–CO6 (MTE + ETE): PO1, PO2, PO3, PO4, PO9 | 6 Theory Skill Dims (TS1–TS6)

Lab Tier CO7–CO10 (Lab only): PO3, PO5, PO6, PO7, PO8, PO9, PO10, PO11 | 8 CA Dims + 13 Project Dims

Marks: Lab 40 (Experiments 30 @ 3.0 each + Project 10) + MTE 10 + ETE 50 = Total 100

SEMESTER IV

COURSE PLAN

Ethical Hacking (CSCF2301)

School of Computing Science & Engineering (SSCSE) | B.Tech CSE | Semester IV | Batch 2026–2030

Integrated Course Plan — Theory COs (CO1–CO6) + Lab COs (CO7–CO10) | New AICTE 11-PO Framework | Full Skill Mapping

PART I

COURSE SYLLABUS

Course Identification, Details, Outcomes, BTL Mapping & Lecture/Lab Plans

1. Course Identification

School:	SSCSE	**Batch:**	2026–2030
Program:	B.Tech	**Current Academic Year:**	2026–27
Branch:	CSE	**Semester:**	IV

2. Course Details

Integrated theory + laboratory model. 10 COs in two tiers: Theory COs (CO1–CO6) via MTE + ETE; Lab COs (CO7–CO10) via Laboratory Assessment only. No cross-evaluation.

S.No	Attribute	Details
1	**Course Code**	**CSCF2301**
2	**Course Title**	**Ethical Hacking**
3	**Credits**	4
4	**Contact Hours (L-T-P-SL)**	3-0-2-3
5	**Course Status**	Core

6	**Course Objective**	Students will learn advanced ethical hacking concepts through hands-on laboratories and real-world security assessment scenarios, gaining practical skills in reconnaissance, vulnerability assessment, system, network, web, wireless, cloud, and IoT security while adhering to ethical, legal, and professional cybersecurity practices.
7	**Course Outcomes (COs)**	**After successful completion of this course, the student will be able to:** **THEORY COs — Assessed via MTE + ETE:** **CO1 (Remember – L1):** Explain the fundamental concepts of ethical hacking, cybersecurity principles, attack methodologies, security threats, and legal and ethical considerations involved in penetration testing. **CO2 (Understand – L2):** Describe reconnaissance, scanning, enumeration, vulnerability assessment techniques, and various cyberattack concepts used in ethical hacking practices. **CO3 (Apply – L3):** Apply ethical hacking methodologies and security assessment tools to identify vulnerabilities in networks, systems, web applications, wireless environments, and cloud platforms. **CO4 (Analyze – L4):** Analyze cyberattack scenarios, vulnerabilities, malware threats, web security issues, wireless attacks, and defensive mechanisms to evaluate organizational security posture. **CO5 (Evaluate – L5):** Evaluate the effectiveness of cybersecurity controls, vulnerability mitigation strategies, penetration testing approaches, and emerging security trends including cloud, IoT, and AI-based security practices. **CO6 (Create – L6):** Design comprehensive ethical hacking assessment methodologies and prepare professional security reports with recommendations for improving organizational cybersecurity resilience. **LAB COs — Assessed via Laboratory Assessment only:** **CO7 (Apply – L3):** Demonstrate the use of ethical hacking and vulnerability assessment tools to perform reconnaissance, scanning, enumeration, network analysis, and security testing in controlled laboratory environments. **CO8 (Create – L5/L6):** Prepare and present structured penetration testing reports documenting

		vulnerabilities, risk analysis, exploitation findings, and appropriate remediation strategies for technical and non-technical stakeholders. **CO9 (Apply – L2/L3):** Collaborate effectively in cybersecurity assessment activities by applying ethical hacking methodologies, interpreting security findings, and recommending solutions to protect digital assets. **CO10 (Apply – L3):** Demonstrate professional and ethical conduct in cybersecurity practices by ensuring responsible vulnerability disclosure, legal compliance, privacy protection, and adherence to industry standards.
8	**Teaching & Learning**	Classroom Instructions (CI) 45 hrs + Lab Instructions (LI) 30 hrs + Self Learning (SL) 45 hrs = 120 hrs
9	**Mode of Examination**	Lab (40 marks) + MTE (10 marks) + ETE (50 marks) = 100 marks. Theory COs: MTE + ETE only. Lab COs: Lab only.
10	**Self Learning (SL: 45 hrs)**	1. **Explore and practice ethical hacking tools** such as Kali Linux, Nmap, Wireshark, Burp Suite, and vulnerability assessment tools to perform reconnaissance, network analysis, vulnerability identification, and security assessment of controlled lab environments. Prepare a technical report documenting tools, methodologies, findings, and mitigation strategies. 2. **Perform a simulated end-to-end penetration testing exercise** involving information gathering, scanning, enumeration, vulnerability assessment, controlled exploitation, security analysis, and preparation of a professional penetration testing report for a mock organizational security scenario. 3. **Study emerging trends in cybersecurity** including cloud security, IoT and OT security, mobile security, AI-assisted ethical hacking, advanced persistent threats, and modern defense mechanisms. Prepare a technical presentation and summary report analyzing current challenges, attack techniques, and recommended security practices.
11	**References**	5. Christopher Negus, Linux Bible, 11th Edition, Wiley, 2025. 6. James F. Kurose and Keith W. Ross, Computer Networking: A Top-Down Approach, 8th Edition, Pearson, 2021 7. William Panek, CEH Certified Ethical Hacker v13 Study Guide, Wiley Sybex

3. Outline Syllabus — Theory Units with CO Mapping (CO1–CO6)

Unit CO mappings refer to Theory COs (CO1–CO6) only. Lab experiments reinforce these units but are assessed under Lab COs (CO7–CO10).

	Topic / Activity	CO Mapping

Unit 1	**Foundations of Ethical Hacking and Reconnaissance: (8-0-0-6 = 14hrs)**	
A	Introduction to Ethical Hacking, Information Security Fundamentals, Legal and Ethical Issues, Cyber Kill Chain, MITRE ATT&CK Framework	CO1, CO2, CO3
B	Footprinting, Open Source Intelligence (OSINT), Google Hacking, WHOIS, DNS Enumeration	
C	Email Tracking, Network Scanning, Host Discovery, Port Scanning, Service Enumeration	
Tools Used	Nmap, WHOIS, nslookup, the Harvester, Maltego Community Edition	
Activities	**Objective:** • Understand ethical hacking concepts, information security principles, and legal considerations. • Perform footprinting and reconnaissance using passive and active information gathering techniques. • Conduct DNS, WHOIS, and email reconnaissance to gather target information. • Scan hosts and networks to identify live systems, open ports, and running services. • Interpret scan results to identify potential attack surfaces.	
Unit 2	**Enumeration, Vulnerability Assessment, and System Exploitation: (10-0-0-9= 19 hrs)**	
A	Enumeration Techniques, Active Directory Enumeration, SMB, LDAP, SNMP Enumeration,	CO1, CO2,CO3,CO5
B	Vulnerability Assessment, CVE, CVSS, Vulnerability Scanners, Password Cracking,	
C	Privilege Escalation, Malware, Trojans, Ransomware, Covering Tracks	
Tools Used	Nessus Essentials / OpenVAS enum4linux John the Ripper	

	Hashcat Metasploit Framework	
Activities	**Objective:** • Perform enumeration of network services, users, and shared resources. • Conduct vulnerability assessments and interpret vulnerability reports. • Analyze password security using password auditing and cracking tools in a controlled environment. • Demonstrate basic exploitation techniques for educational purposes using penetration testing frameworks. • Understand privilege escalation concepts and post-exploitation methodologies.	
Unit 3	**Network Attacks and Defensive Evasion (9-0-0-10 = 19 hrs)**	
A	Packet Sniffing, ARP Spoofing, Man-in-the-Middle Attacks, Social Engineering, Phishing, Vishing, Smishing,	CO2, CO3, CO4, CO5, CO6
B	Denial-of-Service (DoS/DDoS), Session Hijacking	
C	Firewall Evasion, IDS/IPS Evasion, Honeypots	
Tools Used	Wireshark Ettercap hping3 Snort (IDS)	
Activities	**Objective:** • Capture and analyze network traffic to identify protocols and suspicious activities. • Demonstrate packet sniffing and Man-in-the-Middle (MITM) attacks in a controlled laboratory. • Study common social engineering attack techniques and appropriate defensive measures. • Understand the principles of Denial-of-Service (DoS) attacks and mitigation strategies. • Analyze intrusion detection mechanisms and firewall evasion concepts for defensive learning..	
Unit 4	**Web, Wireless, and Mobile Security (9-0-0-10 = 19 hrs)**	
A	Web Server Security, Web Application Security, OWASP Top 10	CO3, CO4, CO5

B	SQL Injection, Cross-Site Scripting (XSS), CSRF, SSRF	
C	Wireless Security (Wi-Fi, WPA2/WPA3), Bluetooth Security, Mobile Platform Security (Android and iOS)	
Tools Used	Burp Suite Community Edition OWASP ZAP DVWA (Damn Vulnerable Web Application) Android Studio Emulator	
Activities	**Objective:** • Assess web server and web application security using ethical testing techniques. • Identify common web vulnerabilities, including those listed in the OWASP Top 10. • Demonstrate SQL Injection and Cross-Site Scripting (XSS) attacks in a safe laboratory environment. • Analyze wireless network security mechanisms and authentication protocols. • Explore fundamental mobile application security concepts and common mobile threats.	
Unit 5	**Emerging Technologies and Cryptography (9-0-0-10 = 19 hrs)**	
A	IoT Security, Operational Technology (OT), SCADA Security, Cloud Computing Security, Cloud Threats	CO2, CO3, CO4, CO5, CO6
B	Virtualization, Encryption, Hashing, PKI, Digital Signatures, TLS/SSL	
C	AI-Assisted Ethical Hacking Concepts	
Tools Used	OpenSSL VeraCrypt	
Activities	**Objective:** • Understand security challenges in IoT, Operational Technology (OT), and cloud computing environments. • Analyze common threats and mitigation strategies for cloud-based systems.	

- Demonstrate the use of cryptographic techniques for confidentiality, integrity, and authentication.
- Perform basic encryption, decryption, hashing, and digital certificate operations using cryptographic tools.
- Examine the role of cryptography in securing modern communication systems and emerging technologies.

4. Topic-wise Bloom's Taxonomy Level Mapping (Theory)

S.No	Topic	L1	L2	L3	L4	L5	L6
1	1.A	□	□				
2	1.B		□	□			
3	1.C		□	□			
4	2.A			□			
5	2.B			□			
6	2.C			□	□		
7	3.A			□	□		□
8	3.B		□	□		□	
9	3.C			□	□		
10	4.A			□	□		
11	4.B			□	□	□	
12	4.C			□			
13	5.A		□	□		□	□
14	5.B			□	□		□
15	5.C			□	□	□	□

5. CO vs Bloom's Taxonomy — All Three Domains (Updated for 10 COs)

□ *Only strong/dominant alignments are mapped. Lab COs (CO7–CO10) extend into Psychomotor and Affective domains, reflecting the skill-based nature of lab and project work.*

CO	Cognitive Domain (L1–L6)						Affective (A1–A5)					Psychomotor (P1–P7)						
CO	L1	L2	L3	L4	L5	L6	A1	A2	A3	A4	A5	P1	P2	P3	P4	P5	P6	P7
CO1	□																	
CO2		□																
CO3			□											□				
CO4				□											□			
CO5					□											□		
CO6						□			□							□	□	
CO7			□					□						□	□			
CO8					□	□			□						□	□	□	
CO9			□							□	□							
CO10			□					□			□			□				

Legend: □ = Strong / Dominant mapping only. Theory COs: primarily Cognitive. Lab COs: span all three domains.

6. Lecture Plan Outline (Theory — 45 Lectures)

Date	Topics to be Covered/Title	UNIT	Total Lectures
DD/MM/YY	Introduction to Ethical Hacking, Information Security Concepts, CIA Triad	UNIT-1	9
DD/MM/YY	Hacker Types, Cyber Threat Landscape, Security Controls, Ethical and Legal Issues		

DD/MM/YY	Cyber Kill Chain, MITRE ATT&CK Framework, Penetration Testing Methodology		
DD/MM/YY	Footprinting Concepts and Passive Information Gathering (OSINT)		
DD/MM/YY	WHOIS, DNS Enumeration, Search Engine Reconnaissance, Email Tracking		
DD/MM/YY	Social Media Intelligence, Metadata Analysis, Maltego Basics		
DD/MM/YY	Network Scanning Fundamentals, Host Discovery Techniques		
DD/MM/YY	Port Scanning, Service Enumeration, Banner Grabbing, Firewall Detection		
DD/MM/YY	Banner Grabbing, Firewall Detection		
DD/MM/YY	Enumeration Concepts, SMB, NetBIOS, SNMP, LDAP Enumeration	UNIT-2	9
DD/MM/YY	Active Directory Enumeration and User Enumeration		
DD/MM/YY	Vulnerability Assessment Process, CVE, CVSS, Risk Assessment		
DD/MM/YY	Vulnerability Assessment Tools (Nessus/OpenVAS)		
DD/MM/YY	Password Security, Authentication Mechanisms, Password Cracking Concepts		
DD/MM/YY	Privilege Escalation Concepts and Countermeasures		
DD/MM/YY	Malware Types: Viruses, Worms, Trojans, Ransomware		
DD/MM/YY	Post-Exploitation Concepts and Covering Tracks		
DD/MM/YY	Enumeration and Vulnerability Assessment Lab Demonstration		
DD/MM/YY	Packet Sniffing Fundamentals and Network Protocol Analysis	UNIT-3	9
DD/MM/YY	Wireshark Packet Capture and Traffic Analysis		
DD/MM/YY	ARP Spoofing and Man-in-the-Middle Attack Concepts		
DD/MM/YY	Social Engineering: Phishing, Vishing, Smishing, Human Factors		
DD/MM/YY	Denial-of-Service (DoS) and Distributed DoS Concepts		
DD/MM/YY	Session Hijacking and Session Management Security		

DD/MM/YY	Intrusion Detection Systems (IDS), IPS, and Honeypots		
DD/MM/YY	Firewall Technologies		
DD/MM/YY	IDS/Firewall Evasion Concepts		
DD/MM/YY	Web Server Architecture and Common Security Issues	UNIT-4	9
DD/MM/YY	Web Application Security Fundamentals and OWASP Top 10		
DD/MM/YY	Authentication, Authorization, and Session Management Vulnerabilities		
DD/MM/YY	SQL Injection: Types, Detection, and Prevention		
DD/MM/YY	Cross-Site Scripting (XSS), CSRF, and File Upload Vulnerabilities		
DD/MM/YY	Burp Suite and OWASP ZAP Demonstration		
DD/MM/YY	Wireless Network Security: Wi-Fi, WPA2/WPA3, Bluetooth		
DD/MM/YY	Mobile Platform Security: Android, iOS, and Mobile Threats		
DD/MM/YY	Web Security Assessment Lab and Discussion		
DD/MM/YY	IoT Security Fundamentals and Common IoT Vulnerabilities	UNIT-5	9
DD/MM/YY	Operational Technology (OT), ICS, and SCADA Security		
DD/MM/YY	Cloud Computing Architecture, Service Models, and Security Challenges		
DD/MM/YY	Cloud Threats, Identity Management, and Shared Responsibility Model		
DD/MM/YY	Cryptography Fundamentals: Symmetric and Asymmetric Encryption		
DD/MM/YY	Hash Functions, Message Authentication Codes, and Digital Signatures		
DD/MM/YY	Public Key Infrastructure (PKI), Certificates, and TLS/SSL		
DD/MM/YY	Cryptographic Tools and Secure Communication		
DD/MM/YY	Artificial Intelligence in Ethical Hacking		

7. Lab Session Plan — List of Experiments (Updated CO7–CO10)

W1–W12: All experiments develop CO7 skills (professional implementation, tool usage, documentation). W13–W15 (teal rows): CO8 (design/real-world), CO9 (ethics/reflection), CO10 (teamwork/presentation). Theory knowledge is applied but NOT re-evaluated in lab.

Week	Session	Experiment	Lab CO	Marks
W1	S-1	Install and configure a virtual ethical hacking laboratory using VMware/Virtual Box and Kali Linux.	**CO7**	3.0
W2	S-2	Perform footprinting and reconnaissance using WHOIS, nslookup, theHarvester, and Maltego to gather publicly available information about a target domain.	**CO7**	3.0
W3	S-3	Conduct network discovery and port scanning using Nmap, and analyze the results to identify active hosts and services.	**CO7**	3.0
W4	S-4	Perform network and service enumeration using tools such as enum4linux and SMB enumeration techniques in a controlled environment.	**CO7**	3.0
W5	S-5	Conduct a vulnerability assessment of a laboratory system using Nessus Essentials or OpenVAS and prepare a vulnerability report with remediation recommendations.	**CO7**	3.0

W6	S-6	Perform an experiment on active and passive finger printing using xprobe2 and nmap.	**CO7**	3.0
W7	S-7	Demonstrate password auditing by evaluating password strength and recovering sample password hashes using John the Ripper or Hashcat in a controlled environment.	**CO7**	3.0
W8	S-8	Demonstrate ARP spoofing and analyze Man-in-the-Middle (MITM) attacks in an isolated laboratory network, followed by implementing defensive measures.	**CO8/CO9**	3.0
W9	S-9	Simulate phishing awareness scenarios and analyze common social engineering techniques while discussing preventive security controls.	**CO8/CO10**	3.0
W10	S-10	Assess a deliberately vulnerable web application (DVWA) using Burp Suite Community Edition or OWASP ZAP to identify common web application vulnerabilities	**CO9/CO10**	3.0
W11	S-11	Demonstrate SQL Injection on a vulnerable web application and implement parameterized queries and input validation as countermeasures.	**CO7**	3.0

W12	S-12	Identify and analyze Cross-Site Scripting (XSS) vulnerabilities in a test application and apply secure coding practices to mitigate them	**CO7**	3.0
W13	S-13	Analyze wireless network security by studying Wi-Fi authentication mechanisms, encryption protocols (WPA2/WPA3), and wireless security best practices.	**CO8**	3.0
W14	S-14	Explore cloud security by configuring identity and access controls in a cloud laboratory environment and evaluating common cloud security risks	**CO8/CO9**	3.0
W15	S-15	Perform cryptographic operations using OpenSSL, including key generation, encryption/decryption, hashing, digital signatures, and certificate verification.	**CO8/CO9**	3.0

PART II

THEORY ASSESSMENT FRAMEWORK

Theory Skill Dimensions, MTE & ETE Structure for Theory COs (CO1–CO6)

8. Theory Skill Dimensions (TS1–TS6) — CO1 through CO6

THEORY COs (CO1–CO6) — Assessed exclusively via MTE and ETE only

Six theory skill dimensions — one per Bloom's level L1–L6 — correspond directly to CO1–CO6. They define the competency measured in each section of MTE and ETE, providing a clear NBA-auditable assessment rationale.

ID	Dimension	What is Measured	CO / BTL	Assessment
TS1	**Ethical Hacking Fundamentals & Cybersecurity Concepts**	Recall ethical hacking terminology, cybersecurity principles, security controls, hacker classifications, cyber laws, penetration testing methodology, reconnaissance concepts, and networking fundamentals.	CO1 | L1–L2	MTE Sec A | ETE Sec A
TS2	**Reconnaissance, Scanning & Vulnerability Assessment**	Explain footprinting, OSINT techniques, network scanning, enumeration methods, vulnerability assessment processes, CVE/CVSS concepts, and interpret scan results.	CO2 | L2	MTE Sec A | ETE Sec A
TS3	**System Exploitation & Network Security Assessment**	Apply ethical hacking tools and techniques to perform password auditing, service enumeration, vulnerability scanning, packet analysis, and controlled security testing in laboratory environments.	CO3 | L3	MTE Sec B | ETE Sec B
TS4	**Web, Wireless & Mobile Security Analysis**	Analyze web application vulnerabilities, SQL Injection, XSS, wireless security mechanisms, mobile platform threats, and recommend appropriate security controls.	CO4 | L4	MTE Sec B | ETE Sec B
TS5	**Cyber Defense, Risk Evaluation & Incident Analysis**	Evaluate network attacks, malware threats, social engineering techniques, IDS/IPS effectiveness, cloud security risks, and justify suitable defensive strategies and mitigation measures.	CO5 | L5	ETE Sec B/C
TS6	**Secure System Design, Cryptography & Professional Ethical Practice**	Design secure solutions using cryptographic techniques, recommend security architectures for cloud and IoT environments, prepare penetration testing reports, and integrate ethical, legal, and professional cybersecurity practices.	CO6 | L6	ETE Sec C

9. Theory Assessment Structure — MTE and ETE

9.1 Mid Term Examination (MTE) — 10 Marks (CO1–CO4 only)

Section	Marks	Skill Dimensions	COs	Question Type
Sec A	**4**	TS1 — Ethical Hacking Fundamentals & Cybersecurity ConceptsTS2 — Reconnaissance, Scanning & Vulnerability Assessment	**CO1, CO2**	Short-answer: definitions.
Sec B	**6**	TS3 — System Exploitation & Network Security AssessmentTS4 — Web, Wireless & Mobile Security Analysis	**CO3, CO4**	Long and descriptive answers
TOTAL	**10**	TS1–TS4	**CO1–CO4**	Units 1–3 covered; CO5 and CO6 assessed only in ETE

9.2 End Term Examination (ETE) — 100 Marks (Scaled to 50) (CO1–CO6)

Section	Marks	Skill Dimensions	COs	Question Type
Sec A	**25**	TS1 — Ethical Hacking Fundamentals & Cybersecurity ConceptsTS2 — Reconnaissance, Scanning & Vulnerability Assessment	**CO1, CO2**	Short questions: definitions.
Sec B	**50**	TS3 — System Exploitation & Network Security AssessmentTS4 — Web, Wireless & Mobile Security Analysis	**CO3, CO4, CO5**	Medium questions: Comparison, Tools and Techniques
Sec C	**25**	TS5 — Cyber Defense, Risk Evaluation & Incident AnalysisTS6 — Secure System Design, Cryptography	**CO5, CO6**	Long/design questions: Applications, working principles/

		& Professional Ethical Practice		
TOTAL	**100**	TS1–TS6 (all)	**CO1–CO6**	Scaled to 50 marks. Minimum 20/50 required to pass.

PART III

LABORATORY ASSESSMENT FRAMEWORK

Evaluation Scheme, CA Rubric, Mini Project Rubric, Skill Dimensions for Lab COs (CO7–CO10)

10. Evaluation Scheme — Overview

Component	Weightage	Marks	COs Assessed
Laboratory Assessment	40%	**40**	Lab COs only: CA experiments
Mid Semester Examination (MTE)	10%	**10**	Theory COs only: CO1, CO2, CO3, CO4
End Semester Examination (ETE)	50%	**50**	Theory COs only: CO1, CO2, CO3, CO4, CO5, CO6
TOTAL	**100%**	**100**	Strict separation — no cross-assessment

11. Laboratory Assessment (40 Marks)

LAB COs (CO7–CO10) — Assessed exclusively via Laboratory Assessment only (CA)

11.1 Component Breakdown

Sub-Component	Quantum	Marks	Remarks
Lab Experiments (CA)	Best 10 of 12	**30**	3.0 marks each — assesses CO7, CO8, CO9
Mini Project/Case Study	1 Project	**10**	Design, implementation, demo & reflection — all 4 Lab COs (CO7–CO10)

TOTAL	—	**40**	

11.2 Per-Experiment CA Rubric (3.0 Marks each — Assesses CO7, CO8, CO9)

Criterion	Marks	CA Skill Dimensions Covered	Marking Guide	Lab CO
Problem Definition & Experimental Design	**1.0**	CA1 — Problem identification, forensic objective, scope definition CA2 — Investigation planning, tool/environment selection CA7 — Methodology, workflow, attack/defense analysis plan	1.0: Well-defined with design | 0.5: Partial | 0: Missing	CO7, CO8
Code Execution & Computational Efficiency	**1.0**	CA3 — Correct execution of scanning/sniffing/auditing/crypto tasks CA4 — Efficient and optimized use of tools/scripts	1.0: Correct & efficient | 0.5: Correct, not optimized | 0: Fails	CO7
Output Analysis, Outcome & Lab Documentation	**0.75**	CA5 — Packet/log/result analysis and interpretation CA6 — Evidence validation, screenshots, observations and conclusion documentation	0.75: Thorough | 0.5: Adequate | 0.25: Partial | 0: Absent	CO8, CO9
Professional Attitude & Ethical Conduct	**0.25**	CA6 — Structured report, screenshots, references, conclusion CA8 — Viva-voce understanding and communication PO7/CO9 — Ethical and responsible cybersecurity practices	0.25: Consistent | 0.10: Occasional | 0: Absent	CO9
Total	**3.0**	All 8 CA skill dimensions covered		

11.3 Best-10-of-N Scoring Scheme

Conducted	Best N Counted	Max Score	Note
> (10 + x)	Best 10	**30 Marks**	x worst dropped
10	All 10	**30 Marks**	No drop
< 10	All	**≤ 30 Marks**	Deficit = zero

11.4 Mini Project Evaluation Rubric (10 Marks — All 4 Lab COs)

Criterion	Marks	Project Skill Dimensions	Marking Guide	Lab CO / PO
SDG Alignment & Problem Scoping	**1.5**	P1 — SDG mapping; societal relevance P2 — Problem scope and stakeholder requirements P4 — Innovative solution proposal with alternatives	1.5: Comprehensive | 1.0: Adequate | 0.5: Partial | 0: Absent	CO8 / PO3, PO6
Project Planning & Financial Awareness	**1.5**	P2 — Timeline, milestones, resource planning P11 — Financial feasibility and cost estimation	1.5: Detailed | 1.0: Adequate | 0.5: Basic | 0: Absent	CO10 / PO10
End-to-End Implementation & System Operation	**2.0**	P5 — Professional toolchain selection P6 — Complete project build and integration P7 — System commissioning and operational testing	2: Fully operational | 1–1.5: Partial | 0–0.5: Non-functional	CO7, CO8 / PO3, PO5
Impact Assessment & Critical Reporting	**2.0**	P8 — Measurable outcome vs stated goals P9 — Statistical/comparative analysis; technical report	2: Rigorous | 1.5: Good | 1: Basic | 0: Absent	CO8, CO10 / PO6
Communication, Presentation & Teamwork	**2.0**	P3 — Communication plan and testing strategy P10 — Professional presentation quality and delivery	2: Excellent | 1.5: Good | 1: Adequate | 0: Poor	CO10 / PO8, PO9
Skill Reflection, Ethics & Professional Attitudes	**1.0**	P12 — Skill growth mapping (pre/post project) P13 — Professional attitudes and ethical conduct	1.0: Reflective & honest | 0.5: Partial | 0: Absent	CO9 / PO7, PO11
Total	**10**	All 13 Project skill dimensions; all 4 Lab COs (CO7–CO10)		

12. CA Skill Dimensions (8 Dimensions — Lab COs only)

ID	Dimension	What is Measured	Lab CO Anchor
CA1	**Problem Definition & Metrics**	Define forensic/security problem; identify measurable attributes, attack indicators, objectives, scope, and success criteria	CO7, CO8
CA2	**Experimental Design & Tool Setup**	Plan experiment/investigation; configure tools and environments such as VirtualBox, Wine, Nmap, Wireshark, IPCop, cryptographic utilities, Linux CLI, and network settings	CO7
CA3	**Code Implementation & Execution**	Correctly execute scanning, sniffing, auditing, fingerprinting, firewall, and cryptographic experiments to obtain expected outputs	CO7
CA4	**Computational Efficiency & Optimization**	Analyze efficiency of scans/captures/configurations; identify bottlenecks, security gaps, and optimization techniques	CO7
CA5	**Output Analysis & Result Interpretation**	Analyze captured packets, logs, scans, fingerprints, and cryptographic outputs; explain findings and derive evidence-based conclusions	CO8
CA6	**Documented Outcome with Verification**	Record experiment results formally with screenshots/logs/output verification and validate against objectives	CO7, CO8
CA7	**Algorithmic Design & Solution Planning**	Design investigation workflow/steps; prepare procedures, attack-defense methodology, flowcharts, or security audit plans before execution	CO7, CO8
CA8	**Lab Record Maintenance & Viva-Voce**	Maintain complete lab records, observations, ethical practices, and demonstrate conceptual understanding during viva	CO7, CO9

13. Project Skill Dimensions (13 Dimensions — Lab COs only)

ID	Dimension	What is Measured	Lab CO / PO Anchor
P1	**SDG Alignment & Social Relevance**	Map project to relevant SDGs; articulate societal value and intended impact	CO8 | PO6
P2	**Problem Scoping & Requirements**	Define boundaries; produce formal problem statement with measurable goals	CO8 | PO2
P3	**Communication & Testing Strategy**	Develop communication plan; design testing strategy; coordinate group activities	CO10 | PO9

P4	**Innovative Solution Proposal**	Propose solution with alternatives; justify selection using design criteria	CO8 | PO3
P5	**Professional Toolchain**	Select and justify development tools; configure professional project environment	CO7 | PO5
P6	**End-to-End Implementation**	Build complete integrated solution incorporating at least 3 syllabus topics	CO7, CO8 | PO3
P7	**System Commissioning & Testing**	Deploy and operate system; conduct edge-case and stress tests	CO7, CO8 | PO5
P8	**Measurable Impact & Outcome**	Evaluate actual outcomes against goals; quantify impact using defined metrics	CO8 | PO6
P9	**Critical Analysis & Reporting**	Perform comparative/statistical analysis; produce structured technical report	CO8, CO10 | PO2, PO4
P10	**Professional Presentation & Teamwork**	Deliver professional presentation; evidence team collaboration and role differentiation	CO10 | PO8, PO9
P11	**Financial Feasibility & Planning**	Estimate project cost; justify resource allocation; discuss cost-effectiveness	CO10 | PO10
P12	**Individual Skill Growth Mapping**	Document pre/post skill gaps; map personal contributions to project dimensions	CO9 | PO11
P13	**Professional Attitude, Ethics & Responsibility**	Demonstrate integrity, ethical conduct, and responsible use of tools/data throughout	CO9 | PO7

14. CO × Skill Dimensions Mapping (10 COs × [6 Theory+ 8 CA + 13 Project Dimensions])

- *Theory COs (CO1–CO6) are fully mapped. Lab COs (CO7–CO10) intentionally have no TS mapping — confirming strict assessment separation.*
- *Theory COs (CO1–CO6) have NO CA alignment — confirms they are NOT evaluated in lab. All CA alignments confined to Lab COs (CO7–CO10).*
- *Theory COs (CO1–CO6) have NO project alignment — confirms strict lab-only assessment. All 13 Project dimensions anchored exclusively to Lab COs (CO7–CO10).*

CO	Theory Skill Dimensions						CA Skill Dimensions								Project Skill Dimensions												
	TS1 Factual Recall	TS2 Conceptual Expl.	TS3 Procedural App.	TS4 Analytical Rsng	TS5 Compar. Eval.	TS6 Synthesis & Design	CA1 :Prob.Def.	CA2 Exp.Setup	CA3 Execution	CA4 Efficiency	CA5 Output Anal.	CA6 Doc.Outcome	CA7 Algo.Design	CA8 Lab Rec./Viva	P1 SDG	P2 Scoping	P3 Comm.	P4 Solution	P5 Tools	P6 Impl.	P7 Sys.Op.	P8 Impact	P9 Analysis	P10 Present.	P11 Financial	P12 Skill Map	P13 Attitude
CO1	H	M																									
CO2	M	H	M																								
CO3		M	H	M																							
CO4			M	H	M																						
CO5				M	H	M																					
CO6			M		M	H																					
CO7							H	H	H	M		M	M	H					H	M	H							
CO8							M		M		H	H	H		H	H		H	M	H	M	H	M					
CO9														M												H	H
CO10																	H						M	H	H		

H = High / Primary M = Medium / Secondary Blank = No direct alignment

PART IV

COMBINED MAPPINGS & REFERENCE

CO–PO Matrix, SDG Mapping, Bloom's Taxonomy Reference, Attendance & Pass/Fail

15. CO–PO and CO–PSO Mapping Matrix (All 10 COs)

Strength Scale: 3 = Substantial (High) | 2 = Moderate | 1 = Slight (Low) | – = Not Applicable. Column averages computed over non-zero entries only.

CO/PO	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PSO1	PSO2	PSO3
CO1	3	2	-	2	2	2	3	1	1	1	2	3	2	2
CO2	3	3	2	2	3	-	2	2	-	1	2	3	3	2
CO3	2	3	3	3	3	-	2	-	-	1	2	3	3	3
CO4	3	2	2	3	3	-	2	-	1	-	2	3	3	2
CO5	2	3	-	2	2	2	2	-	1	2	3	2	3	2
CO6	2	2	-	-	-	1	-	-	3	2	2	2	2	2
CO7	–	–	1	–	3	1	–	–	–	–	–	2	3	3
CO8	–	1	3	1	2	3	–	–	–	–	–	2	3	3
CO9	–	–	–	–	–	–	3	–	–	–	3	–	1	2
CO10	–	–	–	–	–	1	–	3	3	3	2	2	2	2
Avg	2.50	2.29	2.20	2.17	2.57	1.67	2.33	2.00	1.80	1.67	2.25	2.44	2.50	2.30

PO7 (Ethics) now receives mapping from CO9 (strength 3). PO11 (Life-Long Learning) is addressed by both Theory COs and CO9. Lab COs (CO7–CO10) extend coverage to POs 3, 5, 6, 7, 8, 9, 10, 11.

16. CO × PO Alignment Map (H/M Indicators — All 10 COs × 11 POs)

CO	PO1 Eng.Know.	PO2 Prob.Analysis	PO3 Design	PO4 Investigation	PO5 Tool Usage	PO6 Engineer & World	PO7 Ethics	PO8 Teamwork	PO9 Comm.	PO10 Proj.Mgmt	PO11 Lifelong
CO1	H	M	-	M	M	M	H				M
CO2	H	H	M	M	H	-	M	M	-		M
CO3	M	H	H	H	H	-	M	-	-		M
CO4	H	M	M	H	H	-	M	-		-	M
CO5	M	H	-	M	M	M	M	-		M	H
CO6	M	M	-	-	-		-	-	H	M	M
CO7	–	–		–	H		–	–	–	–	–
CO8	–		H		M	H	–	–	–	–	–
CO9	–	–	–	–	–	–	H	–	–	–	H
CO10	–	–	–	–	–		–	H	H	H	M

H = High / Primary **M** = Medium / Secondary *Blank = No direct alignment*

17. Course-to-SDG Mapping Matrix

SDG Goal	Description	Mapping	Justification
SDG 4	**Quality Education**	**3 (High)**	Builds strong foundation in computational thinking and structured programming; aligned with lifelong learning (CO1–CO6, CO9).

SDG 8	Decent Work & Economic Growth	3 (High)	Develops industry-relevant programming and professional tool skills (CO7) directly applicable to employment in technology sectors.
SDG 9	Industry, Innovation & Infrastructure	3 (High)	Enables development of efficient software solutions; fosters innovation through real-world application design (CO6, CO8) and team-based projects (CO10).
SDG 12	Responsible Consumption & Production	2 (Moderate)	Promotes efficient, optimized coding; encourages ethical coding and responsible use of computational resources (CO9, CO7).

18. Bloom's Taxonomy — Domain Level Reference

Cognitive Domain (6 Levels)	Affective Domain (5 Levels)	Psychomotor Domain — Simpson (7 Levels)
L1 — Remember: Recall facts, definitions, basic concepts L2 — Understand: Explain ideas, concepts, principles L3 — Apply: Use knowledge to solve new problems L4 — Analyze: Break down information, examine patterns L5 — Evaluate: Judge, justify, assess, make decisions L6 — Create: Design, develop, produce new solutions	A1 — Receiving: Awareness, willingness to attend A2 — Responding: Active participation and reaction A3 — Valuing: Showing commitment, assigning value A4 — Organizing: Integrating values into personal system A5 — Characterizing: Internalized value system	P1 — Perception: Sensory cues guide motor activity P2 — Set: Mental, physical readiness to act P3 — Guided Response: Basic practice through imitation P4 — Mechanism: Habitual correct performance P5 — Complex Overt Response: Skilled performance P6 — Adaptation: Modify skills for special situations P7 — Origination: Create new solution patterns

OBE Compliance Statement: Theory COs (CO1–CO6) are primarily mapped to the Cognitive domain (L1–L6). Lab COs (CO7–CO10) span all three domains — Cognitive (L2–L6), Psychomotor (P3–P7), and Affective (A2–A5) — reflecting the skill-based nature of laboratory and project assessment.

19. Attendance Policy & Pass/Fail Criteria

19.1 Attendance Policy

Component	Minimum	Applicable To	Consequence
Theory Classes	**70%**	All lecture sessions	Debarred from ETE
Practical / Lab	**70%**	All lab sessions	Debarred from ETE
Combined (Theory + Lab)	**75%**	Combined sessions	Debarred from ETE

Both theory and practical attendance must independently meet 70%. The combined must be 75%. Satisfying one does NOT compensate for a shortfall in the other.

19.2 Pass / Fail Criteria

Condition	Threshold	Status	Remarks
ETE Score (scaled)	**≥ 20 / 50**	**MANDATORY**	40% of ETE; equivalent to ≥ 40/100 on the full paper
Overall Total	**≥ 40 / 100**	**Must pass overall**	Lab 40 + MTE 10 + ETE 50 = 100; 40% overall minimum required

PPS INTEGRATED COURSE PLAN — MEASUREMENT ARCHITECTURE

11 AICTE Programme Outcomes → 10 COs (6 Theory + 4 Lab) → 3 Assessment Instruments → 27 Skill Dimensions (6 TS + 8 CA + 13 Project)

Theory Tier CO1–CO6 (MTE + ETE): PO1, PO2, PO3, PO4, PO9 | 6 Theory Skill Dims (TS1–TS6)

Lab Tier CO7–CO10 (Lab only): PO3, PO5, PO6, PO7, PO8, PO9, PO10, PO11 | 8 CA Dims + 13 Project Dims

Marks: Lab 40 (Experiments 30 @ 3.0 each + Project 10) + MTE 10 + ETE 50 = Total 100

COURSE PLAN

Machine Learning for Cyber Security (CSCF 2302)

School of Computing Science & Engineering (SSCSE) | B.Tech CSE | Semester IV | Batch 2026–2030

Integrated Course Plan — Theory COs (CO1–CO6) + Lab COs (CO7–CO10) | New AICTE 11-PO Framework | Full Skill Mapping

PART I

COURSE SYLLABUS

Course Identification, Details, Outcomes, BTL Mapping & Lecture/Lab Plans

1. Course Identification

School:	SSCSE	**Batch:**	2026–2030
Program:	B.Tech	**Current Academic Year:**	2026–27
Branch:	CSE	**Semester:**	IV

2. Course Details

Integrated theory + laboratory model. 10 COs in two tiers: Theory COs (CO1–CO6) via MTE + ETE; Lab COs (CO7–CO10) via Laboratory Assessment only. No cross-evaluation.

S.No	Attribute	Details
1	**Course Code**	CSCF2302
2	**Course Title**	Machine Learning for Cyber Security / Machine Learning for Cyber Security Lab
3	**Credits**	4
4	**Contact Hours (L-T-P-SL)**	3-0-2-3

5	**Course Status**	Program Elective
6	**Course Objective**	1. To introduce the ideas of learning rule and implement them based on human experience. 2. To conceptualize the working of human brain using SVM, RF and ANN. 3. To become familiar with decision boundaries that can learn from available examples and generalize to form appropriate learning rules for inference systems. To provide the mathematical background for SVM, RF and Neural Network based classification techniques
7	**Course Outcomes (COs)**	**After successful completion of this course, the student will be able to:** **THEORY COs — Assessed via MTE + ETE:** CO1 (Understand – L1/L2): Identify Machine Learning and stochastic concept.. CO2 (Explore – L2/L3): Interpretation of existing models to understand the solution environment. CO3 (Apply – L3): Application of existing mathematical solutions to test problems. CO4 (Analyze – L4/L5): Analyse the logical ability to apply feature engineering to extract hierarchical patterns existing in real life problems. CO5 (Analyze – L4/L5): Build the understanding of learning theory to glance the upcoming world through it. CO6 (Analyze – L2/L4): Appraise recent trends in machine learning and applications **LAB COs — Assessed via Laboratory Assessment only:** CO7 (Apply – L3): Apply ML to detect cyber threats and anomalies. CO8 (Create – L5/L6: Develop and present ML-based cybersecurity solutions. CO9 (Apply – L2/L3): Collaborate to solve cybersecurity problems using ML. CO10 (Apply – L3): Apply ethical and legal practices in ML for cybersecurity.
8	**Teaching & Learning**	Classroom Instructions (CI) 45 hrs + Lab Instructions (LI) 30 hrs + Self Learning (SL) 45 hrs = 120 hrs
9	**Mode of Examination**	Lab (40 marks) + MTE (10 marks) + ETE (50 marks) = 100 marks. Theory COs: MTE + ETE only. Lab COs: Lab only.
10	**Self Learning (SL: 45 hrs)**	1. Explore and implement machine learning models for cyber attack detection usig public cybersecurity datasets. 2. Perform feature engineering, model evaluation, and comparison of ML algorithms for malware or intrusion detection. 3. Develop a mini-project on a cybersecurity application (e.g., phishing detection, malware classification, or network intrusion detection) and prepare a technical report with presentation.

11	**References**	1.Foundations of Machine Learning, Second Edition By MehryarMohri, Afshin Rostamizadeh and Ameet Talwalkar, MIT Press, Second Edition, 2018. 2. Introduction to Machine Learning, Third Edition, By Ethem 3. *Hands-On Machine Learning with Scikit-Learn, Keras, and TensorFlow* — Aurélien Géron — **3rd Edition** 4. *Introduction to Machine Learning with Python* — Andreas C. Müller & Sarah Guido — **1st Edition**

3. Outline Syllabus — Theory Units with CO Mapping (CO1–CO6)

Unit CO mappings refer to Theory COs (CO1–CO6) only. Lab experiments reinforce these units but are assessed under Lab COs (CO7–CO10).

	Topic / Activity	CO Mapping
Unit 1	**Introduction (8-0-0-6 = 14hrs)**	
A	Introduction to Machine Learning, Role of Machine Learning in Cyber Security, The ML Mindset, ML Problem Framing, Common Cyber Security Problems, ML Use Cases in Cyber Security, Identifying Security Problems for ML, Challenges in Cyber Security ML, Applications of ML Standard learning tasks(Machine Learning Pipeline, Classification, Regression, Ranking, Clustering, Dimensionality reduction or Manifold learning)	CO1, CO2, CO3
B	Learning Stages (Security Features, Security Labels, Hyperparameters, Training, Validation and Test Datasets, Loss Function, Model Evaluation), Learning Scenarios (Supervised Learning for Malware and Phishing Detection, Unsupervised Learning for Anomaly and Intrusion Detection, Semi-Supervised Learning for Threat Detection, Online Learning for Real-Time Cyber Defense, Reinforcement Learning for Adaptive Security, Active Learning for Threat Intelligence), Generalization, Supervised Learning, Unsupervised Learning, Reinforcement Learning in Cyber Security.	
C	Cyber Security Data Sources, Security Logs, Network Traffic Data, Malware Datasets, Data Types, Data Preprocessing, Data Cleaning, Missing Values, Noise Removal, Data Integration, Feature Engineering, Feature Selection, Feature Scaling, Normalization, Encoding, PCA, Sampling, Handling Imbalanced Datasets.	
Tools Used	NA	

Activities	**Objective:** • Understand the fundamentals of Machine Learning and its applications in Cyber Security, including learning paradigms and security use cases. • Apply data preprocessing, feature engineering, and dimensionality reduction techniques to prepare cybersecurity datasets for machine learning models. • Analyze cybersecurity problems and select appropriate machine learning approaches for threat detection, classification, and anomaly detection.	
Unit 2	**Supervised Learning Algorithms (10-0-0-9= 19 hrs)**	
A	Regression Models Linear Regression, Cost Function, Gradient Descent, Feature Scaling, Regularization, Ridge Regression, Lasso Regression, Logistic Regression, Logistic Function, Odds and Logit, Decision Boundary, Model Training and Testing.	CO2,CO3,CO4
B	Classification Algorithms Decision Trees, Information Gain, Entropy, Gini Index, Naïve Bayes, Bayesian Classification, K-Nearest Neighbors (KNN), Support Vector Machines (SVM), Linear Discriminant Analysis (LDA), Random Forest.	
C	Model Evaluation and Optimization Confusion Matrix, Accuracy, Precision, Recall, F1-Score, ROC Curve, AUC, Cross Validation, Hyperparameter Tuning, Grid Search, Random Search, Feature Importance, Model Comparison.	
Tools Used	NA	
Activities	Objective: • Understand the principles of regression and classification algorithms used in machine learning. • Apply machine learning models for classification and prediction using appropriate training and testing techniques. • Evaluate and optimize machine learning models using performance metrics, cross-validation, and hyperparameter tuning.	

Unit 3	**Unsupervised Learning Algorithms (9-0-0-10 = 19 hrs)**	
A	Unsupervised Learning Clustering Fundamentals, K-Means Clustering, Hierarchical Clustering, DBSCAN, Density-Based Clustering, Cluster Evaluation, Outlier Detection, Dimensionality Reduction, Principal Component Analysis (PCA)	CO3, CO4, CO5, CO6
B	Neural Networks and Deep Learning Artificial Neural Networks, Perceptron, Activation Functions, Feed Forward Networks, Backpropagation, Deep Neural Networks, Convolutional Neural Networks (CNN), Recurrent Neural Networks (RNN), Long Short-Term Memory (LSTM), Autoencoders.	
C	Deep Learning Fundamentals Network Architecture, Training Deep Models, Batch Processing, Optimizers, Learning Rate Scheduling, Dropout, Batch Normalization, Transfer Learning, Model Evaluation, Hyperparameter Optimization.	
Tools Used	NA	
Activities	**Objective:** • Understand the fundamentals of unsupervised learning, clustering techniques, and dimensionality reduction methods. • Apply neural networks and deep learning models for solving machine learning problems. • Evaluate deep learning models using appropriate training, optimization, and performance evaluation techniques.	
Unit 4	**Advanced Machine Learning Techniques (9-0-0-10 = 19 hrs)**	
A	Ensemble Learning Bagging, Boosting, Random Forest, AdaBoost, Gradient Boosting, XGBoost, Voting Classifiers, Stacking, Ensemble Model Evaluation	CO3, CO4, CO5
B	Explainable and Secure Machine Learning Explainable AI (XAI), Feature Importance, SHAP, LIME, Model Interpretability, Fairness in AI, Bias in Machine Learning, Privacy-Preserving Machine Learning.	
C	Adversarial Machine Learning: Adversarial Examples, Data Poisoning Attacks, Evasion Attacks, Model Extraction Attacks	

Tools Used	NA	
Activities	**Objective:** • Understand ensemble learning techniques and explainable AI concepts for improving machine learning models. • Apply ensemble methods and model interpretation techniques to develop reliable and secure machine learning solutions. • Analyze adversarial attacks and secure machine learning techniques to enhance the robustness of ML models in cybersecurity.	
Unit 5	Machine Learning Frameworks and Emerging Trends (9-0-0-10 = 19 hrs)	
A	Scikit-learn, TensorFlow, Keras, PyTorch	CO2, CO3, CO4, CO5, CO6
B	Generative AI, Large Language Models (LLMs), Federated Learning, Future Trends in AI for Cyber Security	
C	Case studies : Malware Detection, Phishing Detection, Intrusion Detection Systems, Spam Filtering, Network Traffic Analysis, Security Log Analysis, Insider Threat Detection, Threat Intelligence.	
Tools Used	NA	
Activities	**Objective:** • Understand machine learning frameworks and emerging AI technologies used in cyber security. • Apply machine learning frameworks to develop AI-based solutions for cybersecurity problems. • Analyze real-world cybersecurity case studies using machine learning and AI techniques.	

4. Topic-wise Bloom's Taxonomy Level Mapping (Theory)

S.No	Topic	L1	L2	L3	L4	L5	L6
1	1.A	□	□				
2	1.B		□	□			
3	1.C		□	□			
4	2.A			□			
5	2.B			□			
6	2.C			□	□		
7	3.A			□	□		□
8	3.B		□	□		□	
9	3.C			□	□		
10	4.A			□	□		
11	4.B			□	□	□	
12	4.C			□			
13	5.A		□	□		□	□
14	5.B			□	□		
15	5.C			□	□	□	

5. CO vs Bloom's Taxonomy — All Three Domains (Updated for 10 COs)

□ *Only strong/dominant alignments are mapped. Lab COs (CO7–CO10) extend into Psychomotor and Affective domains, reflecting the skill-based nature of lab and project work.*

CO	Cognitive Domain (L1–L6)						Affective (A1–A5)					Psychomotor (P1–P7)						
CO	L1	L2	L3	L4	L5	L6	A1	A2	A3	A4	A5	P1	P2	P3	P4	P5	P6	P7

CO1	□																
CO2		□															
CO3			□										□				
CO4				□										□			
CO5					□										□		
CO6						□			□						□	□	
CO7			□					□					□	□			
CO8					□	□			□					□	□	□	
CO9			□							□	□						
CO10			□					□			□		□				

Legend: □ = Strong / Dominant mapping only. Theory COs: primarily Cognitive. Lab COs: span all three domains.

6. Lecture Plan Outline (Theory — 45 Lectures)

Date	Topics to be Covered	Unit	Total Lectures
DD/MM/YY	Introduction to Machine Learning, Role of Machine Learning in Cyber Security, The ML Mindset, ML Problem Framing, Common Cyber Security Problems, ML)	**UNIT-1**	**8**
DD/MM/YY	Use Cases in Cyber Security, Identifying Security Problems for ML, Challenges in Cyber Security ML,		
DD/MM/YY	Applications of ML Standard learning tasks(Machine Learning Pipeline, Classification, Regression, Ranking, Clustering, Dimensionality reduction or Manifold learning		
DD/MM/YY	Learning Stages (Security Features, Security Labels, Hyperparameters, Training, Validation and Test Datasets, Loss Function, Model Evaluation), Learning Scenarios (Supervised Learning for Malware and Phishing Detection, Unsupervised Learning for Anomaly and Intrusion Detection		
DD/MM/YY	Semi-Supervised Learning for Threat Detection, Online Learning for Real-Time Cyber Defense, Reinforcement Learning for Adaptive Security, Active Learning for Threat Intelligence), Generalization, Supervised Learning, Unsupervised Learning, Reinforcement Learning in Cyber Security.		

DD/MM/YY	Cyber Security Data Sources, Security Logs, Network Traffic Data, Malware Datasets, Data Types, Data Preprocessing, Data Cleaning, Missing Values, Noise Removal,.		
DD/MM/YY	Data Integration, Feature Engineering, Feature Selection, Feature Scaling, Normalization, Encoding,		
DD/MM/YY	PCA, Sampling, Handling Imbalanced Datasets		
DD/MM/YY	Regression Models Linear Regression, Cost Function, Gradient Descent, Feature Scaling, Regularization,	**UNIT-2**	**10**
DD/MM/YY	Ridge Regression, Lasso Regression, Logistic Regression, Logistic Function		
DD/MM/YY	Odds and Logit, Decision Boundary		
DD/MM/YY	Model Training and Testing		
DD/MM/YY	Classification Algorithms Decision Trees, Information Gain, Entropy, Gini Index,.		
DD/MM/YY	Naïve Bayes, Bayesian Classification, K-Nearest Neighbors (KNN), Support Vector Machines (SVM),		
DD/MM/YY	Linear Discriminant Analysis (LDA),		
DD/MM/YY	Random Forest		
DD/MM/YY	Model Evaluation and Optimization Confusion Matrix, Accuracy, Precision, Recall		
DD/MM/YY	F1-Score, ROC Curve, AUC, Cross Validation, Hyperparameter Tuning, Grid Search, Random Search		
DD/MM/YY	Feature Importance, Model Comparison.		
DD/MM/YY	Clustering Fundamentals, K-Means Clustering, Hierarchical Clustering, DBSCAN, Density-Based Clustering, Cluster Evaluation	**UNIT-3**	**9**
DD/MM/YY	Outlier Detection, Dimensionality Reduction, Principal Component Analysis (PCA)		
DD/MM/YY	Artificial Neural Networks, Perceptron, Activation Functions		
DD/MM/YY	Feed Forward Networks, Backpropagation, Deep Neural Networks, Convolutional Neural Networks (CNN),.		
DD/MM/YY	Recurrent Neural Networks (RNN), Long Short-Term Memory (LSTM), Autoencoders		
DD/MM/YY	Network Architecture, Training Deep Models, Batch Processing, Optimizers,.		
DD/MM/YY	Learning Rate Scheduling, Dropout, Batch Normalization		
DD/MM/YY	Transfer Learning, Model Evaluation		
DD/MM/YY	Hyperparameter Optimization		

DD/MM/YY	Bagging, Boosting, Random Forest,	**UNIT-4**	**9**
DD/MM/YY	AdaBoost, Gradient Boosting, XGBoost		
DD/MM/YY	Voting Classifiers, Stacking, Ensemble Model Evaluation		
DD/MM/YY	Explainable AI (XAI), Feature Importance		
DD/MM/YY	SHAP, LIME, Model Interpretability, Fairness in AI, Bias in Machine Learning,		
DD/MM/YY	Privacy-Preserving Machine Learning.		
DD/MM/YY	Adversarial Machine Learning: Adversarial Examples,		
DD/MM/YY	Data Poisoning Attacks, Evasion Attacks, Model Extraction Attacks		
DD/MM/YY	Machine Learning frameworks	**UNIT-5**	**9**
DD/MM/YY	Scikit-learn, TensorFlow,		
DD/MM/YY	Keras, PyTorch		
DD/MM/YY	Generative AI,		
DD/MM/YY	Large Language Models (LLMs),		
DD/MM/YY	Federated Learning,		
DD/MM/YY	Future Trends in AI for Cyber Security		
DD/MM/YY	Case studies : Malware Detection, Phishing Detection		
DD/MM/YY	Intrusion Detection Systems, Spam Filtering, Network Traffic Analysis, Security Log Analysis		
DD/MM/YY	Insider Threat Detection, Threat Intelligence.		

7. Lab Session Plan — List of Experiments (Updated CO7–CO10)

W1–W12: All experiments develop CO7 skills (professional implementation, tool usage, documentation). W13–W15 (teal rows): CO8 (design/real-world), CO9 (ethics/reflection), CO10 (teamwork/presentation). Theory knowledge is applied but NOT re-evaluated in lab.

Week	Session	Experiment	Lab CO	Marks
W1	S-1	Install and configure Python, Jupyter Notebook, Scikit-learn, TensorFlow, and cybersecurity datasets.	**CO7**	3.0

W2	S-2	Load, visualize, and preprocess a cybersecurity dataset (NSL-KDD, CICIDS2017, or Phishing Dataset)	**CO7**	3.0
W3	S-3	Detect phishing websites using Logistic Regression.	**CO7**	3.0
W4	S-4	Classify spam emails using Naïve Bayes.	**CO7**	3.0
W5	S-5	Detect malicious URLs using Decision Tree Classification.	**CO7**	3.0
W6	S-6	Detect network intrusions using K-Nearest Neighbors (KNN).	**CO7**	3.0
W7	S-7	Detect anomalous network traffic using K-Means Clustering	**CO7**	3.0
W8	S-8	Perform anomaly detection using DBSCAN clustering.	**CO8/CO9**	3.0
W9	S-9	Detect brute-force attacks from authentication logs	**CO8/CO10**	3.0

W10	S-10	Implement Principal Component Analysis (PCA) and compare model accuracy before and after PCA.	**CO9/CO10**	3.0
W11	S-11	Perform k-fold cross-validation on a malware detection dataset,	**CO7**	3.0
W12	S-12	Implement ensemble learning using Voting Classifier for cyber attack classification.	**CO7**	3.0
W13	S-13	Build a simple cyber attack prediction model and visualize the prediction results.	**CO8**	3.0
W14	S-14	Develop a basic dashboard to display ML model performance using Python (Accuracy, Precision, Recall, F1-Score).	**CO8/CO9**	3.0
W15	S-15	Mini Project: Develop a simple cyber threat detection system using any ML algorithm.	**CO8/CO9**	3.0

Instructions: Write C programs, compile, execute and test with suitable test cases. Lab record (aim, algorithm, code, output, result) must be submitted before the next session.

PART II
THEORY ASSESSMENT FRAMEWORK

8. Theory Skill Dimensions (TS1–TS6) — CO1 through CO6

THEORY COs (CO1–CO6) — Assessed exclusively via MTE and ETE only

Six theory skill dimensions — one per Bloom's level L1–L6 — correspond directly to CO1–CO6. They define the competency measured in each section of MTE and ETE, providing a clear NBA-auditable assessment rationale.

ID	Dimension	What is Measured	CO / BTL	Assessment
TS1	**Factual Recall & Conceptual Recognition**	Recall machine learning terminology, AI concepts, learning paradigms, cybersecurity datasets, data preprocessing techniques, feature engineering methods, and evaluation metrics.	CO1 | L1–L2	MTE Sec A | ETE Sec A
TS2	**Conceptual Explanation & Logical Interpretation**	Explain supervised, unsupervised, and deep learning algorithms, regression and classification models, clustering techniques, neural networks, and their role in cybersecurity.	CO2 | L2	MTE Sec A | ETE Sec A
TS3	**Procedural Application & Problem Solving**	Apply data preprocessing, feature engineering, machine learning algorithms, model training, testing, and evaluation techniques to solve cybersecurity problems such as malware, phishing, spam, and intrusion detection.	CO3 | L3	MTE Sec B | ETE Sec B
TS4	**Analytical Reasoning & Model Evaluation**	Analyze machine learning model performance using confusion matrix, accuracy, precision, recall, F1-score, ROC-AUC, cross-validation, and compare different algorithms for cybersecurity applications.	CO4 | L4	MTE Sec B | ETE Sec B
TS5	**Comparative Evaluation & Optimization**	Compare machine learning algorithms, optimize models using feature selection, hyperparameter tuning, ensemble learning, and explain model predictions using Explainable AI techniques.	CO5 | L5	ETE Sec B/C
TS6	**Design, Integration & Professional Practice**	Design end-to-end machine learning solutions for cybersecurity, integrate ML frameworks with security datasets, develop intelligent threat detection systems, and demonstrate ethical and responsible AI practices.	CO6 | L6	ETE Sec C

9. Theory Assessment Structure — MTE and ETE

9.1 Mid Term Examination (MTE) — 10 Marks (CO1–CO4 only)

Section	Marks	Skill Dimensions	COs	Question Type
Sec A	**4**	TS1 — Factual Recall TS2 — Conceptual Explanation	**CO1, CO2**	Short-answer: definitions.
Sec B	**6**	TS3 — Procedural Application & Problem Solving TS4 — Analytical Reasoning & Model Evaluation	**CO3, CO4**	Long and descriptive answers
TOTAL	**10**	TS1–TS4	**CO1–CO4**	Units 1–3 covered; CO5 and CO6 assessed only in ETE

9.2 End Term Examination (ETE) — 100 Marks (Scaled to 50) (CO1–CO6)

Section	Marks	Skill Dimensions	COs	Question Type
Sec A	**25**	TS1 — Factual Recall TS2 — Conceptual Explanation	**CO1, CO2**	Short questions: definitions.
Sec B	**50**	TS3 — Procedural Application TS4 — Analytical Reasoning TS5 — Comparative Evaluation	**CO3, CO4, CO5**	Medium questions: Comparison, Tools and Techniques
Sec C	**25**	TS5 — Comparative Evaluation TS6 — Design, Integration & Professional Practice	**CO5, CO6**	Long/design questions: Applications, working principles/

TOTAL	**100**	TS1–TS6 (all)	**CO1–CO6**	Scaled to 50 marks. Minimum 20/50 required to pass.

PART III

LABORATORY ASSESSMENT FRAMEWORK

Evaluation Scheme, CA Rubric, Mini Project Rubric, Skill Dimensions for Lab COs (CO7–CO10)

10. Evaluation Scheme — Overview

Component	Weightage	Marks	COs Assessed
Laboratory Assessment	40%	**40**	Lab COs only: CA experiments
Mid Semester Examination (MTE)	10%	**10**	Theory COs only: CO1, CO2, CO3, CO4
End Semester Examination (ETE)	50%	**50**	Theory COs only: CO1, CO2, CO3, CO4, CO5, CO6
TOTAL	**100%**	**100**	Strict separation — no cross-assessment

11. Laboratory Assessment (40 Marks)

LAB COs (CO7–CO10) — Assessed exclusively via Laboratory Assessment only (CA)

11.1 Component Breakdown

Sub-Component	Quantum	Marks	Remarks
Lab Experiments (CA)	Best 10 of 12	**30**	3.0 marks each — assesses CO7, CO8, CO9
Mini Project/Case Study	1 Project	**10**	Design, implementation, demo & reflection — all 4 Lab COs (CO7–CO10)
TOTAL	—	**40**	

11.2 Per-Experiment CA Rubric (3.0 Marks each — Assesses CO7, CO8, CO9)

Criterion	Marks	CA Skill Dimensions Covered	Marking Guide	Lab CO
Problem Definition & Experimental Design	**1.0**	CA1 – Problem identification and ML objective, CA2 – Dataset selection and preprocessing strategy, CA7 – ML workflow, feature engineering, and model selection	1.0: Well-defined with design | 0.5: Partial | 0: Missing	CO7, CO8
Model Implementation & Computational Efficiency	**1.0**	CA3 – Correct implementation of ML algorithms, CA4 – Efficient coding, model training, parameter tuning, and use of ML frameworks	1.0: Correct & efficient | 0.5: Correct, not optimized | 0: Fails	CO7
Model Evaluation, Result Analysis & Documentation	**0.75**	CA5 – Performance evaluation using Accuracy, Precision, Recall, F1-score, ROC, Confusion Matrix, CA6 – Interpretation of results, comparison of models, report preparation	0.75: Thorough | 0.5: Adequate | 0.25: Partial | 0: Absent	CO8, CO9
Professional Attitude & Ethical Conduct	**0.25**	CA6 – Structured documentation and presentation, CA8 – Viva-voce and technical communication, PO7/CO10 – Ethical AI, data privacy, and responsible use of ML in Cyber Security	0.25: Consistent | 0.10: Occasional | 0: Absent	CO9
Total	**3.0**	All 8 CA skill dimensions covered		

11.3 Best-10-of-N Scoring Scheme

Conducted	Best N Counted	Max Score	Note
> (10 + x)	Best 10	**30 Marks**	x worst dropped
10	All 10	**30 Marks**	No drop
< 10	All	**≤ 30 Marks**	Deficit = zero

11.4 Mini Project Evaluation Rubric (10 Marks — All 4 Lab COs)

Criterion	Marks	Project Skill Dimensions	Marking Guide	Lab CO / PO
SDG Alignment & Problem Scoping	**1.5**	P1 — SDG mapping; societal relevance P2 — Problem scope and stakeholder requirements P4 — Innovative solution proposal with alternatives	1.5: Comprehensive | 1.0: Adequate | 0.5: Partial | 0: Absent	CO8 / PO3, PO6
Project Planning & Financial Awareness	**1.5**	P2 — Timeline, milestones, resource planning P11 — Financial feasibility and cost estimation	1.5: Detailed | 1.0: Adequate | 0.5: Basic | 0: Absent	CO10 / PO10
End-to-End Implementation & System Operation	**2.0**	P5 — Professional toolchain selection P6 — Complete project build and integration P7 — System commissioning and operational testing	2: Fully operational | 1–1.5: Partial | 0–0.5: Non-functional	CO7, CO8 / PO3, PO5
Impact Assessment & Critical Reporting	**2.0**	P8 — Measurable outcome vs stated goals P9 — Statistical/comparative analysis; technical report	2: Rigorous | 1.5: Good | 1: Basic | 0: Absent	CO8, CO10 / PO6
Communication, Presentation & Teamwork	**2.0**	P3 — Communication plan and testing strategy P10 — Professional presentation quality and delivery	2: Excellent | 1.5: Good | 1: Adequate | 0: Poor	CO10 / PO8, PO9
Skill Reflection, Ethics & Professional Attitudes	**1.0**	P12 — Skill growth mapping (pre/post project) P13 — Professional attitudes and ethical conduct	1.0: Reflective & honest | 0.5: Partial | 0: Absent	CO9 / PO7, PO11
Total	**10**	All 13 Project skill dimensions; all 4 Lab COs (CO7–CO10)		

12. CA Skill Dimensions (8 Dimensions — Lab COs only)

ID	Dimension	What is Measured	Lab CO Anchor

CA1	Problem Definition & Dataset Understanding	Define the machine learning problem, identify cybersecurity objectives, select appropriate datasets, define features, labels, and success criteria.	CO7, CO8
CA2	Experimental Design & Environment Setup	Plan the ML experiment, configure Python, Jupyter Notebook, Scikit-learn, TensorFlow/Keras, prepare datasets, and select suitable ML algorithms.	CO7
CA3	Model Implementation & Execution	Implement machine learning algorithms, perform data preprocessing, feature engineering, model training, testing, and prediction correctly.	CO7
CA4	Model Optimization & Computational Efficiency	Optimize model performance using feature selection, hyperparameter tuning, cross-validation, and efficient utilization of ML frameworks.	CO7
CA5	Model Evaluation & Result Interpretation	Evaluate models using Confusion Matrix, Accuracy, Precision, Recall, F1-Score, ROC-AUC, compare models, and interpret results.	CO8
CA6	Documentation & Outcome Verification	Prepare structured lab reports with code, outputs, graphs, screenshots, observations, and validate results against objectives.	CO7, CO8
CA7	ML Workflow & Solution Design	Design complete machine learning workflows including data preparation, model selection, training, testing, evaluation, and cybersecurity solution planning.	CO7, CO8
CA8	Lab Record, Presentation & Professional Ethics	Maintain laboratory records, demonstrate conceptual understanding during viva, communicate results effectively, and follow ethical AI and cybersecurity practices.	CO7, CO9

13. Project Skill Dimensions (13 Dimensions — Lab COs only)

ID	Dimension	What is Measured	Lab CO / PO Anchor
P1	**SDG Alignment & Social Relevance**	Map project to relevant SDGs; articulate societal value and intended impact	CO8 | PO6
P2	**Problem Scoping & Requirements**	Define boundaries; produce formal problem statement with measurable goals	CO8 | PO2
P3	**Communication & Testing Strategy**	Develop communication plan; design testing strategy; coordinate group activities	CO10 | PO9
P4	**Innovative Solution Proposal**	Propose solution with alternatives; justify selection using design criteria	CO8 | PO3
P5	**Professional Toolchain**	Select and justify development tools; configure professional project environment	CO7 | PO5
P6	**End-to-End Implementation**	Build complete integrated solution incorporating at least 3 syllabus topics	CO7, CO8 | PO3
P7	**System Commissioning & Testing**	Deploy and operate system; conduct edge-case and stress tests	CO7, CO8 | PO5
P8	**Measurable Impact & Outcome**	Evaluate actual outcomes against goals; quantify impact using defined metrics	CO8 | PO6
P9	**Critical Analysis & Reporting**	Perform comparative/statistical analysis; produce structured technical report	CO8, CO10 | PO2, PO4
P10	**Professional Presentation & Teamwork**	Deliver professional presentation; evidence team collaboration and role differentiation	CO10 | PO8, PO9
P11	**Financial Feasibility & Planning**	Estimate project cost; justify resource allocation; discuss cost-effectiveness	CO10 | PO10
P12	**Individual Skill Growth Mapping**	Document pre/post skill gaps; map personal contributions to project dimensions	CO9 | PO11
P13	**Professional Attitude, Ethics & Responsibility**	Demonstrate integrity, ethical conduct, and responsible use of tools/data throughout	CO9 | PO7

14. CO × Skill Dimensions Mapping (10 COs × [6 Theory+ 8 CA + 13 Project Dimensions])

- *Theory COs (CO1–CO6) are fully mapped. Lab COs (CO7–CO10) intentionally have no TS mapping — confirming strict assessment separation.*
- *Theory COs (CO1–CO6) have NO CA alignment — confirms they are NOT evaluated in lab. All CA alignments confined to Lab COs (CO7–CO10).*
- *Theory COs (CO1–CO6) have NO project alignment — confirms strict lab-only assessment. All 13 Project dimensions anchored exclusively to Lab COs (CO7–CO10).*

CO	Theory Skill Dimensions						CA Skill Dimensions								Project Skill Dimensions												
	TS1 Factual Recall	TS2 Conceptual Expl.	TS3 Procedural App.	TS4 Analytical Rsng	TS5 Compar. Eval.	TS6 Synthesis & Design	CA1 :Prob.Def.	CA2 Exp.Setup	CA3 Execution	CA4 Efficiency	CA5 Output Anal.	CA6 Doc.Outcome	CA7 Algo.Design	CA8 Lab Rec./Viva	P1 SDG	P2 Scoping	P3 Comm.	P4 Solution	P5 Tools	P6 Impl.	P7 Sys.Op.	P8 Impact	P9 Analysis	P10 Present.	P11 Financial	P12 Skill Map	P13 Attitude
CO1	H	M																									
CO2	M	H	M																								
CO3		M	H	M																							
CO4			M	H	M																						
CO5				M	H	M																					
CO6			M		M	H																					
CO7							H	H	H	M		M	M	H					H	M	H						
CO8							M		M		H	H	H		H	H		H	M	H	M	H	M				
CO9														M												H	H
CO10																	H						M	H	H		

H = High / Primary M = Medium / Secondary Blank = No direct alignment

PART IV

COMBINED MAPPINGS & REFERENCE

CO–PO Matrix, SDG Mapping, Bloom's Taxonomy Reference, Attendance & Pass/Fail

15. CO–PO and CO–PSO Mapping Matrix (All 10 COs)

Strength Scale: 3 = Substantial (High) | 2 = Moderate | 1 = Slight (Low) | – = Not Applicable. Column averages computed over non-zero entries only.

CO/PO	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PSO1	PSO2	PSO3
CO1	3	2	-	2	2	2	3	1	1	1	2	3	2	2
CO2	3	3	2	2	3	-	2	2	-	1	2	3	3	2
CO3	2	3	3	3	3	-	2	-	-	1	2	3	3	3
CO4	3	2	2	3	3	-	2	-	1	-	2	3	3	2
CO5	2	3	-	2	2	2	2	-	1	2	3	2	3	2
CO6	2	2	-	-	-	1	-	-	3	2	2	2	2	2
CO7	–	–	1	–	3	1	–	–	–	–	–	2	3	3
CO8	–	1	3	1	2	3	–	–	–	–	–	2	3	3
CO9	–	–	–	–	–	–	3	–	–	–	3	–	1	2
CO10	–	–	–	–	–	1	–	3	3	3	2	2	2	2
Avg	2.50	2.29	2.20	2.17	2.57	1.67	2.33	2.00	1.80	1.67	2.25	2.44	2.50	2.30

PO7 (Ethics) now receives mapping from CO9 (strength 3). PO11 (Life-Long Learning) is addressed by both Theory COs and CO9. Lab COs (CO7–CO10) extend coverage to POs 3, 5, 6, 7, 8, 9, 10, 11.

16. CO × PO Alignment Map (H/M Indicators — All 10 COs × 11 POs)

CO	PO1 Eng.Know.	PO2 Prob.Analysis	PO3 Design	PO4 Investigation	PO5 Tool Usage	PO6 Engineer & World	PO7 Ethics	PO8 Teamwork	PO9 Comm.	PO10 Proj.Mgmt	PO11 Lifelong
CO1	H	M	-	M	M	M	H				M
CO2	H	H	M	M	H	-	M	M	-		M
CO3	M	H	H	H	H	-	M	-	-		M
CO4	H	M	M	H	H	-	M	-		-	M
CO5	M	H	-	M	M	M	M	-		M	H
CO6	M	M	-	-	-		-	-	H	M	M
CO7	–	–		–	H		–	–	–	–	–
CO8	–		H		M	H	–	–	–	–	–
CO9	–	–	–	–	–	–	H	–	–	–	H
CO10	–	–	–	–	–		–	H	H	H	M

H = High / Primary M = Medium / Secondary *Blank = No direct alignment*

17. Course-to-SDG Mapping Matrix

SDG Goal	Description	Mapping	Justification
SDG 4	**Quality Education**	**3 (High)**	Develops strong foundations in Machine Learning, Artificial Intelligence, and Cyber Security through hands-on learning, problem-solving, and lifelong learning skills (CO1–CO6).
SDG 8	**Decent Work & Economic Growth**	**3 (High)**	Equips students with industry-relevant skills in machine learning, data analytics, cybersecurity, and AI frameworks, enhancing employability in emerging technology domains (CO3–CO6).

SDG 9	**Industry, Innovation & Infrastructure**	3 (High)	Promotes the design of intelligent cyber defense systems, secure AI solutions, and innovative machine learning models for cybersecurity applications (CO4–CO6).
SDG 12	**Peace, Justice & Strong Institutions**	2 (Moderate)	Supports secure digital infrastructure through AI-based threat detection, intrusion detection, malware analysis, and ethical cybersecurity practices (CO2–CO6).

18. Bloom's Taxonomy — Domain Level Reference

Cognitive Domain (6 Levels)	Affective Domain (5 Levels)	Psychomotor Domain — Simpson (7 Levels)
L1 — Remember: Recall facts, definitions, basic concepts	A1 — Receiving: Awareness, willingness to attend	P1 — Perception: Sensory cues guide motor activity
L2 — Understand: Explain ideas, concepts, principles	A2 — Responding: Active participation and reaction	P2 — Set: Mental, physical readiness to act
L3 — Apply: Use knowledge to solve new problems	A3 — Valuing: Showing commitment, assigning value	P3 — Guided Response: Basic practice through imitation
L4 — Analyze: Break down information, examine patterns	A4 — Organizing: Integrating values into personal system	P4 — Mechanism: Habitual correct performance
L5 — Evaluate: Judge, justify, assess, make decisions	A5 — Characterizing: Internalized value system	P5 — Complex Overt Response: Skilled performance
L6 — Create: Design, develop, produce new solutions		P6 — Adaptation: Modify skills for special situations
		P7 — Origination: Create new solution patterns

OBE Compliance Statement: Theory COs (CO1–CO6) are primarily mapped to the Cognitive domain (L1–L6). Lab COs (CO7–CO10) span all three domains — Cognitive (L2–L6), Psychomotor (P3–P7), and Affective (A2–A5) — reflecting the skill-based nature of laboratory and project assessment.

19. Attendance Policy & Pass/Fail Criteria

19.1 Attendance Policy

Component	Minimum	Applicable To	Consequence
Theory Classes	**70%**	All lecture sessions	Debarred from ETE
Practical / Lab	**70%**	All lab sessions	Debarred from ETE
Combined (Theory + Lab)	**75%**	Combined sessions	Debarred from ETE

Both theory and practical attendance must independently meet 70%. The combined must be 75%. Satisfying one does NOT compensate for a shortfall in the other.

19.2 Pass / Fail Criteria

Condition	Threshold	Status	Remarks
ETE Score (scaled)	**≥ 20 / 50**	**MANDATORY**	40% of ETE; equivalent to ≥ 40/100 on the full paper
Overall Total	**≥ 40 / 100**	**Must pass overall**	Lab 40 + MTE 10 + ETE 50 = 100; 40% overall minimum required

PPS INTEGRATED COURSE PLAN — MEASUREMENT ARCHITECTURE

11 AICTE Programme Outcomes → 10 COs (6 Theory + 4 Lab) → 3 Assessment Instruments → 27 Skill Dimensions (6 TS + 8 CA + 13 Project)

Theory Tier CO1–CO6 (MTE + ETE): PO1, PO2, PO3, PO4, PO9 | 6 Theory Skill Dims (TS1–TS6)

Lab Tier CO7–CO10 (Lab only): PO3, PO5, PO6, PO7, PO8, PO9, PO10, PO11 | 8 CA Dims + 13 Project Dims

Marks: Lab 40 (Experiments 30 @ 3.0 each + Project 10) + MTE 10 + ETE 50 = Total 100

COURSE PLAN

Open-source Tools for Cyber Security & Forensics (CSCF2303)

School of Computing Science & Engineering (SSCSE) | B.Tech CSE | Semester IV | Batch 2026–2030

Integrated Course Plan — Theory COs (CO1–CO6) + Lab COs (CO7–CO10) | New AICTE 11-PO Framework | Full Skill Mapping

PART I

COURSE SYLLABUS

Course Identification, Details, Outcomes, BTL Mapping & Lecture/Lab Plans

1. Course Identification

School:	SSCSE	**Batch:**	2026–2030
Program:	B.Tech	**Current Academic Year:**	2026–27
Branch:	CSE	**Semester:**	IV

2. Course Details

Integrated theory + laboratory model. 10 COs in two tiers: Theory COs (CO1–CO6) via MTE + ETE; Lab COs (CO7–CO10) via Laboratory Assessment only. No cross-evaluation.

S.No	Attribute	Details
1	**Course Code**	**CSCF2303**
2	**Course Title**	Open-source Tools for Cyber Security & Forensics
3	**Credits**	4
4	**Contact Hours (L-T-P-SL)**	3-0-2-3
5	**Course Status**	Core

6	**Course Objective**	1. To develop foundational knowledge and practical skills in using open-source tools for penetration testing, vulnerability assessment, and host reconnaissance in cyber security environments. 2. To build an understanding of legal, ethical, and professional considerations in cyber security and digital forensics while applying responsible security practices. 3.To explain and apply methodologies, tools, and techniques for identifying, analyzing, and mitigating social engineering and network-based security attacks. 4. To develop proficiency in threat prevention and defense strategies for securing real-time systems and mitigating targeted cyber attacks using open-source security tools..
7	**Course Outcomes (COs)**	**After successful completion of this course, the student will be able to:** **THEORY COs — Assessed via MTE + ETE:** **LAB COs — Assessed via Laboratory Assessment only:** CO1(Understand – L1/L2): Acquire knowledge of open-source tools for penetration testing and vulnerability assessment. CO2 (Explore – L2/L3): Develop an understanding of legal and ethical considerations in cyber security and digital forensics. CO3(Apply – L3): Explain the methodologies and tools used in identifying and mitigating social engineering attacks. CO4(Analyze – L4/L5): Explain and apply techniques for performing host reconnaissance using open-source tools. CO5 (Analyze – L4/L5): Analyze and execute network attack techniques to understand network security vulnerabilities. CO6 (Analyze – L2/L4): Gain proficiency in threat prevention strategies to secure real-time systems and mitigate targeted attacks using open source tool. CO7 (L4 – Analyze): Analyze network vulnerabilities and cyber threats using open-source security tools. CO8 (L5/L6 – Create): Prepare and present security assessment and forensic report CO9 (L3 – Apply): Apply open-source tools for security testing, monitoring, and forensic analysis. CO10 (L3 – Apply): Demonstrate ethical and professional practices while using cybersecurity tools.
8	**Teaching & Learning**	Classroom Instructions (CI) 45 hrs + Lab Instructions (LI) 30 hrs + Self Learning (SL) 45 hrs = 120 hrs
9	**Mode of Examination**	Lab (40 marks) + MTE (10 marks) + ETE (50 marks) = 100 marks. Theory COs: MTE + ETE only. Lab COs: Lab only.

10	**Self Learning (SL: 45 hrs)**	1. Perform Network Scanning and Vulnerability Mapping using Nmap 2. Open Source Intelligence (OSINT) and Footprinting Analysis using Maltego 3. Packet Inspection and Traffic Analysis using Wireshark
11	**References**	Textbook: 1. Open Source Security Tools: A Practical Guide to Security Applications, Tony Howlett, Prentice Hall, Pearson Education, Inc 2. Implementing Enterprise Cyber Security with Open-Source Software and Standard Architecture: Volume II, Anand Handa, Rohit Negi, S. Venkatesan, Sandeep K. Shukla

3. Outline Syllabus — Theory Units with CO Mapping (CO1–CO6)

Unit CO mappings refer to Theory COs (CO1–CO6) only. Lab experiments reinforce these units but are assessed under Lab COs (CO7–CO10).

	Topic / Activity	CO Mapping
Unit 1	**Fundamentals of Cyber Security and Open-Source Tools (8-0-0-6 = 14hrs)**	
A	Understanding threats, vulnerabilities, and attacks Overview of the Cyber Security landscape and the importance of open-source tools	CO1, CO2, CO3
B	Ethical and legal implications of using open-source tools in cybersecurity	
C	Using Open-Source tools	
Tools Used	namp	
Activities	**Objective:** • Understand cyber threats, vulnerabilities, and common attacks. • Explore the cybersecurity landscape and use of open-source security tools. • Apply ethical and legal practices while using open-source cybersecurity tool	

Unit 2	**Network Security and Penetration Testing Tools (10-0-0-9= 19 hrs)**	
A	Network Scanning and Enumeration, Scanning and analyzing open ports, services, and vulnerabilities	CO3, CO4
B	Introduction to penetration testing stages and methodologies	
C	Using Open-Source tools for Penetration Testing	
Tools Used	nikto	
Activities	**Objective:** • Perform network scanning and host enumeration using open-source tools. • Analyze open ports, services, and system vulnerabilities. • Apply penetration testing methodologies using open-source security tools.	
Unit 3	**Social Engineering and Web Application Security (9-0-0-10 = 19 hrs)**	
A	Types of social engineering attacks: phishing, pretexting, and baiting	CO2, CO3, CO4
B	Introduction to OWASP Top 10 vulnerabilities	
C	Using Open Source tools for Social Engineering and Web Application Security	
Tools Used	burpsute	
Activities	**Objective:** • Identify common social engineering attacks and their techniques. • Understand the OWASP Top 10 web application vulnerabilities. • Use open-source tools to assess social engineering and web application security.	
Unit 4	**Digital Forensics and Evidence Collection (9-0-0-10 = 19 hrs)**	

A	Stages of digital forensics: identification, preservation, collection, analysis, and reporting	CO3, CO4, CO6
B	Evidence Handling and Reporting, Chain of custody and preserving digital evidence integrity	
C	Open source tools for Digital Forensics	
Tools Used	FTK, Autopsy	
Activities	**Objective:** • Understand the stages of digital forensic investigation. • Apply proper evidence handling and chain of custody procedures. • Use open-source digital forensic tools for evidence collection and analysis	
Unit 5	**Advanced Threat Detection and Mitigation Techniques (9-0-0-10 = 19 hrs)**	
A	Host and Network Intrusion Detection Systems (IDS)	C01, C03, CO5, CO6
B	Log Analysis and Threat Hunting, Analyzing logs for indicators of compromise (IoCs)	
C	Open Source tools for log analysis and threat monitoring	
Tools Used	CLi	
Activities	**Objective:** • Understand host and network intrusion detection systems (IDS). • Analyze logs to identify Indicators of Compromise (IoCs) and cyber threats. • Use open-source tools for log analysis and threat monitoring.	

4. Topic-wise Bloom's Taxonomy Level Mapping (Theory)

S.No	Topic	L1	L2	L3	L4	L5	L6

1	1.A	□	□				
2	1.B		□	□			
3	1.C		□	□			
4	2.A			□			
5	2.B			□			
6	2.C			□	□		
7	3.A			□	□		□
8	3.B		□	□		□	
9	3.C			□	□		
10	4.A			□	□		
11	4.B			□	□	□	
12	4.C			□			
13	5.A		□	□		□	□
14	5.B			□	□		
15	5.C			□	□	□	

5. CO vs Bloom's Taxonomy — All Three Domains (Updated for 10 COs)

□ *Only strong/dominant alignments are mapped. Lab COs (CO7–CO10) extend into Psychomotor and Affective domains, reflecting the skill-based nature of lab and project work.*

CO	Cognitive Domain (L1–L6)						Affective (A1–A5)					Psychomotor (P1–P7)						
CO	L1	L2	L3	L4	L5	L6	A1	A2	A3	A4	A5	P1	P2	P3	P4	P5	P6	P7
CO1	□																	
CO2		□																
CO3			□											□				

CO4				□											□			
CO5					□											□		
CO6						□			□							□	□	
CO7			□		✓			□					✓	□	□			
CO8					□	□			□						□	□	□	
CO9			□							□	□							
CO10			□					□			□			□			✓	

Legend: □ = Strong / Dominant mapping only. Theory COs: primarily Cognitive. Lab COs: span all three domains.

6. Lecture Plan Outline (Theory — 45 Lectures)

Date	Topics to be Covered	Unit	Total Lectures
DD/MM/YY	Fundamentals of Cyber Security and Open-Source Tools	**UNIT-1**	**8**
DD/MM/YY	Understanding threats		
DD/MM/YY	vulnerabilities,		
DD/MM/YY	Attacks		
DD/MM/YY	Risk		
DD/MM/YY	Overview of the Cyber Security landscape		
DD/MM/YY	Software/Tools		
DD/MM/YY	Contributor		
DD/MM/YY	Ethical and legal implications of using open-source tools in cybersecurity	**UNIT-2**	**10**
DD/MM/YY	the importance of open-source tools		
DD/MM/YY	Using Open-Source tools		
DD/MM/YY	Network Security and Penetration Testing Tools		
DD/MM/YY	Network Scanning and Enumeration		
DD/MM/YY	Scanning and analyzing open ports		
DD/MM/YY	services, and vulnerabilities		

DD/MM/YY	Introduction to penetration testing stages		
DD/MM/YY	Using Open-Source tools for Penetration Testing		
DD/MM/YY	WiresharK		
DD/MM/YY	nmap		
DD/MM/YY	Social Engineering and Web Application Security	**UNIT-3**	**9**
DD/MM/YY	Types of social engineering attacks		
DD/MM/YY	phishing, pretexting, and baiting		
DD/MM/YY	Whaling		
DD/MM/YY	Baiting		
DD/MM/YY	Introduction to OWASP Top 10 vulnerabilities		
DD/MM/YY	Introduction to OWASP Top 10 vulnerabilities		
DD/MM/YY	Introduction to OWASP Top 10 vulnerabilities		
DD/MM/YY	Introduction to OWASP Top 10 vulnerabilities		
DD/MM/YY	Using Open Source tools for Social Engineering and Web Application Security	**UNIT-4**	**9**
DD/MM/YY	Brupsuit		
DD/MM/YY	Metasploit		
DD/MM/YY	Digital Forensics and Evidence Collection		
DD/MM/YY	Stages of digital forensics		
DD/MM/YY	identification, preservation		
DD/MM/YY	collection		
DD/MM/YY	analysis, and reporting		
DD/MM/YY	Evidence Handling and Reporting	**UNIT-5**	**9**
DD/MM/YY	Chain of custody		
DD/MM/YY	preserving digital evidence integrity		
DD/MM/YY	Autopsy		
DD/MM/YY	Advanced Threat Detection and Mitigation Techniques		
DD/MM/YY	Host and Network Intrusion Detection Systems		
DD/MM/YY	Log Analysis		
DD/MM/YY	Threat Hunting		
DD/MM/YY	Analyzing logs for indicators of compromise (IoCs),		

DD/MM/YY	Open Source tools for log analysis and threat monitoring		

7. Lab Session Plan — List of Experiments (Updated CO7–CO10)

W1–W12: All experiments develop CO7 skills (professional implementation, tool usage, documentation). W13–W15 (teal rows): CO8 (design/real-world), CO9 (ethics/reflection), CO10 (teamwork/presentation). Theory knowledge is applied but NOT re-evaluated in lab.

Week	Session	Experiment	Lab CO	Marks
W1	S-1	Installation and Familiarization with Cyber Security Tools	CO7	3.0
W2	S-2	Basic Network Discovery Using Nmap	CO7	3.0
W3	S-3	Packet Capture and Analysis Using Wireshark	CO7	3.0
W4	S-4	Network Enumeration Using Nmap	CO7	3.0
W5	S-5	Vulnerability Assessment Using OpenVAS (Greenbone)	CO7	3.0
W6	S-6	Web Server Security Assessment Using Nikto	CO7	3.0
W7	S-7.	HTTP Request Analysis Using Burp Suite Community Edition	CO7	3.0
W8	S-8	Web Application Security Testing Using OWASP ZAP	CO8/CO9	3.0

W9	S-9	Network using tcpdump	**CO8/CO10**	3.0
W10	S-10	Disk Image Analysis Using Autopsy	**CO9/CO10**	3.0
W11	S-11	Deleted File Recovery Using TestDisk and PhotoRec	**CO7**	3.0
W12	S-12	Basic System Log Analysis	**CO7**	3.0
W13	S-13	Basic Intrusion Detection Using open source tools	**CO8**	3.0
W14	S-14	Use python script for port scanning	**CO8/CO9**	3.0
W15	S-15	Use FTK for imaging and analysis	**CO8/CO9**	3.0

PART II

THEORY ASSESSMENT FRAMEWORK

Theory Skill Dimensions, MTE & ETE Structure for Theory COs (CO1–CO6)

8. Theory Skill Dimensions (TS1–TS6) — CO1 through CO6

THEORY COs (CO1–CO6) — Assessed exclusively via MTE and ETE only

Six theory skill dimensions — one per Bloom's level L1–L6 — correspond directly to CO1–CO6. They define the competency measured in each section of MTE and ETE, providing a clear NBA-auditable assessment rationale.

ID	Dimension	What is Measured	CO / BTL	Assessment
TS1	**Fundamentals of Cyber Security and Open-Source Tools**	Acquire knowledge of open-source tools for penetration testing and vulnerability assessment.	CO1 | L1–L2	CA | MTE Sec A | ETE Sec A
TS2	**Network Security and Penetration Testing Tools**	Develop an understanding of legal and ethical considerations in cyber security and digital forensics	CO2 | L2–L3	CA | MTE Sec A | ETE Sec A
TS3	**Social Engineering and Web Application Security**	Explain the methodologies and tools used in identifying and mitigating social engineering attacks.	CO3 | L3	CA | MTE Sec B | ETE Sec B
TS4	**Digital Forensics and Evidence Collection**	Explain and apply techniques for performing host reconnaissance using open-source tools	CO4 | L4–L5	MTE Sec B | ETE Sec B
TS5	**Advanced Threat Detection and Mitigation Techniques**	Analyze and execute network attack techniques to understand network security vulnerabilities.	CO5 | L4–L5	ETE Sec B/C
TS6	**Advanced Threat Detection and Mitigation Techniques**	Gain proficiency in threat prevention strategies to secure real-time systems and mitigate targeted attacks using open source tool.	CO6 | L2–L4	ETE Sec C

9. Theory Assessment Structure — MTE and ETE

9.1 Mid Term Examination (MTE) — 10 Marks (CO1–CO4 only)

Section	Marks	Skill Dimensions	COs	Question Type
Sec A	**4**	TS1 — Factual Recall TS2 — Conceptual Explanation	**CO1, CO2**	Short-answer: definitions.
Sec B	**6**	TS3 — Procedural Application TS4 — Analytical Reasoning	**CO3, CO4**	Long and descriptive answers
TOTAL	**10**	TS1–TS4	**CO1–CO4**	Units 1–3 covered; CO5 and CO6 assessed only in ETE

9.2 End Term Examination (ETE) — 100 Marks (Scaled to 50) (CO1–CO6)

Section	Marks	Skill Dimensions	COs	Question Type
Sec A	**25**	TS1 — Factual Recall TS2 — Conceptual Explanation	**CO1, CO2**	Short questions: definitions.
Sec B	**50**	TS3 — Procedural Application TS4 — Analytical Reasoning TS5 — Comparative Evaluation	**CO3, CO4, CO5**	Medium questions: Comparison, Tools and Techniques, Algorithms
Sec C	**25**	TS5 — Comparative Evaluation TS6 — Synthesis & Design	**CO5, CO6**	Long/design questions: Applications, working principles/
TOTAL	**100**	TS1–TS6 (all)	**CO1–CO6**	Scaled to 50 marks. Minimum 20/50 required to pass.

PART III
LABORATORY ASSESSMENT FRAMEWORK

Evaluation Scheme, CA Rubric, Mini Project Rubric, Skill Dimensions for Lab COs (CO7–CO10)

10. Evaluation Scheme — Overview

Component	Weightage	Marks	COs Assessed
Laboratory Assessment	40%	**40**	Lab COs only: CA experiments
Mid Semester Examination (MTE)	10%	**10**	Theory COs only: CO1, CO2, CO3, CO4
End Semester Examination (ETE)	50%	**50**	Theory COs only: CO1, CO2, CO3, CO4, CO5, CO6
TOTAL	**100%**	**100**	Strict separation — no cross-assessment

11. Laboratory Assessment (40 Marks)

LAB COs (CO7–CO10) — Assessed exclusively via Laboratory Assessment only (CA)

11.1 Component Breakdown

Sub-Component	Quantum	Marks	Remarks
Lab Experiments (CA)	Best 10 of 12	**30**	3.0 marks each — assesses CO7, CO8, CO9
Mini Project/Case Study	1 Project	**10**	Design, implementation, demo & reflection — all 4 Lab COs (CO7–CO10)
TOTAL	—	**40**	

11.2 Per-Experiment CA Rubric (3.0 Marks each — Assesses CO7, CO8, CO9)

Criterion	Marks	CA Skill Dimensions Covered	Marking Guide	Lab CO
Problem Definition & Experimental Design	**1.0**	**CA1** —Identification of cybersecurity problem, objectives, and scope. **CA2** —Experiment planning, tool selection, and environment configuration. **CA7** — Security methodology,	1.0: Well-defined with design | 0.5: Partial | 0: Missing	CO7, CO8

		attack simulation, threat analysis, and mitigation approach.		
Code Execution & Computational Efficiency	**1.0**	**CA3** - Correct execution of network scanning, vulnerability assessment, penetration testing, and forensic tasks. **CA4** -Effective use of open-source cybersecurity tools and techniques.	1.0: Correct & efficient | 0.5: Correct, not optimized | 0: Fails	CO7
Output Analysis, Outcome & Lab Documentation	**0.75**	**CA5** —Analysis and interpretation of scan results, logs, vulnerabilities, and forensic evidence. **CA6** — Preparation of structured reports with observations, screenshots, evidence, and conclusions.	0.75: Thorough | 0.5: Adequate | 0.25: Partial | 0: Absent	CO8, CO9
Professional Attitude & Ethical Conduct	**0.25**	CA6 —Preparation of structured reports with observations, screenshots, evidence, and conclusions. CA8 —PO7/CO9 — Ethical and responsible cybersecurity practices	0.25: Consistent | 0.10: Occasional | 0: Absent	CO9
Total	**3.0**	All 8 CA skill dimensions covered		

11.3 Best-10-of-N Scoring Scheme

Conducted	Best N Counted	Max Score	Note
> (10 + x)	Best 10	**30 Marks**	x worst dropped
10	All 10	**30 Marks**	No drop
< 10	All	**≤ 30 Marks**	Deficit = zero

11.4 Mini Project Evaluation Rubric (10 Marks — All 4 Lab COs)

Criterion	Marks	Project Skill Dimensions	Marking Guide	Lab CO / PO
SDG Alignment & Problem Scoping	**1.5**	P1 — SDG mapping; societal relevance	1.5: Comprehensive | 1.0: Adequate |	CO8 / PO3, PO6

		P2 — Problem scope and stakeholder requirements P4 — Innovative solution proposal with alternatives	0.5: Partial | 0: Absent	
Project Planning & Financial Awareness	**1.5**	P2 — Timeline, milestones, resource planning P11 — Financial feasibility and cost estimation	1.5: Detailed | 1.0: Adequate | 0.5: Basic | 0: Absent	CO10 / PO10
End-to-End Implementation & System Operation	**2.0**	P5 — Professional toolchain selection P6 — Complete project build and integration P7 — System commissioning and operational testing	2: Fully operational | 1–1.5: Partial | 0–0.5: Non-functional	CO7, CO8 / PO3, PO5
Impact Assessment & Critical Reporting	**2.0**	P8 — Measurable outcome vs stated goals P9 — Statistical/comparative analysis; technical report	2: Rigorous | 1.5: Good | 1: Basic | 0: Absent	CO8, CO10 / PO6
Communication, Presentation & Teamwork	**2.0**	P3 — Communication plan and testing strategy P10 — Professional presentation quality and delivery	2: Excellent | 1.5: Good | 1: Adequate | 0: Poor	CO10 / PO8, PO9
Skill Reflection, Ethics & Professional Attitudes	**1.0**	P12 — Skill growth mapping (pre/post project) P13 — Professional attitudes and ethical conduct	1.0: Reflective & honest | 0.5: Partial | 0: Absent	CO9 / PO7, PO11
Total	**10**	All 13 Project skill dimensions; all 4 Lab COs (CO7–CO10)		

12. CA Skill Dimensions (8 Dimensions — Lab COs only)

ID	Dimension	What is Measured	Lab CO Anchor
CA1	**Problem Definition & Metrics**	Define cryptographic problem, objectives, scope, and success criteria	CO7, CO8

CA2	**Experimental Design & Tool Setup**	Configure cryptographic tools, environments, and security utilities	CO7
CA3	**Code Implementation & Execution**	Execute encryption, hashing, authentication, and security experiments	CO7
CA4	**Computational Efficiency & Optimization**	Evaluate performance and optimize cryptographic implementations	CO7
CA5	**Output Analysis & Result Interpretation**	Analyze ciphertexts, logs, packets, and security outputs	CO8
CA6	**Documented Outcome with Verification**	Record observations, screenshots, outputs, and validate results	CO7, CO8
CA7	**Algorithmic Design & Solution Planning**	Design secure workflows and cryptographic methodologies	CO7, CO8
CA8	**Lab Record Maintenance & Viva-Voce**	Maintain lab records and demonstrate conceptual understanding	CO7, CO9

13. Project Skill Dimensions (13 Dimensions — Lab COs only)

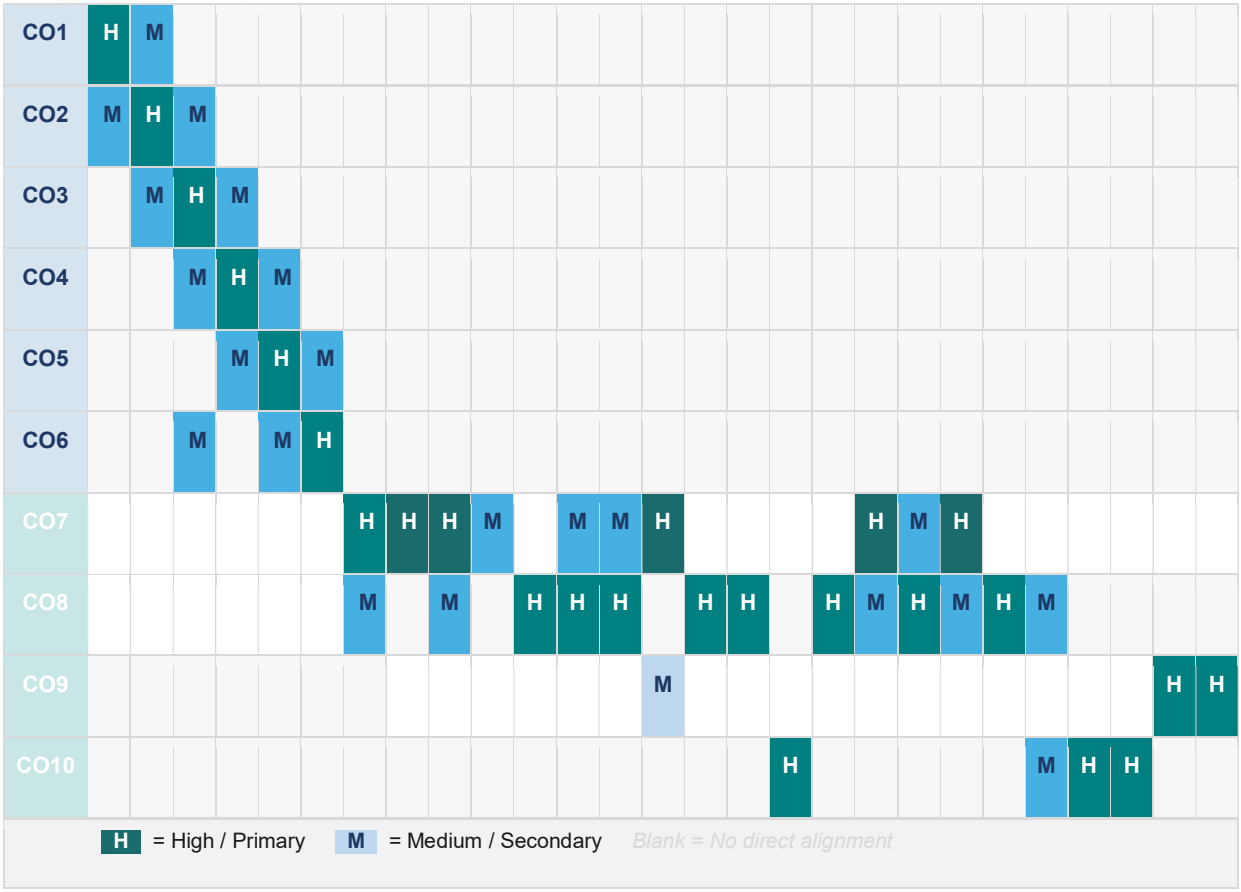
ID	Dimension	What is Measured	Lab CO / PO Anchor
P1	**SDG Alignment & Social Relevance**	Map project to relevant SDGs; articulate societal value and intended impact	CO8 | PO6
P2	**Problem Scoping & Requirements**	Define boundaries; produce formal problem statement with measurable goals	CO8 | PO2
P3	**Communication & Testing Strategy**	Develop communication plan; design testing strategy; coordinate group activities	CO10 | PO9
P4	**Innovative Solution Proposal**	Propose solution with alternatives; justify selection using design criteria	CO8 | PO3
P5	**Professional Toolchain**	Select and justify development tools; configure professional project environment	CO7 | PO5
P6	**End-to-End Implementation**	Build complete integrated solution incorporating at least 3 syllabus topics	CO7, CO8 | PO3

P7	**System Commissioning & Testing**	Deploy and operate system; conduct edge-case and stress tests	CO7, CO8 | PO5
P8	**Measurable Impact & Outcome**	Evaluate actual outcomes against goals; quantify impact using defined metrics	CO8 | PO6
P9	**Critical Analysis & Reporting**	Perform comparative/statistical analysis; produce structured technical report	CO8, CO10 | PO2, PO4
P10	**Professional Presentation & Teamwork**	Deliver professional presentation; evidence team collaboration and role differentiation	CO10 | PO8, PO9
P11	**Financial Feasibility & Planning**	Estimate project cost; justify resource allocation; discuss cost-effectiveness	CO10 | PO10
P12	**Individual Skill Growth Mapping**	Document pre/post skill gaps; map personal contributions to project dimensions	CO9 | PO11
P13	**Professional Attitude, Ethics & Responsibility**	Demonstrate integrity, ethical conduct, and responsible use of tools/data throughout	CO9 | PO7

14. CO × Skill Dimensions Mapping (10 COs × [6 Theory+ 8 CA + 13 Project Dimensions])

- *Theory COs (CO1–CO6) are fully mapped. Lab COs (CO7–CO10) intentionally have no TS mapping — confirming strict assessment separation.*
- *Theory COs (CO1–CO6) have NO CA alignment — confirms they are NOT evaluated in lab. All CA alignments confined to Lab COs (CO7–CO10).*
- *Theory COs (CO1–CO6) have NO project alignment — confirms strict lab-only assessment. All 13 Project dimensions anchored exclusively to Lab COs (CO7–CO10).*

CO	Theory Skill Dimensions						CA Skill Dimensions								Project Skill Dimensions												
	TS1 Factual Recall	TS2 Conceptual Expl.	TS3 Procedural App.	TS4 Analytical Rsng	TS5 Compar. Eval.	TS6 Synthesis & Design	CA1 :Prob.Def.	CA2 Exp.Setup	CA3 Execution	CA4 Efficiency	CA5 Output Anal.	CA6 Doc.Outcome	CA7 Algo.Design	CA8 Lab Rec./Viva	P1 SDG	P2 Scoping	P3 Comm.	P4 Solution	P5 Tools	P6 Impl.	P7 Sys.Op.	P8 Impact	P9 Analysis	P10 Present.	P11 Financial	P12 Skill Map	P13 Attitude



PART IV

COMBINED MAPPINGS & REFERENCE

CO–PO Matrix, SDG Mapping, Bloom's Taxonomy Reference, Attendance & Pass/Fail

15. CO–PO and CO–PSO Mapping Matrix (All 10 COs)

Strength Scale: 3 = Substantial (High) | 2 = Moderate | 1 = Slight (Low) | – = Not Applicable. Column averages computed over non-zero entries only.

CO/PO	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PSO1	PSO2	PSO3
CO1	3	3	3	-	2	2	-	-	3	-	-	-	3	-
CO2	3	3	3	2	2	-	-	-	-	-	-	-	-	-

CO3	3	3	3	2	2	2	3	-	-	2	-	3	2	3
CO4	3	3	3	-	3	2	3	-	2	-	2	3	-	-
CO5	3	3	2	3	2	-	2	-	3	3	3	2	2	2
CO6	2	3	3	2	3	3	3	3	-	-	3	3	2	3
CO7	–	2	1	–	3	2	–	–	–	–	–	2	3	3
CO8	–	1	3	1	2	3	–	–	–	–	–	2	3	3
CO9	–	–	2	–	–	2	3	–	–	1	3	–	1	2
CO10	2	–	–	–	–	1	–	3	3	3	2	2	2	2
Avg	2.71	2.63	2.56	2.00	2.38	2.13	2.80	3.00	2.75	2.25	2.60	2.43	2.25	2.57

PO7 (Ethics) now receives mapping from CO9 (strength 3). PO11 (Life-Long Learning) is addressed by both Theory COs and CO9. Lab COs (CO7–CO10) extend coverage to POs 3, 5, 6, 7, 8, 9, 10, 11.

16. CO × PO Alignment Map (H/M Indicators — All 10 COs × 11 POs)

CO	PO1 Eng.Know.	PO2 Prob.Analysis	PO3 Design	PO4 Investigation	PO5 Tool Usage	PO6 Engineer & World	PO7 Ethics	PO8 Teamwork	PO9 Comm.	PO10 Proj.Mgmt	PO11 Lifelong
CO1	H	H	H	-	M	M	-	-	H	-	-
CO2	H	H	H	M	M	-	-	-	-	-	-
CO3	H	H	H	M	M	M	H	-	-	M	-
CO4	H	H	H	-	H	M	H	-	M	-	M
CO5	H	H	M	H	M	-	M	-	H	H	H

CO6	M	H	H	M	H	H	H	H	-	-	H
CO7	–	M		–	H	M	–	–	–	–	–
CO8	–		H		M	H	–	–	–	–	–
CO9	–	–	M	–	–	M	H	–	–		H
CO10	M	–	–	–	–		–	H	H	H	M

H = High / Primary M = Medium / Secondary *Blank = No direct alignment*

17. Course-to-SDG Mapping Matrix

SDG Goal	Description	Mapping	Justification
SDG 4	**Quality Education**	**3 (High)**	Builds strong foundation in computational thinking and structured programming; aligned with lifelong learning (CO1–CO6, CO9).
SDG 8	**Decent Work & Economic Growth**	**3 (High)**	Develops industry-relevant programming and professional tool skills (CO7) directly applicable to employment in technology sectors.
SDG 9	**Industry, Innovation & Infrastructure**	**3 (High)**	Enables development of efficient software solutions; fosters innovation through real-world application design (CO6, CO8) and team-based projects (CO10).
SDG 12	**Responsible Consumption & Production**	**2 (Moderate)**	Promotes efficient, optimized coding; encourages ethical coding and responsible use of computational resources (CO9, CO7).

18. Bloom's Taxonomy — Domain Level Reference

Cognitive Domain (6 Levels)	Affective Domain (5 Levels)	Psychomotor Domain — Simpson (7 Levels)
L1 — Remember: Recall facts, definitions, basic concepts	A1 — Receiving: Awareness, willingness to attend	P1 — Perception: Sensory cues guide motor activity

L2 — Understand: Explain ideas, concepts, principles L3 — Apply: Use knowledge to solve new problems L4 — Analyze: Break down information, examine patterns L5 — Evaluate: Judge, justify, assess, make decisions L6 — Create: Design, develop, produce new solutions	A2 — Responding: Active participation and reaction A3 — Valuing: Showing commitment, assigning value A4 — Organizing: Integrating values into personal system A5 — Characterizing: Internalized value system	P2 — Set: Mental, physical readiness to act P3 — Guided Response: Basic practice through imitation P4 — Mechanism: Habitual correct performance P5 — Complex Overt Response: Skilled performance P6 — Adaptation: Modify skills for special situations P7 — Origination: Create new solution patterns

OBE Compliance Statement: Theory COs (CO1–CO6) are primarily mapped to the Cognitive domain (L1–L6). Lab COs (CO7–CO10) span all three domains — Cognitive (L2–L6), Psychomotor (P3–P7), and Affective (A2–A5) — reflecting the skill-based nature of laboratory and project assessment.

19. Attendance Policy & Pass/Fail Criteria

19.1 Attendance Policy

Component	Minimum	Applicable To	Consequence
Theory Classes	**70%**	All lecture sessions	Debarred from ETE
Practical / Lab	**70%**	All lab sessions	Debarred from ETE
Combined (Theory + Lab)	**75%**	Combined sessions	Debarred from ETE

Both theory and practical attendance must independently meet 70%. The combined must be 75%. Satisfying one does NOT compensate for a shortfall in the other.

19.2 Pass / Fail Criteria

Condition	Threshold	Status	Remarks

ETE Score (scaled)	**≥ 20 / 50**	**MANDATORY**	40% of ETE; equivalent to ≥ 40/100 on the full paper
Overall Total	**≥ 40 / 100**	**Must pass overall**	Lab 40 + MTE 10 + ETE 50 = 100; 40% overall minimum required

PPS INTEGRATED COURSE PLAN — MEASUREMENT ARCHITECTURE

11 AICTE Programme Outcomes → 10 COs (6 Theory + 4 Lab) → 3 Assessment Instruments → 27 Skill Dimensions (6 TS + 8 CA + 13 Project)

Theory Tier CO1–CO6 (MTE + ETE): PO1, PO2, PO3, PO4, PO9 | 6 Theory Skill Dims (TS1–TS6)

Lab Tier CO7–CO10 (Lab only): PO3, PO5, PO6, PO7, PO8, PO9, PO10, PO11 | 8 CA Dims + 13 Project Dims

Marks: Lab 40 (Experiments 30 @ 3.0 each + Project 10) + MTE 10 + ETE 50 = Total 100

SEMESTER V

COURSE PLAN

Security Threats Intelligence and Risk Management (CSCF3101)

SSCSE-Sharda School of Computing Science & Engineering | B.Tech CSE | Semester V | Batch 2025–2029

Theory-Only Course Plan — All 6 COs (CO1–CO6) | Theory Skill Dimensions TS1–TS6 | CA + MTE + ETE Assessment

PART I

COURSE SYLLABUS

Course Identification, Details, Outcomes, BTL Mapping & Lecture Plan

1. Course Identification

School:	SSCSE-Sharda School of Computing Science & Engineering	**Batch:**	2026-2030
Program:	B.Tech	**Current Academic Year:**	2026-27
Branch:	CSE	**Semester:**	V
Course Code:	CSCF3101	**Course Type:**	Core — Theory Only

2. Course Details

THEORY-ONLY COURSE — All 6 COs (CO1–CO6) are assessed exclusively via Continuous Assessment (CA), MTE, and ETE. No laboratory component.

S.No	Attribute	Details

1	**Course Code**	**CSCF3101**
2	**Course Title**	**Security Threats Intelligence and Risk Management**
3	**Credits**	3
4	**Contact Hours (L-T-P-SL)**	3-0-0-3 (Theory: 45 hrs Classroom + 45 hrs Self Learning = 90 hrs total)
5	**Course Status**	**Core — Theory Only (No Laboratory Component)**
6	**Course Objectives**	The subject provides a foundational platform for Cyber Security Aspirants by providing Cyber Security Awareness and Training that heighten the chances of catching a scam or attack before it is fully enacted, minimizing damage to the resources and ensuring the protection of information technology assets.
7	**Course Outcomes (COs)**	CO1 (Analyze/Evaluate – L4/L5): Analyze and evaluate the cyber security requirements and security posture of an organization to identify potential threats, vulnerabilities, and protection needs. CO2 (Analyze – L4/L5): Determine, analyze, and assess software vulnerabilities along with appropriate security solutions to minimize the risk of cyber exploitation and attacks. CO3 (Apply/Analyze – L3/L4): Measure the performance of cyber security systems and troubleshoot security issues using monitoring, auditing, and diagnostic techniques. CO4 (Apply – L3): Implement cyber security solutions and utilize cyber security, information assurance, and cyber/computer forensics tools and technologies in practical environments. CO5 (Understand/Analyze – L2/L4): Comprehend and execute risk management processes, including risk assessment, risk treatment methods, and evaluation of key risk and performance indicators. CO6 (Create/Evaluate – L5/L6): Design and develop an effective security architecture for organizations by integrating network, system, and cloud security principles.
8	**Course Description**	Understand principles of web security and guarantee a secure network by monitoring and analyzing the nature of attacks through cyber/computer forensics software/tools.
9	**Teaching & Learning Scheme**	Classroom Instructions (CI): 45 hrs | Self Learning (SL): 45 hrs | Total: 90 hrs
10	**Mode of Examination**	**Theory Only. CA: 25% | MTE: 15% | ETE: 60% | Total: 100 marks**
11	**Textbook**	Kurt J. Engemann and Jason A. Witty, Cybersecurity Risk Management, De Gruyter, 2024.
12	**References**	1.Christopher J. Hodson, Cyber Risk Management (2nd Edition), Kogan Page, 2024.

		2.Iqbal H. Sarker, AI-Driven Cybersecurity and Threat Intelligence: Cyber 3Automation, Intelligent Decision-Making and Explainability, Springer, 2024. 4 Keshav Kaushik and Ishu Sharma, Next-Generation Cybersecurity: AI, ML, and Blockchain, Springer Nature, 2024.

3. Outline Syllabus with CO Mapping

All CO mappings in this section refer to Theory COs (CO1–CO6). This is a theory-only course; all assessment is via CA, MTE, and ETE.

	Topic	CO Mapping
	Unit 1: Introduction	
A	Security threats - Sources of security threats- Motives	**CO1, CO2,CO3**
B	Target Assets and vulnerabilities – Consequences of threats- E-mail threats	**CO1, CO2,CO3**
C	Web-threats - Intruders and Hackers, Insider threats, Cybercrimes	**CO1,CO2,CO3**
	Unit 2: Network Threats	
A	Network Threats: Active/ Passive – Interference – Interception – Impersonation	**CO3, CO2, CO4**
B	Worms – Virus – Spam's – Ad ware - Spy ware – Trojans and covert channels – Backdoors – Bots	**CO3, CO2, CO4**
C	IP Spoofing - ARP spoofing - Session Hijacking - Sabotage-Internal treats- Environmental threats - Threats to Server security	**CO2, CO3, CO4**
	Unit 3: Security Threat	
A	Security Threat Management: Risk Assessment - Forensic Analysis - Security threat correlation	**CO1, CO4,CO6**

B	Threat awareness - Vulnerability sources and assessment- Vulnerability assessment tools -Threat identification - Threat Analysis - Threat Modeling - Model for Information Security Planning	**CO1, CO4, CO6**
C	Concepts of risk-based planning and risk management of computer and information systems.	**CO1, CO4, CO6**
	Unit 4: Security Elements	
A	Security Elements: Authorization and Authentication - types, policies and techniques	**CO5, CO6**
B	Security certification - Security monitoring and Auditing - Security Requirements Specifications	**CO5, CO6**
C	Security Policies and Procedures, Firewalls, IDS, Log Files, Honey Pots	**CO5, CO6**
	Unit 5: Access control & Human factors	
A	Access control, Trusted Computing and multilevel security - Security models	**CO4,CO5, CO6**
B	Trusted Systems, Software security issues, Physical and infrastructure security	**CO4, CO5, CO6**
C	Human factors – Security awareness, training , Email and Internet use policies.	**CO4, CO5, CO6**

4. Topic-wise Bloom's Taxonomy Level Mapping

S.No	Topic	L1 Remember	L2 Understand	L3 Apply	L4 Analyze	L5 Evaluate	L6 Create
1	1.A	✓	✓				
2	1.B	✓	✓	✓			
3	1.C		✓	✓	✓		
4	2.A	✓	✓	✓			
5	2.B	✓	✓	✓	✓		

6	2.C		✓	✓	✓	✓	
7	3.A	✓	✓	✓			
8	3.B		✓	✓	✓	✓	
9	3.C		✓	✓	✓	✓	✓
10	4.A	✓	✓	✓			
11	4.B		✓	✓	✓	✓	
12	4.C		✓	✓	✓	✓	✓
13	5.A	✓	✓	✓	✓		
14	5.B		✓	✓	✓	✓	
15	5.C		✓	✓	✓	✓	✓

5. CO vs Bloom's Taxonomy — All Three Domains

Only strong/dominant alignments are mapped. This is a theory-only course; Psychomotor mapping is limited to Guided Response (P3) for algorithm implementation in CO3. Affective domain appears at A3 (Valuing) for efficiency analysis in CO4 and CO5.

CO	Cognitive Domain (L1–L6)						Affective (A1–A5)					Psychomotor (P1–P7)						
CO	L1	L2	L3	L4	L5	L6	A1	A2	A3	A4	A5	P1	P2	P3	P4	P5	P6	P7
CO1				✓	✓			✓	✓									
CO2				✓	✓			✓		✓								
CO3			✓	✓					✓				✓	✓				

CO4			✓						✓	✓				✓	✓			
CO5		✓		✓				✓	✓				✓		✓			
CO6					✓	✓				✓	✓					✓	✓	

Legend: ✓= Strong / Dominant mapping. Theory-oriented Cloud Security course: Cognitive domain is primary. Psychomotor domain (P3) is limited to implementation and practical analysis of cloud security mechanisms, intrusion detection, and firewall configuration. Affective domain (A3) reflects valuing security, monitoring, and efficient protection mechanisms in cloud environments.

6. Lecture Plan Outline (Theory — 45 Lectures / 45 Hours)

Total classroom contact: 45 hours across 5 units. Self-Learning activities (45 hrs) are structured separately in Section 11.

Date	Topics to be Covered/Title	UNIT	Total Lectures
DD/MM/YY	Introduction to Security threats	UNIT-1	10
DD/MM/YY	Sources of security threats- Motives		
DD/MM/YY	Motives Behind Security Attacks		
DD/MM/YY	Target Assets in Cybersecurity		
DD/MM/YY	Vulnerabilities in Information Systems		
DD/MM/YY	Consequences of Security Threats		
DD/MM/YY	E-mail Threats		
DD/MM/YY	Web Threats		
DD/MM/YY	Intruders, Hackers and Insider Threats		
DD/MM/YY	Cybercrimes and Case Studies		

DD/MM/YY	Introduction to Network Threats	UNIT-2	8
DD/MM/YY	Active and Passive Threats		
DD/MM/YY	Malware Threats – I		
DD/MM/YY	Malware Threats – II		
DD/MM/YY	Spoofing Attacks		
DD/MM/YY	Session Hijacking		
DD/MM/YY	Internal and Environmental Threats		
DD/MM/YY	Threats to Server Security		
DD/MM/YY	Introduction to Security Threat Management	UNIT-3	10
DD/MM/YY	Risk Assessment Fundamentals		
DD/MM/YY	Risk Assessment Techniques		
DD/MM/YY	Forensic Analysis		
DD/MM/YY	Security Threat Correlation and Awareness		
DD/MM/YY	Vulnerability Sources and Assessment		
DD/MM/YY	Vulnerability Assessment Tools		
DD/MM/YY	Threat Identification and Threat Analysis		
DD/MM/YY	Threat Modeling and Information Security Planning		

DD/MM/YY	Risk-Based Planning and Risk Management		
DD/MM/YY	Introduction to Security Elements	UNIT-4	10
DD/MM/YY	Authentication		
DD/MM/YY	Authorization		
DD/MM/YY	Security Policies and Techniques		
DD/MM/YY	Security Certification		
DD/MM/YY	Security Monitoring and Auditing		
DD/MM/YY	Security Requirement Specifications		
DD/MM/YY	Firewalls and Intrusion Detection Systems		
DD/MM/YY	Log Files and Security Analysis		
DD/MM/YY	Honey Pots and Security Procedures		
DD/MM/YY	Introduction to Trusted Systems	UNIT-5	8
DD/MM/YY	Software Security Issues		
DD/MM/YY	Physical and Infrastructure Security		
DD/MM/YY	Human Factors in Security		
DD/MM/YY	Security Awareness and Training		

DD/MM/YY	Email and Internet Use Policies		
DD/MM/YY	Access Control and Trusted Computing		
DD/MM/YY	Multilevel Security and Security Models		

PART II

THEORY ASSESSMENT FRAMEWORK

Theory Skill Dimensions, CO × TS Mapping, CA / MTE / ETE Structure

7. Theory Skill Dimensions (TS1–TS6)

THEORY-ONLY COURSE — All 6 COs (CO1–CO6) are assessed exclusively via Continuous Assessment (CA), MTE, and ETE. No laboratory component.

Six Theory Skill Dimensions — one per Bloom's progression (L1–L4) — correspond directly to the six COs. They define precisely what competency is being measured in each section of the CA, MTE, and ETE, providing a clear NBA-auditable assessment rationale.

ID	Dimension	What is Measured	CO / BTL	Assessment
TS1	Cyber Security Requirements & Threat Identification	Analyze cyber security requirements, identify organizational threats, vulnerabilities, risks, and evaluate security posture for protection planning	CO1 | L4–L5	CA | MTE Sec A | ETE Sec A

TS2	Software Vulnerability Assessment & Security Solutions	Determine and analyze software vulnerabilities, assess cyber exploitation risks, and evaluate appropriate security solutions and countermeasures	CO2 | L4–L5	CA | MTE Sec B | ETE Sec B
TS3	Security Monitoring & Troubleshooting Application	Apply cyber security monitoring, auditing, and diagnostic techniques to measure system performance and troubleshoot security issues	CO3 | L3–L4	CA | MTE Sec B | ETE Sec B
TS4	Cyber Security Implementation & Forensic Tools	Implement cyber security solutions and utilize information assurance, cyber security, and cyber/computer forensic tools in practical environments	CO4 | L3	CA | Practical | ETE Sec B
TS5	Risk Management & Risk Evaluation	Understand and execute risk assessment, risk treatment, key risk indicators, and performance evaluation processes in information security management	CO5 | L2–L4	MTE Sec B | ETE Sec C
TS6	Security Architecture Design & Integration	Design and develop secure architectures by integrating network security, system security, and cloud security principles for organizational protection	CO6 | L5–L6	ETE Sec C | Project/Case Study

8. CO × Theory Skill Dimension Mapping (6 COs × 6 Dimensions)

Each CO maps primarily to one TS dimension (H) with adjacent dimensions receiving secondary mapping (M), reflecting the progressive Bloom's structure of this course.

CO	TS1 Conceptual Recall	TS2 Process Interpretation	TS3 Algorithmic Application	TS4 Performance Evaluation	TS5 Memory System Analysis	TS6 File & Disk Evaluation

CO1	H	M			M	
CO2	M	H	M			
CO3		M	H	M		
CO4			M	H	M	
CO5				M	H	M
CO6	M		M	M	M	H

H = High / Primary alignment M = Medium / Secondary alignment Blank = No direct alignment

9. Continuous Assessment (CA) — 25 Marks

CA is formative and covers COs progressively as the syllabus is taught. It includes numerical-based assignments, a technical video learning report, and a real-world case study — mirroring TS1 through TS6.

9.1 CA Component Breakdown (Sample)

Component	Quantum	Marks	COs Assessed	Skill Dimensions
Assignments 1–5 (Numerical / Problem-based)	5 assignments	**15**	CO1, CO2, CO3, CO4	TS1, TS2, TS3, TS4
Technical Video Learning Report	1 Report + Presentation	**5**	CO2, CO3	TS2, TS3
Real-World Case Study (Report)	1 Report	**5**	CO4, CO5, CO6	TS4, TS5, TS6
TOTAL	—	**25**	CO1–CO6	TS1–TS6

9.2 Assignment-wise CO & TS Mapping

Item	Topic / Focus	COs	TS Dims	SL Hours	Evaluation Criteria

Assignment 1	Cyber security requirements, organizational threats, vulnerabilities, and security posture analysis	CO1	TS1	5h SL	Report submission + conceptual evaluation
Assignment 2	Software vulnerability assessment, cyber exploitation risks, and implementation of security solutions	CO2	TS2	5h SL	Short-answer and conceptual analysis
Assignment 3	Security monitoring, auditing techniques, troubleshooting methods, and diagnostic analysis of cyber security systems	CO3	TS2, TS3	5h SL	Security mechanism implementation + comparative analysis
Assignment 4	Implementation of cyber security solutions, information assurance practices, and cyber/computer forensic tools	CO4	TS3, TS4	5h SL	Analytical report + security evaluation
Assignment 5	Risk assessment, risk treatment methods, key risk indicators, and organizational risk management strategies	CO5	TS4, TS5, TS6	5h SL	Threat analysis + comparative performance evaluation
Video Learning Report	Technical video on network security, system security, cloud security, digital forensics, IDS/IPS, or security architecture (minimum 3 hrs) with structured report and presentation	CO3, CO4, CO6	TS2, TS3	10h SL	Report: learning outcomes, key concepts, self-reflection. Presentation: 10 min
Case Study Report	Real-world cyber security case study such as ransomware attacks, enterprise security architecture, cloud security breaches, risk management frameworks, or forensic investigations with detailed analysis	CO1, CO5, CO6	TS4, TS5, TS6	10h SL	Technical depth, data collection, fact finding, comparative analysis

10. Mid Term Examination (MTE) — 15 Marks (Units 1–3)

MTE covers Units 1–3 (CO1, CO2, CO3, CO4). CO5 and CO6 are assessed in ETE only. MTE maps to TS1–TS4.

Section	Marks	Theory Skill Dimensions	COs Assessed	Question Type & Guidance
Section A	**10**	TS1 — Cyber Security Requirement Analysis & Threat Identification	CO1	Analytical and evaluative questions on identifying cyber security requirements, analyzing organizational threats, assessing vulnerabilities, evaluating security posture, and recommending protection mechanisms for information systems
Section B	**15**	TS2 — Software Vulnerability Assessment & Security Solution Evaluation	CO2	Scenario-based and analytical problems involving identification of software vulnerabilities, assessment of cyber exploitation risks, comparison of security countermeasures, and evaluation of appropriate security solutions
TOTAL	**25**	TS1–TS4	**CO1–CO4**	Units 1–3 only. CO5 and CO6 assessed in ETE only.

11. End Term Examination (ETE) — 60 Marks (All Units, All COs)

ETE is comprehensive — all 5 units and all 6 COs. Full progression from TS1 (recall) through TS6 (evaluation). Minimum 20/50 required to pass.

Section	Marks	Theory Skill Dimensions	COs Assessed	Question Type & Guidance
Section A	20	TS1 — Cyber Security Requirement Analysis TS2 — Software Vulnerability Assessment	CO1, CO2	Short-answer questions on cyber security requirements, organizational threats, vulnerabilities, security posture analysis, software vulnerabilities, cyber exploitation

				risks, and basic security countermeasures
Section B	25	TS3 — Security Monitoring & Troubleshooting Application TS4 — Security Implementation & Forensic Tools TS5 — Risk Management Evaluation	CO3, CO4, CO5	Medium-level analytical and application questions on security monitoring, auditing, troubleshooting techniques, implementation of cyber security solutions, forensic tools, risk assessment, risk treatment methods, and evaluation of security incidents
Section C	15	TS5 — Risk Management Evaluation TS6 — Security Architecture Design	CO5, CO6	Long analytical and evaluative questions involving organizational risk management, risk mitigation strategies, security architecture design, integration of network/system/cloud security, enterprise security case studies, and evaluation of protection frameworks
TOTAL	**60**	TS1–TS6 (all)	**CO1–CO6**	Scaled from 100-mark paper if needed. Minimum 20/50 to pass.

11.1 CO-wise Assessment Instrument Summary

CO	CO Statement (Short)	CA (25)	MTE (25)	ETE (50)	TS	PO Primary
CO1	Analyze organizational cyber security requirements, identify threats/vulnerabilities, and evaluate security posture for protection planning	✓	✓	✓	TS1	PO1, PO2, PO3, PO4
CO2	Determine and assess software vulnerabilities along with suitable security countermeasures and protection mechanisms	✓	✓	✓	TS2	PO1, PO2, PO3, PO4
CO3	Measure cyber security system performance and troubleshoot issues using monitoring, auditing, and diagnostic techniques	✓	✓	✓	TS3	PO1, PO3, PO4, PO5
CO4	Implement cyber security, information assurance, and cyber/computer forensic tools in practical environments	✓	✓	✓	TS4	PO2, PO4, PO9, PO10

CO5	Comprehend and execute risk assessment, risk treatment, and evaluation of risk/performance indicators	✓	—	✓	TS5	PO1, PO2, PO8, PO9, PO10
CO6	Design and develop integrated security architectures using network, system, and cloud security principles	✓	—	✓	TS6	PO1, PO2, PO4, PO10, PO11

CO5 and CO6 are NOT assessed in MTE (only Units 1–3 are covered at mid-semester). They are assessed in CA (self-learning activities) and ETE.

PART III

COMBINED MAPPINGS & REFERENCE

CO–PO Matrix, CO–PO Alignment, Self-Learning Activities, Bloom's Reference, Attendance & Pass/Fail

12. CO–PO and CO–PSO Mapping Matrix (Original Framework)

Strength Scale: 3 = Substantial (High) | 2 = Moderate | 1 = Slight (Low) | – = Not Applicable. Averages computed over non-zero entries only. PO framework as per the original course design.

CO	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PSO1	PSO2	PSO3
CO1	3	3	2	1	-	-	-	-	-	-	3	3	2	1
CO2	3	3	2	2	2	-	-	-	-	-	3	3	3	-
CO3	3	3	2	3	3	2	2	2	2	2	2	3	2	3
CO4	2	2	1	1	2	2	2	2	-	1	2	2	2	2
CO5	2	3	2	2	3	3	2	1	2	2	1	2	2	3
CO6	3	3	3	2	3	3	3	2	2	3	3	3	3	3

Avg	2.67	2.83	2.00	1.83	2.16	1.66	1.5	1.16	1.00	1.33	2.33	2.66	2.33	2.00

13. CO × PO Alignment Map (H/M Indicators — All 6 COs)

CO	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PO12	PSO1	PSO2	PSO3
CO1	H	H	M								H	H	M		H
CO2	H	H	M	M	M						H	H	H		H
CO3	H	H	M	H	H	M	M	M	M	M	M	H	M	H	H
CO4	M	M			M	M	M	M			M	M	M	M	M
CO5	M	H	M	M	H	H	M		M	M		M	M	H	M
CO6	H	H	H	M	H	H	H	M	M	H	H	H	H	H	H

H = High / Primary alignment **M** = Medium / Secondary alignment *Blank = No direct alignment*

14. Self-Learning Activities (SL: 45 Hours)

S.No	Activity	Hours	COs / TS	Evaluation Criteria
1	**Assignment Writing (5 assignments, problem-based, one per unit focus area)**	5 assignments × 3 hrs each Total = 15 hrs	CO1–CO4 TS1–TS4	Evaluated based on the assignment submitted; analyze software vulnerabilities
2	**Mini Literature Review on a Technical Topic**	Video viewing: 7 hrs Report preparation: 7 hrs Presentation: 6 hrs Total = 20 hrs	CO2, CO3 TS2, TS3	Report + Presentation based on video learning outcomes; Measure the performance and troubleshoot cyber security systems

3	**Open-Source Project Contribution (GitHub based)**	Data collection/study: 5 hrs Report preparation: 5 hrs Total = 10 hrs	CO4, CO5, CO6 TS4, TS5, TS6	Evaluated based on in-depth study, technical depth, data collected, fact finding, and analytical conclusions drawn
	TOTAL Self-Learning Hours	**45 hours**	CO1–CO6	All activities are compulsory. Submission deadlines communicated at the start of the semester.

15. Bloom's Taxonomy — Domain Level Reference

Cognitive Domain (6 Levels)	Affective Domain (5 Levels)	Psychomotor Domain — Simpson (7 Levels)
L1 — Remember: Recall facts, definitions, basic concepts L2 — Understand: Explain ideas, concepts, and principles L3 — Apply: Use knowledge to solve problems in new situations L4 — Analyze: Break down information, examine relationships L5 — Evaluate: Judge, justify, assess, and make decisions L6 — Create: Design, develop, and produce new artefacts	A1 — Receiving: Awareness and willingness to attend A2 — Responding: Active participation and reaction A3 — Valuing: Commitment and assigning value to content A4 — Organizing: Integrating values into a personal system A5 — Characterizing: Internalized value system	P1 — Perception: Sensory cues guide motor activity P2 — Set: Mental, physical readiness to act P3 — Guided Response: Practice through imitation/trial P4 — Mechanism: Habitual correct performance P5 — Complex Overt Response: Skilled performance P6 — Adaptation: Modify skills for special situations P7 — Origination: Create new solution patterns

OBE Compliance Statement: This is a theory-only course. All 6 COs are mapped primarily to the Cognitive domain (L1–L5). Psychomotor domain (P3) appears only for CO3 (algorithm implementation as mental tracing). Affective domain (A3) appears for CO4 and CO5, reflecting valuing of algorithmic efficiency.

16. Attendance Policy & Pass / Fail Criteria

16.1 Attendance Policy

Component	Minimum	Applicable To	Consequence
Theory Classes	**75%**	All lecture sessions	Debarred from ETE if below threshold

Self-Learning / Assignment Submission	**All activities**	SL activities (30 hrs)	Incomplete SL affects CA score directly

Theory attendance must meet 75% minimum. Missing SL activities (assignments, video report, case study) directly impacts CA marks and is not compensable by exam performance.

16.2 Pass / Fail Criteria

Condition	Threshold	Status	Remarks
ETE Score	**≥ 24 / 60**	**MANDATORY**	40% of ETE paper required; failing ETE means failing the course regardless of CA + MTE
Overall Total (CA + MTE + ETE)	**≥ 40 / 100**	**Must pass overall**	CA 25 + MTE 25 + ETE 50 = 100; 40% overall minimum required

CSCF3101— Security Threats Intelligence and Risk Management

Theory-Only Course | 6 COs (CO1–CO6) | 3 Assessment Instruments | 6 Theory Skill Dimensions (TS1–TS6)

CO1–CO2: Conceptual / Understand → TS1, TS2 → CA + MTE Sec A + ETE Sec A

CO3–CO4: Apply / Analyze → TS3, TS4 → CA + MTE Sec B + ETE Sec B

CO5–CO6: Analyze / Evaluate → TS5, TS6 → CA + ETE Sec B/C

CA 25 marks + MTE 25 marks + ETE 50 marks = Total 100 marks

COURSE PLAN

Disaster Recovery Management (CSCF3200)

Sharda School of Computing Science & Engineering |B. Tech CSE, Cyber Security & Forensics | Semester V | Batch 2026–2030

Theory-Only Course Plan — All 6 COs (CO1–CO6) | Theory Skill Dimensions TS1–TS6 | CA + MTE + ETE Assessment

PART I

COURSE SYLLABUS

Course Identification, Details, Outcomes, BTL Mapping & Lecture Plan

1. Course Identification

School:	SSCSE- Sharda School of Computing Science & Engineering	**Batch:**	2026 – 2030
Program:	B. Tech	**Current Academic Year:**	2028-29
Branch:	Cyber Security & Forensics	**Semester:**	V
Course Code:	**CSCF3200**	**Course Type:**	Core — Theory Only

2. Course Details

 THEORY-ONLY COURSE — All 6 COs (CO1–CO6) are assessed exclusively via Continuous Assessment (CA), MTE, and ETE. No laboratory component.

S.No	Attribute	Details
1	**Course Code**	**CSCF3200**
2	**Course Title**	**Disaster Recovery Management**
3	**Credits**	3

4	**Contact Hours (L-T-P-SL)**	3-0-0-3 (Theory: 45 hrs. Classroom + 45 hrs. Self-Learning = 90 hrs. total)
5	**Course Status**	**Core — Theory Only (No Laboratory Component)**
6	**Course Objectives**	1.Understanding of the core principles and strategies of Disaster Recovery (DR) through structured lectures and guided assignments. 2. Apply theoretical DR concepts to real-world scenarios, enhancing their analytical and problem-solving skills. 3. Investigate current issues, risks, and challenges in Business Continuity Management (BCM), including technical, organizational, and regulatory aspects. 4. Evaluate key regulations and standards governing BCM practices, enabling them to design compliant and resilient recovery plans.
7	**Course Outcomes (COs)**	**After successful completion of this course, students will be able to:** **CO1 (Understand – L1/L2):** Explain disaster concepts and risk reduction strategies. **CO2 (Understand/Apply – L2/L3):** Illustrate the disaster management cycle and its stages. **CO3 (Apply – L3):** Adapt the knowledge of Business Continuity Management in emergency situations. **CO4 (Analyze – L3/L4):** Summarize the application of the Business Continuity Management development process. **CO5 (Analyze/Evaluate – L4/L5):** Analyze and evaluate research work in the field of emergencies and disaster management, with insight into the role and limitations of science in society. **CO6 (Apply/Analyze – L3/L4):** Demonstrate the capacity to manage public health aspects during disasters.
8	**Course Description**	This course aims to introduce students to the fundamental concepts and techniques in disaster recovery and business continuity management.
9	**Teaching & Learning Scheme**	Classroom Instructions (CI): 45 hrs. | Self Learning (SL): 45 hrs. | Total: 90 hrs.
10	**Mode of Examination**	**Theory Only. CA: 25% | MTE: 15% | ETE: 60% | Total: 100 marks**
11	**Textbook**	1. Michael Wallace and Lawrence Webber, *The Disaster Recovery Handbook: A Step-by-Step Plan to Ensure Business Continuity and Protect Vital Operations, Facilities, and Assets*, 2nd Edition, AMACOM, 2017. 2. Susan Snedaker, *Business Continuity and Disaster Recovery Planning for IT Professionals*, 2nd Edition, Syngress (Elsevier), 2013.
12	**References**	**1. Michael E. Whitman, Herbert J. Mattord, and Andrew Green, *Principles of Incident Response and Disaster Recovery*, 3rd Edition, Cengage Learning, 2018.** *(Useful for incident response, disaster recovery lifecycle, emergency response, recovery operations.)* **2. Harold F. Tipton and Micki Krause, *Information Security Management Handbook*, 6th Edition, Auerbach Publications / CRC Press.** *(Reference for BCM governance, security resilience, organizational continuity.)*

		3. **Ravi Das, *Business Recovery and Continuity in a Mega Disaster: Cybersecurity Lessons Learned from the COVID-19 Pandemic*, Apress, 2022.** *(Ravi Das is an Indian-origin cybersecurity author; this is highly relevant for cyber resilience, BCM, continuity planning, and disaster recovery in cybersecurity contexts.)*

3. Outline Syllabus with CO Mapping

ℹ *All CO mappings in this section refer to Theory COs (CO1–CO6). This is a theory-only course; all assessment is via CA, MTE, and ETE.*

	Topic	CO Mapping
Unit 1	**Introduction to Disaster and Disaster Recovery**	
A	Concepts of hazards, vulnerability, risk, disaster recovery, natural and man-made disasters, rapid onset and slow onset disasters, impact on organizations and critical systems	**CO1**
B	Difference between accidents and disasters, simple and complex disasters, socio-economic and organizational impacts, psychosocial issues, emergency recovery considerations	**CO1, CO6**
C	Relationship between disasters, development, and resilience; stakeholders in disaster recovery; rehabilitation, resettlement, inter-sectoral coordination, recovery models	**CO1, CO2, CO6**
Unit 2	**Disaster Risk Reduction and Preparedness**	
A	Disaster risk reduction strategies, disaster management cycle, preparedness planning, action plans, early warning systems, disaster relief components, community-based resilience	**CO2**
B	Vulnerability assessment, risk analysis, preparedness policies, capacity analysis, public awareness mechanisms, disaster readiness planning	**CO2, CO4**
C	Sustainable disaster recovery management, rehabilitation planning, reconstruction strategies, psychosocial recovery, long-term resilience building	**CO2, CO5, CO6**
Unit 3	**Disaster Recovery Management Cycle and Critical Infrastructure Recovery**	
A	Disaster recovery lifecycle, pre-disaster risk assessment, risk mapping, mitigation planning, business impact analysis, critical infrastructure preparedness	**CO2, CO3**

B	Emergency response, evacuation, communication systems, search and rescue coordination, incident command systems, emergency operations center functions	CO3, CO4, CO6
C	Restoration of critical infrastructure, early recovery, reconstruction, redevelopment, international recovery frameworks and standards	CO3, CO4, CO5
Unit 4	**Business Continuity Management (BCM)**	
A	Introduction, definition, scope, importance of business continuity management in disaster recovery	CO3
B	BCM framework, continuity planning drivers, risk management integration, resilience planning	CO3, CO4
C	Roles, responsibilities, governance, communication plans, continuity teams, stakeholder coordination	CO4, CO5
Unit 5	**Development and Implementation of BCM**	
A	Developing effective BCM capabilities, continuity planning lifecycle, recovery planning, testing and validation	CO4, CO5
B	Software tools and technologies supporting BCM, backup strategies, recovery automation, disaster recovery systems	CO3, CO5
C	BCM implementation case studies, best practices, lessons learned, continuous improvement in disaster recovery planning	CO5, CO6

4. Topic-wise Bloom's Taxonomy Level Mapping

S.No	Topic	L1 Remember	L2 Understand	L3 Apply	L4 Analyze	L5 Evaluate	L6 Create
1	1.A	☐	☐				
2	1.B	☐	☐		☐		
3	1.C	☐	☐	☐	☐		
4	2.A	☐	☐	☐			
5	2.B	☐	☐	☐	☐		
6	2.C	☐	☐	☐	☐	☐	

7	3.A	□	□	□	□		
8	3.B	□	□	□	□		
9	3.C	□	□	□	□	□	
10	4.A	□	□				
11	4.B	□	□	□	□		
12	4.C	□	□	□	□	□	
13	5.A	□	□	□	□	□	□
14	5.B	□	□	□	□	□	
15	5.C	□	□	□	□	□	□

5. CO vs Bloom's Taxonomy — All Three Domains

ℹ *Only strong/dominant alignments are mapped. This is a theory-only course; Psychomotor mapping is limited to Guided Response (P3) for algorithm implementation in CO3. Affective domain appears at A3 (Valuing) for efficiency analysis in CO4 and CO5.*

CO	Cognitive Domain (L1–L6)						Affective (A1–A5)					Psychomotor (P1–P7)						
CO	L1	L2	L3	L4	L5	L6	A1	A2	A3	A4	A5	P1	P2	P3	P4	P5	P6	P7
CO1	□	□					□											
CO2		□	□				□	□					□	□				
CO3		□	□	□				□	□				□	□	□			
CO4			□	□	□				□					□	□			
CO5				□	□	□			□	□				□	□			
CO6		□	□	□	□			□	□				□	□	□			

Legend: □ = Strong / Dominant mapping. Theory-only course: Cognitive domain is primary. Psychomotor (P3) limited to CO3 (algorithm implementation). Affective (A3) for CO4 and CO5 (valuing efficiency).

6. Lecture Plan Outline (Theory — 45 Lectures / 45 Hours)

ℹ *Total classroom contact: 45 hours across 5 units. Self-Learning activities (45 hrs.) are structured separately in Section 11.*

Date	Topics to be Covered/Title	UNIT	Total Lectures
DD/MM/YYYY	Introduction to Disaster Recovery Management and Course Overview	Unit 1	8
DD/MM/YYYY	Concepts of Hazard, Vulnerability, Risk and Disaster Recovery		
DD/MM/YYYY	Natural Disasters: Earthquake, Cyclone, Floods, Volcanoes		
DD/MM/YYYY	Man-Made Disasters and Organizational Impact		
DD/MM/YYYY	Slow Onset and Rapid Onset Disasters		
DD/MM/YYYY	Difference between Accidents and Disasters; Simple vs Complex Disasters		
DD/MM/YYYY	Social, Economic, Gender and Psychosocial Issues in Disasters, Disaster, Development, Stakeholders,		
DD/MM/YYYY	Rehabilitation and Recovery Models		
DD/MM/YYYY	Disaster Risk Reduction Strategies	Unit 2	9
DD/MM/YYYY	Disaster Management Cycle and Disaster Phases		
DD/MM/YYYY	Preparedness Plans, Action Plans and Early Warning Systems		
DD/MM/YYYY	Disaster Relief Components: Water, Food, Shelter, Sanitation, Health		
DD/MM/YYYY	Community-Based DRR and Structural/Non-Structural Measures		
DD/MM/YYYY	Vulnerability Assessment and Risk Analysis		
DD/MM/YYYY	Preparedness Policies, Roles, Responsibilities and Public Awareness		
DD/MM/YYYY	Sustainable Recovery, Reconstruction and Capacity Building		
DD/MM/YYYY	Psychosocial Recovery and Long-Term Resilience Planning		
DD/MM/YYYY	Disaster Recovery Lifecycle and Paradigm Shift	Unit 3	9
DD/MM/YYYY	Risk Assessment, Risk Mapping, Zonation and Micro zonation		
DD/MM/YYYY	Prevention, Mitigation and Business Impact Analysis		
DD/MM/YYYY	Early Warning Systems and Capacity Development		

DD/MM/YYYY	Emergency Response, Evacuation and Disaster Communication		
DD/MM/YYYY	Search & Rescue, Incident Command System, Emergency Operations Centre		
DD/MM/YYYY	Relief, Rehabilitation and Damage Assessment		
DD/MM/YYYY	Critical Infrastructure Restoration and Early Recovery		
DD/MM/YYYY	Reconstruction, Redevelopment and International Frameworks		
DD/MM/YYYY	Introduction, Scope and Importance of BCM		
DD/MM/YYYY	BCM Framework and Core Concepts		
DD/MM/YYYY	Drivers of Business Continuity Management		
DD/MM/YYYY	BCM Risk Management Integration		
DD/MM/YYYY	Organizational Resilience and Recovery Governance	**Unit 4**	**8**
DD/MM/YYYY	Roles and Responsibilities in BCM		
DD/MM/YYYY	Communication Planning and Crisis Coordination		
DD/MM/YYYY	BCM Teams and Stakeholder Management		
DD/MM/YYYY	BCM Policy Development and Recovery Documentation		
DD/MM/YYYY	Developing Effective BCM Capabilities		
DD/MM/YYYY	Business Continuity Planning Lifecycle		
DD/MM/YYYY	Recovery Planning, Testing and Validation		
DD/MM/YYYY	Software Tools Supporting BCM		
DD/MM/YYYY	Backup Strategies and Disaster Recovery Automation	**Unit 5**	**10**
DD/MM/YYYY	Disaster Recovery Systems and Technologies		
DD/MM/YYYY	BCM Best Practices and Real-World Case Studies		
DD/MM/YYYY	Lessons Learned and Continuous Improvement		
DD/MM/YYYY	Lessons Learned and Continuous Improvement		
DD/MM/YYYY	Course Revision / Integrated Case Discussion		

PART II

THEORY ASSESSMENT FRAMEWORK

Theory Skill Dimensions, CO × TS Mapping, CA / MTE / ETE Structure

7. Theory Skill Dimensions (TS1–TS6)

□ THEORY-ONLY COURSE — All 6 COs (CO1–CO6) are assessed exclusively via Continuous Assessment (CA), MTE, and ETE. No laboratory component.

□ *Six Theory Skill Dimensions — one per Bloom's progression (L1–L4) — correspond directly to the six COs. They define precisely what competency is being measured in each section of the CA, MTE, and ETE, providing a clear NBA-auditable assessment rationale.*

ID	Dimension	What is Measured	CO / BTL	Assessment
TS1	Conceptual Recall & Disaster Fundamentals	Recall and explain fundamental concepts of disasters, hazards, vulnerabilities, risks, disaster recovery principles, disaster classifications, and risk reduction terminology	CO1 | L1–L2	CA | MTE Sec A | ETE Sec A
TS2	Disaster Management Interpretation & Preparedness Planning	Explain disaster management cycle, preparedness strategies, risk reduction mechanisms, emergency planning, and community resilience frameworks	CO2 | L2–L3	CA | MTE Sec A | ETE Sec A
TS3	Business Continuity & Recovery Application	Apply business continuity principles, disaster recovery planning methods, infrastructure resilience concepts, continuity frameworks, and emergency response planning	CO3 | L3	CA | MTE Sec B | ETE Sec B
TS4	Disaster Recovery Analysis & Framework Evaluation	Analyze disaster recovery processes, emergency response mechanisms, continuity frameworks, risk assessment outputs, and organizational recovery effectiveness	CO4 | L4–L5	MTE Sec B | ETE Sec B
TS5	Strategic BCM Evaluation & Recovery Planning	Evaluate BCM development processes, continuity capabilities, disaster recovery strategies, organizational resilience planning, and best practices	CO5 | L4–L5	ETE Sec B/C
TS6	Public Health & Operational Disaster Recovery Management	Analyze public health response, psychosocial recovery, emergency coordination, communication systems, operational recovery planning, and rehabilitation mechanisms	CO6 | L3–L5	ETE Sec C

8. CO × Theory Skill Dimension Mapping (6 COs × 6 Dimensions)

ℹ *Each CO maps primarily to one TS dimension (H) with adjacent dimensions receiving secondary mapping (M), reflecting the progressive Bloom's structure of this course.*

CO	TS1 Conceptual Recall	TS2 Process Interpretation	TS3 Algorithmic Application	TS4 Performance Evaluation	TS5 Memory System Analysis	TS6 File & Disk Evaluation
CO1	H	M				
CO2	M	H	M			
CO3		M	H	M		
CO4			M	H	M	
CO5				M	H	M
CO6		M		M		H

H = High / Primary alignment **M** = Medium / Secondary alignment *Blank = No direct alignment*

9. Continuous Assessment (CA) — 25 Marks

□ *CA is formative and covers COs progressively as the syllabus is taught. It includes numerical-based assignments, a technical video learning report, and a real-world case study — mirroring TS1 through TS6.*

9.1 CA Component Breakdown (Sample)

Component	Quantum	Marks	COs Assessed	Skill Dimensions
Assignments 1–5 (Conceptual / Case-based / Planning Exercises)	5 Assignments	15	CO1, CO2, CO3, CO4	CO1, CO2, CO3, CO4
Technical Video Learning Report + Presentation	1 Report + Presentation	5	CO2, CO3, CO4	TS2, TS3, TS4
Real-World Disaster Recovery / BCM Case Study Report	1 Report	5	CO4, CO5, CO6	CO4, CO5, CO6
TOTAL	—	25	CO1–CO6	TS1–TS6

9.2 Assignment-wise CO & TS Mapping

Item	Topic / Focus	COs	TS Dims	SL Hours	Evaluation Criteria
Assignment 1	Disaster fundamentals: hazards, vulnerabilities, risks, disaster classifications, disaster recovery concepts	CO1	TS1	5 hrs.	Conceptual understanding, terminology accuracy, disaster scenario interpretation
Assignment 2	Disaster management cycle, preparedness planning, risk reduction strategies, emergency planning	CO2	TS2	5 hrs.	Preparedness planning, disaster cycle interpretation, structured response design
Assignment 3	Business continuity management, disaster recovery planning, infrastructure resilience, continuity frameworks	CO3	TS3	5 hrs.	BCM application, recovery planning logic, continuity strategy formulation
Assignment 4	Disaster recovery framework analysis, emergency response evaluation, continuity process assessment	CO4	TS4	5 hrs.	Analytical reasoning, framework comparison, response effectiveness evaluation
Assignment 5	BCM development strategies, organizational recovery capability, public health operational recovery analysis	CO5, CO6	TS5, TS6	5 hrs.	Strategic evaluation, operational recovery analysis, recommendations
Video Learning Report	Technical video on disaster recovery, BCM implementation, emergency response frameworks, resilience planning (minimum 3 hrs)	CO2, CO3, CO4	TS2, TS3, TS4	9 hrs.	Report on learning outcomes, concept understanding, BCM/disaster recovery insights, self-reflection; Presentation (10 min)
Case Study Report	Real-world disaster recovery / BCM case study (e.g., COVID business continuity, cyberattack recovery, infrastructure disruption, disaster response failure/success)	CO4, CO5, CO6	TS4, TS5, TS6	11 hrs.	Technical depth, case investigation, factual analysis, recovery evaluation, mitigation recommendations

10. Mid Term Examination (MTE) — 15 Marks (Units 1–3)

ℹ *MTE covers Units 1–3 (CO1, CO2, CO3, CO4). CO5 and CO6 are assessed in ETE only. MTE maps to TS1–TS4.*

Section	Marks	Theory Skill Dimensions	COs Assessed	Question Type & Guidance
Section A	**10**	TS1 — Conceptual Recall & Disaster Fundamentals TS2 — Disaster Management & Preparedness Planning	**CO1, CO2**	**Short-answer questions:** disaster definitions, hazard/vulnerability concepts, disaster classifications, risk reduction strategies, disaster management cycle, preparedness planning, emergency concepts
Section B	**15**	TS3 — BCM & Recovery Application TS4 — Recovery Analysis & Framework Evaluation	**CO2, CO3, CO4**	**Analytical/application questions:** disaster recovery planning, emergency response scenarios, business continuity concepts, framework comparison, disaster communication, critical infrastructure recovery
TOTAL	**25**	**TS1–TS4**	**CO1–CO4**	**Units 1–3 only. CO5 and CO6 assessed in ETE only.**

11. End Term Examination (ETE) — 60 Marks (All Units, All COs)

ℹ *ETE is comprehensive — all 5 units and all 6 COs. Full progression from TS1 (recall) through TS6 (evaluation). Minimum 20/50 required to pass.*

Section	Marks	Theory Skill Dimensions	COs Assessed	Question Type & Guidance
Section A	15	TS1 — Conceptual Recall & Disaster Fundamentals TS2 — Disaster Management & Preparedness Planning	CO1, CO2	**Short questions (all units):** definitions, frameworks, BCM concepts, disaster recovery terminology, preparedness principles, emergency response concepts
Section B	25	TS3 — BCM & Recovery Application TS4 — Recovery Analysis & Framework Evaluation TS5 — Strategic BCM Evaluation	CO3, CO4, CO5	**Medium analytical questions:** disaster recovery planning, business continuity framework application, risk analysis, BCM development, continuity strategy evaluation, recovery planning scenarios
Section C	10	TS5 — Strategic BCM Evaluation	CO5, CO6	**Long/evaluation questions:** BCM case analysis, organizational resilience evaluation, public health disaster

		TS6 — Public Health & Operational Recovery		response, rehabilitation strategies, disaster recovery case studies
TOTAL	50	TS1–TS6 (all)	CO1–CO6	Scaled from 100-mark paper if needed. Minimum 20/50 to pass.

11.1 CO-wise Assessment Instrument Summary

CO	CO Statement (Short)	CA (25)	MTE (25)	ETE (50)	TS	PO Primary
CO1	Explain disaster concepts, hazards, vulnerabilities, risks, and disaster recovery fundamentals	□	□	□	TS1	PO1, PO2
CO2	Illustrate disaster management cycle, preparedness planning, and risk reduction strategies	□	□	□	TS2	PO1, PO2, PO3
CO3	Apply principles of business continuity management and disaster recovery planning	□	□	□	TS3	PO1, PO3, PO5
CO4	Analyze disaster recovery frameworks, emergency response mechanisms, and continuity processes	□	□	□	TS4	PO2, PO4, PO5
CO5	Evaluate BCM development strategies, disaster recovery capabilities, and organizational resilience	□	—	□	TS5	PO3, PO4, PO12
CO6	Examine public health, communication, and operational recovery aspects during disasters	□	—	□	TS6	PO2, PO6, PO8

□ *CO5 and CO6 are NOT assessed in MTE (only Units 1–3 is covered at mid-semester). They are assessed in CA (self-learning activities) and ETE.*

PART III

COMBINED MAPPINGS & REFERENCE

CO–PO Matrix, CO–PO Alignment, Self-Learning Activities, Bloom's Reference, Attendance & Pass/Fail

12. CO–PO and CO–PSO Mapping Matrix (Original Framework)

Strength Scale: 3 = Substantial (High) | 2 = Moderate | 1 = Slight (Low) | = Not Applicable. Averages computed over non-zero entries only. PO framework as per the original course design.

CO	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PSO1	PSO2	PSO3
CO1	3	2	-	-	-	2	2	-	-	-	2	-	-	3
CO2	3	3	-	2	-	2	2	1	-	-	2	-	-	3
CO3	3	-	-	-	2	-	-	-	-	2	2	2	-	3
CO4	-	-	2	-	2	-	-	-	2	2	-	2	-	-
CO5	3	3	-	2	-	2	3	2	-	2	3	3	-	3
CO6	2	-	-	2	-	3	3	-	2	-	2	2	2	2
Avg	2.80	2.67	2.00	2.00	2.00	2.25	2.50	1.50	2.00	2.00	2.20	2.25	2.00	2.80

13. CO × PO Alignment Map (H/M Indicators — All 6 COs)

CO	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PSO1	PSO2	PSO3
CO1	H	M				M	M				M			H
CO2	H	H		M		M	M				M			H
CO3	H				M					M	M	M		H
CO4			M		M				M	M		M		

CO5	H	H		M		M	H	M		M	H	H		H
CO6	M			M		H	H		M		M	M	M	M

H = High / Primary alignment **M** = Medium / Secondary alignment *Blank = No direct alignment*

14. Self-Learning Activities (SL: 45 Hours)

S.No	Activity	Hours	COs / TS	Evaluation Criteria
1	Technical Video-Based Learning related to Disaster Recovery / BCM / Emergency Management (e.g., disaster response case documentaries, BCM implementation, crisis management, cyber disaster recovery, public health emergency response)	**Total = 15 hrs.**	CO2, CO3, CO4 TS2, TS3, TS4	Report + presentation based on learning outcomes, disaster preparedness concepts, BCM understanding, recovery planning insights, case interpretation, and self-reflection
2	Real-World Case Study Analysis (e.g., COVID continuity management, flood recovery planning, earthquake emergency response, cyberattack recovery, healthcare disaster response)	**Total = 15 hrs.**	CO4, CO5, CO6 TS4, TS5, TS6	Evaluated based on technical depth, disaster recovery analysis, factual investigation, strategic evaluation, public health recovery understanding, and mitigation recommendations
3	Technical Video-Based Learning related to Disaster Recovery / BCM / Emergency Management (e.g., disaster response case documentaries, BCM implementation, crisis management, cyber disaster recovery, public health emergency response)	**Total = 15 hrs.**	CO2, CO3, CO4 TS2, TS3, TS4	Report + presentation based on learning outcomes, disaster preparedness concepts, BCM understanding, recovery planning insights, case interpretation, and self-reflection
	TOTAL Self-Learning Hours	45 Hours	CO1–CO6	All activities are compulsory. Submission deadlines communicated at the start of the semester.

15. Bloom's Taxonomy — Domain Level Reference

Cognitive Domain (6 Levels)	Affective Domain (5 Levels)	Psychomotor Domain — Simpson (7 Levels)

L1 — Remember: Recall facts, definitions, basic concepts L2 — Understand: Explain ideas, concepts, and principles L3 — Apply: Use knowledge to solve problems in new situations L4 — Analyze: Break down information, examine relationships L5 — Evaluate: Judge, justify, assess, and make decisions L6 — Create: Design, develop, and produce new artefacts	A1 — Receiving: Awareness and willingness to attend A2 — Responding: Active participation and reaction A3 — Valuing: Commitment and assigning value to content A4 — Organizing: Integrating values into a personal system A5 — Characterizing: Internalized value system	P1 — Perception: Sensory cues guide motor activity P2 — Set: Mental, physical readiness to act P3 — Guided Response: Practice through imitation/trial P4 — Mechanism: Habitual correct performance P5 — Complex Overt Response: Skilled performance P6 — Adaptation: Modify skills for special situations P7 — Origination: Create new solution patterns

 OBE Compliance Statement: This is a theory-only course. All 6 COs are mapped primarily to the Cognitive domain (L1–L5). Psychomotor domain (P3) appears only for CO3 (algorithm implementation as mental tracing). Affective domain (A3) appears for CO4 and CO5, reflecting valuing of algorithmic efficiency.

16. Attendance Policy & Pass / Fail Criteria

16.1 Attendance Policy

Component	Minimum	Applicable To	Consequence
Theory Classes	**75%**	All lecture sessions	Debarred from ETE if below threshold
Self-Learning / Assignment Submission	**All activities**	SL activities (45 hrs.)	Incomplete SL affects CA score directly

 Theory attendance must meet 75% minimum. Missing SL activities (assignments, video report, case study) directly impacts CA marks and is not compensable by exam performance.

16.2 Pass / Fail Criteria

Condition	Threshold	Status	Remarks
ETE Score	≥ 24 / 60	**MANDATORY**	40% of ETE paper required; failing ETE means failing the course regardless of CA + MTE
Overall Total (CA + MTE + ETE)	≥ 40 / 100	**Must pass overall**	CA 25 + MTE 25 + ETE 50 = 100; 40% overall minimum required

CSCF3200— Disaster Recovery Management

Theory-Only Course | 6 COs (CO1–CO6) | 3 Assessment Instruments | 6 Theory Skill Dimensions (TS1–TS6)

CO1–CO2: Conceptual / Understand → TS1, TS2 → CA + MTE Sec A + ETE Sec A

CO3–CO4: Apply / Analyze → TS3, TS4 → CA + MTE Sec B + ETE Sec B

CO5–CO6: Analyze / Evaluate → TS5, TS6 → CA + ETE Sec B/C

CA 25 marks + MTE 25 marks + ETE 50 marks = Total 100 marks

COURSE PLAN

Mobile and Wireless Security (CSCF3201)

Sharda School of Computing Science & Engineering | B.Tech CSE | Semester V | Batch 2025–2029

Theory-Only Course Plan — All 6 COs (CO1–CO6) | Theory Skill Dimensions TS1–TS6 | CA + MTE + ETE Assessment

PART I

COURSE SYLLABUS

Course Identification, Details, Outcomes, BTL Mapping & Lecture Plan

1. Course Identification

School:	SSCSE-Sharda School of Computing Science & Engineering	**Batch:**	2026-2030
Program:	B.Tech	**Current Academic Year:**	2026-30
Branch:	CSE	**Semester:**	V
Course Code:	CSCF3201	**Course Type:**	Theory Only

2. Course Details

THEORY-ONLY COURSE — All 6 COs (CO1–CO6) are assessed exclusively via Continuous Assessment (CA), MTE, and ETE. No laboratory component.

S.No	Attribute	Details
1	**Course Code**	**CSCF3201**
2	**Course Title**	**Mobile and Wireless Security**
3	**Credits**	3
4	**Contact Hours (L-T-P-SL)**	3-0-0-3 (Theory: 45 hrs Classroom + 45 hrs Self Learning = 90 hrs total)
5	**Course Status**	**Core — Theory Only (No Laboratory Component) Elective**
6	**Course Objectives**	1. Here are the Course Objectives tailored for your syllabus, matching the tone, depth, and structured format of your reference example: 2. Introduce the fundamentals of wireless networking principles, information theory distinctions between wired and wireless mediums, and the structural challenges posed by mobility in ad-hoc and sensor networks. 3. Provide knowledge of vulnerabilities inherent to wireless architectures, 802.11 protocols, broadcast mediums, and the foundational design of secure routing, localization, and cryptographic key pre-distribution mechanisms. 4. Develop the ability to analyze wireless network threats, including source authentication failures, selfishness issues, power exploitation, and denial-of-service (DoS/DDoS) attack vectors within sensor environments. 5. Enable students to design and implement robust client-server architectures using socket programming, handling concurrent processing, low-level system calls, multi-threading, and remote procedure calls. 6. Familiarize students with next-generation internet protocols by examining advanced IPv6 features, stateless auto-configuration, cross-protocol tunneling, and translation techniques to bridge legacy and modern network ecosystems.
7	**Course Outcomes (COs)**	**After successful completion of this course, students will be able to:** CO1 (Understand – L1/L2) Identify and understand the fundamental distinctions between wired and wireless networks from an information theory perspective, the impacts of mobility, and the core structural architectures of MANETs and Wireless Sensor Networks (WSNs). CO2 (Explore – L2/L3) Explore the specific security vulnerabilities inherent in wireless protocols (802.11, Satellite, IP broadcast), the cross-layer impacts on the IP stack from the MAC layer up, and the advanced architectural features of IPv6. CO3 (Apply – L3) Apply secure protocol design principles to achieve resilient routing, localization, and data aggregation, while implementing robust source authentication, non-repudiation, and key pre-distribution mechanisms. CO4 (Analyze – L4) Analyze and implement low-level network communication interfaces using socket programming, handling byte ordering, concurrent client-server system calls, and multi-threaded TCP/UDP architectures.

		CO5 (Analyze – L4/L5) Analyze wireless-specific network threats, including DoS/DDoS vectors, power management exploitation, and node selfishness, while evaluating adaptive information-processing and defense reactions in sensor environments. CO6 (Evaluate – L5)Evaluate and compare next-generation internet protocol mechanisms, including IPv6 routing protocols, IPv4-to-IPv6 translation/tunneling techniques, and secure group communication efficiency.
8	**Course Description**	This course introduces the fundamental security challenges, protocols, and architectural principles of mobile and wireless networks. It covers the distinction between wired and wireless information theory, the impact of mobility on network performance, and secure communication in MANETs and Wireless Sensor Networks (WSNs). The course provides technical exposure to socket programming for concurrent client-server software, source authentication, and cryptographic key management. Furthermore, it explores defense mechanisms against wireless-specific threats like DoS/DDoS and selfishness issues, while providing a deep dive into next-generation internet protocols, specifically IPv6 features, tunneling, and translation techniques to secure heterogeneous network environments.
9	**Teaching & Learning Scheme**	Classroom Instructions (CI): 45 hrs | Self Learning (SL): 45 hrs | Total: 90 hrs
10	**Mode of Examination**	**Theory Only. CA: 25% | MTE: 15% | ETE: 60% | Total: 100 marks**
11	**Textbook**	Douglas E. Comer," Internetworking with TCP/IP, Principles, Protocols, and Architecture", Addison-Wesley, 5th edition, Vol 1. 2005.
12	**References**	1. Behrouz A. Forouzan, "Data Communications and Networking", McGraw-Hill, 5th edition, 2012 2. Wendell Odom, "CCNP Route 642-902, CCIE", Official Certification Guide, Pearson education, 2010.

3. Outline Syllabus with CO Mapping

All CO mappings in this section refer to Theory COs (CO1–CO6). This is a theory-only course; all assessment is via CA, MTE, and ETE.

	Topic	CO Mapping
	Unit 1: Wireless Network Basics:	
A	Distinction between wired and wireless networks from information theory;	**CO1**

B	Effect of mobility on networks & systems - Mobile Ad Hoc Networks - Wireless Sensor Networks - Location Discovery	CO1,CO2
C	In-Network Processing - Routing - Energy Efficiency - Clustering	CO1, CO4
	Unit 2: Security in Wireless Networks	
A	Issues of security in wireless; IP broadcast, Satellite broadcast; issues of information capacity; issues of 802.11 protocols;	CO1, CO3
B	design of secure protocols; Secure routing - Secure localization - Secure and resilient data aggregation - Key pre-distribution and management	CO2, CO4
C	Encryption and authentication - Security in group communication - Impact on IP stack from MAC layer and up	CO2, CO5
	Unit 3: Source authentication	
A	Source authentication of transmissions, and non-repudiation;	CO2, CO3
B	Power management and selfishness issues, attacks in wireless networks;	CO3, CO4
C	DOS and DDOS attacks, reaction to attacks, information processing for sensor networks.	CO3, CO6
	Unit 4: Socket Programming	
A	Introduction to Socket Programming- Concurrent Processing in Client-Server Software-Byte ordering and address conversion functions	CO3,CO4
B	Socket Interface - System calls used with sockets - Iterative server and concurrent server- Multi protocol and Multi service server- TCP/UDP Client server programs	CO4
C	Thread Creation and Termination – TCP Echo Server using threads- Remote Procedure Call.	CO4, CO5
	Unit 5: Next Generation Internet Protocol	
A	Introduction to IPv6 – IPv6 Advanced Features –V4 and V6 header comparison	CO5, CO6
B	V6 Address types –Stateless auto configuration	CO5, CO6
C	IPv6 routing protocols – IPV4- V6 Tunneling and Translation Techniques.	CO5, CO6

4. Topic-wise Bloom's Taxonomy Level Mapping

S.No	Topic	L1 Remember	L2 Understand	L3 Apply	L4 Analyze	L5 Evaluate	L6 Create
1	1.A	□	□				
2	1.B	□	□				
3	1.C		□				
4	2.A		□	□			
5	2.B		□	□			
6	2.C			□	□		
7	3.A	□	□				
8	3.B		□	□	□		
9	3.C			□	□	□	
10	4.A		□				
11	4.B		□	□	□		□
12	4.C			□	□	□	
13	5.A		□	□			□
14	5.B			□	□		
15	5.C		□	□	□		□

5. CO vs Bloom's Taxonomy — All Three Domains

□ *Only strong/dominant alignments are mapped. This is a theory-only course; Psychomotor mapping is limited to Guided Response (P3) for algorithm implementation in CO3. Affective domain appears at A3 (Valuing) for efficiency analysis in CO4 and CO5.*

CO	Cognitive Domain (L1–L6)						Affective (A1–A5)					Psychomotor (P1–P7)						
CO	L1	L2	L3	L4	L5	L6	A1	A2	A3	A4	A5	P1	P2	P3	P4	P5	P6	P7
CO1	□	□																
CO2		□	□															
CO3			□	□											□			
CO4				□	□				□									
CO5				□	□			□										
CO6		□	□	□														

Legend: □ = Strong / Dominant mapping. Theory-only course: Cognitive domain is primary. Psychomotor (P3) limited to CO3 (algorithm implementation). Affective (A3) for CO4 and CO5 (valuing efficiency).

6. Lecture Plan Outline (Theory — 45 Lectures / 45 Hours)

□ *Total classroom contact: 45 hours across 5 units. Self-Learning activities (45 hrs) are structured separately in Section 11.*

Date	Topics to be Covered/Title	UNIT	Total Lectures
DD/MM/YY	Introduction to Information Theory: Channel capacity, bandwidth, and noise constraints.	UNIT-1	9

DD/MM/YY	Fundamental Distinctions: Structural and theoretical differences between wired and wireless mediums.		
DD/MM/YY	Impact of Mobility: How node movement affects network topology, link stability, and system performance.		
DD/MM/YY	Mobile Ad Hoc Networks (MANETs): Architecture, self-configuring characteristics, and design challenges.		
DD/MM/YY	Wireless Sensor Networks (WSNs): Sensor node architecture, constraints (power, memory), and applications.		
DD/MM/YY	Location Discovery: Localization techniques, GPS dependency vs. anchor-based and anchor-free positioning algorithms.		
DD/MM/YY	In-Network Processing: Data aggregation, compression, and reducing redundant transmissions within WSNs.		
DD/MM/YY	Wireless Routing Protocols: Proactive, reactive, and hybrid routing strategies for dynamic topologies.		
DD/MM/YY	Energy Efficiency & Clustering: Energy-aware design and cluster-head election mechanisms (e.g., LEACH protocol)		
DD/MM/YY	Wireless Security Vulnerabilities: Open broadcast nature, eavesdropping, and physical layer vulnerabilities.	UNIT-2	9
DD/MM/YY	Broadcast Medium Issues: Risks and security challenges inherent to IP broadcast and Satellite broadcast networks.		
DD/MM/YY	Information Capacity Constraints: Balancing security overhead (encryption/headers) with limited wireless channel capacity.		
DD/MM/YY	802.11 Protocol Vulnerabilities: Weaknesses in WEP, WPA, WPA2, and WPA3 standard architectures.		
DD/MM/YY	Secure Routing Design: Mitigating routing attacks (sinkhole, wormhole, blackhole) in ad-hoc environments.		
DD/MM/YY	Secure Localization: Protecting location discovery against spoofing, replay attacks, and malicious anchor nodes.		
DD/MM/YY	Secure and Resilient Data Aggregation: Ensuring data integrity during in-network processing against compromised aggregator nodes.		
DD/MM/YY	Key Pre-distribution and Management: Cryptographic key distribution models for resource-constrained sensor networks.		
DD/MM/YY	Cross-Layer Security Impacts: How MAC layer behavior and security vulnerabilities propagate up the IP stack.		
DD/MM/YY	Source Authentication Foundations: Methods to verify sender identity over wireless transmissions.	UNIT-3	9
DD/MM/YY	Non-Repudiation Mechanisms: Ensuring accountability and preventing transmission denial in wireless systems.		
DD/MM/YY	Power Management Exploitation: Attacks targeting the sleep-wake cycles of resource-constrained nodes.		
DD/MM/YY	Node Selfishness: Misbehavior where nodes refuse to forward packets to conserve their own energy.		
DD/MM/YY	Incentives & Cooperation: Protocols for enforcing cooperation and penalizing selfish nodes (e.g., reputation systems).		
DD/MM/YY	Wireless DoS Attacks: Jamming at the physical layer and collision generation at the MAC layer.		

DD/MM/YY	Wireless DDoS Vectors: Distributed flooding attacks, resource exhaustion, and routing table overflow.		
DD/MM/YY	Reaction to Attacks: Intrusion detection, node isolation, and dynamic reconfiguration strategies in wireless networks.		
DD/MM/YY	Information Processing for Sensor Defense: Utilizing localized data analysis to detect anomalies and sensor tampering.		
DD/MM/YY	Introduction to Socket Programming: The network abstraction layer, socket types (Stream vs. Datagram), and descriptors.	UNIT-4	9
DD/MM/YY	Byte Ordering & Data Marshaling: Handling Big-Endian vs. Little-Endian formats using network-to-host (ntohs/ntohl) and host-to-network (htons/htonl) functions.		
DD/MM/YY	Address Conversion & Structures: Manipulating IP addresses using sockaddr_in, inet_pton, and inet_ntop.		
DD/MM/YY	Core Socket System Calls: Deep dive into socket(), bind(), listen(), accept(), connect(), send(), and recv().		
DD/MM/YY	Iterative Client-Server Software: Architecture and limitations of handling one connection at a time.		
DD/MM/YY	Concurrent Server Implementations: Multi-processing servers using fork() and handling zombie processes.		
DD/MM/YY	Multi-Protocol and Multi-Service Servers: Designing servers capable of handling both TCP/UDP or managing multiple network ports concurrently.		
DD/MM/YY	Thread Creation and Management: POSIX threads (pthread_create, pthread_join, pthread_detach) for lightweight server concurrency.		
DD/MM/YY	Multi-threaded TCP Echo Server & RPC: Building a production-ready echo server using threads, followed by an introduction to Remote Procedure Calls.		
DD/MM/YY	Introduction to IPv6: Limitations of IPv4, driver factors for adoption, and the IPv6 address space layout.	UNIT-5	9
DD/MM/YY	Advanced IPv6 Features: Simplified header format, extension headers, flow labeling, and built-in security (IPsec).		
DD/MM/YY	Header Comparison: Side-by-side analysis of IPv4 and IPv6 fields, noting removed, renamed, and modified elements.		
DD/MM/YY	IPv6 Address Architecture: Unicast, Anycast, and Multicast configurations (and the elimination of Broadcast).		
DD/MM/YY	Stateless Address Autoconfiguration (SLAAC): How nodes discover networks and generate addresses using Neighbor Discovery Protocol (NDP).		
DD/MM/YY	State Management: Comparing SLAAC with Stateful configuration (DHCPv6) and link-local address generation.		
DD/MM/YY	IPv6 Routing Protocols: Adaptations of routing standards for IPv6, including RIPng, OSPFv3, and MP-BGP.		
DD/MM/YY	Coexistence Strategies - Tunneling: Encapsulating IPv6 packets inside IPv4 headers (e.g., 6to4, Teredo).		
DD/MM/YY	Coexistence Strategies - Translation: Protocol translation mechanisms like NAT64/DNS64 to bridge heterogeneous IPv4/IPv6 networks.		

PART II

THEORY ASSESSMENT FRAMEWORK

Theory Skill Dimensions, CO × TS Mapping, CA / MTE / ETE Structure

7. Theory Skill Dimensions (TS1–TS6)

THEORY-ONLY COURSE — All 6 COs (CO1–CO6) are assessed exclusively via Continuous Assessment (CA), MTE, and ETE. No laboratory component.

Six Theory Skill Dimensions — one per Bloom's progression (L1–L4) — correspond directly to the six COs. They define precisely what competency is being measured in each section of the CA, MTE, and ETE, providing a clear NBA-auditable assessment rationale.

ID	Dimension	What is Measured	CO / BTL	Assessment
TS1	Foundations & Wireless Theory	Recall information theory distinctions and wireless architectures; identify mobility impacts on MANETs and WSNs.	CO1 | L1–L2	CA | MTE Sec A | ETE Sec A
TS2	Protocol Vulnerability Interpretation	Explain 802.11, Satellite, and Broadcast vulnerabilities; interpret header structures and MAC-to-IP stack security impacts.	CO2 | L2–L3	CA | MTE Sec A | ETE Sec A
TS3	Secure Protocol Application	Apply principles of secure routing, localization, and data aggregation; implement authentication and non-repudiation mechanisms.	CO3 | L3	CA | MTE Sec B | ETE Sec B
TS4	Socket Interface & Traffic Analysis	Analyze network communication using socket system calls; evaluate concurrent processing, byte ordering, and thread management.	CO4 | L4	MTE Sec B | ETE Sec B
TS5	Threat Modeling & Attack Analysis	Analyze wireless threats including DoS/DDoS, power management exploitation, and node selfishness/incentive mechanisms.	CO5 | L4–L5	ETE Sec B/C
TS6	Next-Gen Strategy & Case Evaluation	Evaluate IPv6 features, routing protocols, and tunneling/translation techniques; apply strategies to heterogeneous network cases.	CO6 | L2–L5	ETE Sec C

8. CO × Theory Skill Dimension Mapping (6 COs × 6 Dimensions)

Each CO maps primarily to one TS dimension (H) with adjacent dimensions receiving secondary mapping (M), reflecting the progressive Bloom's structure of this course.

CO	TS1 Conceptual Recall	TS2 Process Interpretation	TS3 Algorithmic Application	TS4 Performance Evaluation	TS5 Memory System Analysis	TS6 File & Disk Evaluation
CO1	H	M				
CO2	M	H	M			
CO3		M	H	M		
CO4			M	H	M	
CO5				M	H	M
CO6		M		M	M	H

H = High / Primary alignment M = Medium / Secondary alignment Blank = No direct alignment

9. Continuous Assessment (CA) — 25 Marks

CA is formative and covers COs progressively as the syllabus is taught. It includes numerical-based assignments, a technical video learning report, and a real-world case study — mirroring TS1 through TS6.

9.1 CA Component Breakdown (Sample)

Component	Quantum	Marks	COs Assessed	Skill Dimensions
Assignments 1–5 (Analysis Problem-based)	5 assignments	**15**	CO1, CO2, CO3, CO4	TS1, TS2, TS3, TS4

Technical Video Learning Report	1 Report + Presentation	**5**	CO2, CO3	TS2, TS3
Real-World Case Study (Report)	1 Report	**5**	CO4, CO5, CO6	TS4, TS5, TS6
TOTAL	—	**25**	CO1–CO6	TS1–TS6

9.2 Assignment-wise CO & TS Mapping

Item	Topic / Focus	COs	TS Dims	SL Hours	Evaluation Criteria
Assignment 1	Unit 1 Fundamentals: Wireless channel theory, mobility impacts, and WSN/MANET architecture distinctions.	CO1	TS1	8h SL	Report submission + conceptual evaluation
Assignment 2	Protocol Analysis: Interpreting 802.11 frames, broadcast vulnerabilities, and MAC-to-IP stack impacts.	CO2	TS2	8h SL	Technical report on protocol structure & vulnerabilities
Assignment 3	Secure Protocols: Implementing secure routing and localization algorithms for ad-hoc environments.	CO3	TS3	8h SL	Simulation results + behavioral trace analysis
Assignment 4	Socket Programming: Developing concurrent TCP/UDP servers and handling byte-ordering/multi-threading.	CO3, CO4	TS3, TS4	8h SL	Source code quality + socket communication report
Assignment 5	Attack & Defense: Analyzing DoS/DDoS vectors in wireless nodes and evaluating reaction strategies.	CO4, CO5	TS4, TS5	8h SL	Comparative analysis of mitigation mechanisms
Video Learning Report	Next-Gen IPv6: Technical video on IPv6 routing, tunneling, or SLAAC (min 3 hrs); structured report + presentation.	CO5, CO6	TS5, TS6	5h SL	Report: learning outcomes, key concepts, self-reflection. Presentation: 10 min

10. Mid Term Examination (MTE) — 15 Marks (Units 1–3)

MTE covers Units 1–3 (CO1, CO2, CO3, CO4). CO5 and CO6 are assessed in ETE only. MTE maps to TS1–TS4.

Section	Marks	Theory Skill Dimensions	COs Assessed	Question Type & Guidance
Section A	10	TS1 — Foundations & Wireless Theory TS2 — Protocol Vulnerability Interpretation	CO1, CO2	Short-answer: Define wireless channel constraints, explain the difference between MANETs and WSNs, identify 802.11 protocol weaknesses, and describe the impact of mobility on network stability.
Section B	15	TS3 — Secure Protocol Application TS4 — Socket Interface & Traffic Analysis	CO2, CO3, CO4	Analytical problems: Design a secure routing mechanism for a given topology; apply key pre-distribution logic; interpret socket system call sequences for client-server communication; analyze 802.11 packet headers for security markers.
TOTAL	25	TS1–TS4	CO1–CO4	Units 1–3 only. CO5 (Threat Modeling) and CO6 (Next-Gen Protocols) assessed in ETE only.

11. End Term Examination (ETE) — 60 Marks (All Units, All COs)

ETE is comprehensive — all 5 units and all 6 COs. Full progression from TS1 (recall) through TS6 (evaluation). Minimum 20/50 required to pass.

Section	Marks	Theory Skill Dimensions	COs Assessed	Question Type & Guidance
Section A	15	TS1 — Foundations & Wireless TheoryTS2 — Protocol Vulnerability Interpretation	CO1, CO2	Short questions (all units): Definitions of MANET/WSN architectures, information theory limits, 802.11 header components, and IPv6 address types.
Section B	35	TS3 — Secure Protocol ApplicationTS4 — Socket Interface & Traffic AnalysisTS5 — Threat Modeling & Attack Analysis	CO3, CO4, CO5	Medium questions: Designing secure data aggregation; tracing multi-threaded socket server logic; analyzing packet captures for DoS/DDoS markers; and explaining energy-exhaustion attacks.

Section C	10	TS5 — Threat Modeling & Attack AnalysisTS6 — Next-Gen Strategy & Case Evaluation	CO5, CO6	Long/evaluation questions: Comparing IPv4-to-IPv6 transition strategies (Tunneling vs. Translation); evaluating the efficiency of key management in heterogeneous networks; and case study analysis of sensor network defenses.
TOTAL	60	TS1–TS6 (all)	CO1–CO6	Scaled from 100-mark paper if needed. Covers full course lifecycle from wireless basics to advanced secure networking protocols.

11.1 CO-wise Assessment Instrument Summary

CO	CO Statement (Short)	CA (25)	MTE (25)	ETE (50)	TS	PO Primary
CO1	Understand wireless taxonomy, mobility impacts, and basic architectures (MANETs/WSNs)	✓	✓	✓	TS1	PO1, PO2, PO3, PO4
CO2	Interpret protocol vulnerabilities (802.11), broadcast issues, and IPv6 structural features	✓	✓	✓	TS2	PO1, PO3, PO4
CO3	Apply secure design for routing, localization, and source authentication mechanisms	✓	✓	✓	TS3	PO1, PO2, PO3, PO4
CO4	Analyze network communication via socket programming and concurrent server logic	✓	✓	✓	TS4	PO9, PO10, PO11
CO5	Analyze wireless threats including DoS/DDoS, power exploitation, and selfishness	✓	—	✓	TS5	PO1, PO2, PO8, PO9, PO10
CO6	Evaluate next-gen routing, tunneling strategies, and secure group communication cases	✓	—	✓	TS6	PO1, PO2, PO10, PO11

CO5 and CO6 are NOT assessed in MTE (only Units 1–3 are covered at mid-semester). They are assessed in CA (self-learning activities) and ETE.

PART III

COMBINED MAPPINGS & REFERENCE

CO–PO Matrix, CO–PO Alignment, Self-Learning Activities, Bloom's Reference, Attendance & Pass/Fail

12. CO–PO and CO–PSO Mapping Matrix (Original Framework)

Strength Scale: 3 = Substantial (High) | 2 = Moderate | 1 = Slight (Low) | – = Not Applicable. Averages computed over non-zero entries only. PO framework as per the original course design.

CO	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PSO1	PSO2	PSO3
CO1	3	3	2	1	-	-	-	-	-	-	2	2	3	2
CO2	3	3	2	2	2	-	-	-	-	-	3	3	3	3
CO3	3	3	2	3	3	2	-	2	2	2	2	3	2	3
CO4	2	2	1	1	2	2	2	2	-	1	2	2	2	2
CO5	2	3	2	2	3	3	2	-	2	2	1	2	2	2
CO6	3	3	3	2	3	3	3	2	2	3	3	3	3	3
Avg	**2.67**	**2.83**	**2.00**	**1.83**	**2.17**	**1.67**	**1.50**	**1.00**	**1.00**	**1.17**	**2.33**	**2.50**	**2.50**	**2.50**

13. CO × PO Alignment Map (H/M Indicators — All 6 COs)

CO	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PSO1	PSO2	PSO3

CO1	H	H	M								M	M	H	M
CO2	H	H	M	M	M						H	H	H	H
CO3	H	H	M	H	H	M		M	M	M	M	H	M	H
CO4	M	M			M	M	M	M			M	M	M	M
CO5	M	H	M	M	H	H	M		M	M		M	M	M
CO6	H	H	H	M	H	H	H	M	M	H	H	H	H	H

H = High / Primary alignment **M** = Medium / Secondary alignment *Blank = No direct alignment*

14. Self-Learning Activities (SL: 45 Hours)

S.No	Activity	Hours	COs / TS	Evaluation Criteria
1	Technical Video based learning related to the subject	Duration of video = 5h Report preparation & Presentation = 10h Total = 15h	CO1–CO4TS1–TS4	Report /presentation based on the video learning outcomes.
2	Mini Literature Review on a Technical Topic	Reading articles=10 h; Summary report= 5 h, Total=15 h	CO2, CO3, CO5TS2, TS3, TS5	Depth of literature review, comparison of approaches, referencing quality
3	Technical Blog Writing / Documentation on Course Topic	Study=7 h; Writing=8 h Total=15 h	CO4, CO5, CO6TS4, TS5, TS6	Technical clarity, originality, explanation with examples/diagrams
	TOTAL Self-Learning Hours	45 hrs	CO1–CO6	All activities are compulsory. Submission deadlines communicated at the start of the semester.

15. Bloom's Taxonomy — Domain Level Reference

Cognitive Domain (6 Levels)	Affective Domain (5 Levels)	Psychomotor Domain — Simpson (7 Levels)
L1 — Remember: Recall facts, definitions, basic concepts L2 — Understand: Explain ideas, concepts, and principles L3 — Apply: Use knowledge to solve problems in new situations L4 — Analyze: Break down information, examine relationships L5 — Evaluate: Judge, justify, assess, and make decisions L6 — Create: Design, develop, and produce new artefacts	A1 — Receiving: Awareness and willingness to attend A2 — Responding: Active participation and reaction A3 — Valuing: Commitment and assigning value to content A4 — Organizing: Integrating values into a personal system A5 — Characterizing: Internalized value system	P1 — Perception: Sensory cues guide motor activity P2 — Set: Mental, physical readiness to act P3 — Guided Response: Practice through imitation/trial P4 — Mechanism: Habitual correct performance P5 — Complex Overt Response: Skilled performance P6 — Adaptation: Modify skills for special situations P7 — Origination: Create new solution patterns

OBE Compliance Statement: This is a theory-only course. All 6 COs are mapped primarily to the Cognitive domain (L1–L5). Psychomotor domain (P3) appears only for CO3 (algorithm implementation as mental tracing). Affective domain (A3) appears for CO4 and CO5, reflecting valuing of algorithmic efficiency.

16. Attendance Policy & Pass / Fail Criteria

16.1 Attendance Policy

Component	Minimum	Applicable To	Consequence
Theory Classes	**75%**	All lecture sessions	Debarred from ETE if below threshold
Self-Learning / Assignment Submission	**All activities**	SL activities (45 hrs)	Incomplete SL affects CA score directly

Theory attendance must meet 75% minimum. Missing SL activities (assignments, video report, case study) directly impacts CA marks and is not compensable by exam performance.

16.2 Pass / Fail Criteria

Condition	Threshold	Status	Remarks
ETE Score	**≥ 24 / 60**	**MANDATORY**	40% of ETE paper required; failing ETE means failing the course regardless of CA + MTE
Overall Total (CA + MTE + ETE)	**≥ 40 / 100**	**Must pass overall**	CA 25 + MTE 15 + ETE 50 = 100; 40% overall minimum required

(…….)— MEASUREMENT ARCHITECTURE SUMMARY

Theory-Only Course | 6 COs (CO1–CO6) | 3 Assessment Instruments | 6 Theory Skill Dimensions (TS1–TS6)

CO1–CO2: Conceptual / Understand → TS1, TS2 → CA + MTE Sec A + ETE Sec A

CO3–CO4: Apply / Analyze → TS3, TS4 → CA + MTE Sec B + ETE Sec B

CO5–CO6: Analyze / Evaluate → TS5, TS6 → CA + ETE Sec B/C

CA 25 marks + MTE 25 marks + ETE 50 marks = Total 100 marks

SEMESTER VI

sCOURSE PLAN

Windows and Linux Hardening (CSCF3302)

School of Computing Science & Engineering (SSCSE) | B.Tech CSE | Semester VI | Batch 2026–2030

Integrated Course Plan — Theory COs (CO1–CO6) + Lab COs (CO7–CO10) | New AICTE 11-PO Framework | Full Skill Mapping

PART I

COURSE SYLLABUS

Course Identification, Details, Outcomes, BTL Mapping & Lecture/Lab Plans

1. Course Identification

School:	SSCSE	**Batch:**	2026–2030
Program:	B.Tech	**Current Academic Year:**	2026–27
Branch:	CSE	**Semester:**	VI

2. Course Details

Integrated theory + laboratory model. 10 COs in two tiers: Theory COs (CO1–CO6) via MTE + ETE; Lab COs (CO7–CO10) via Laboratory Assessment only. No cross-evaluation.

S.No	Attribute	Details
1	**Course Code**	**CSCF3302**
2	**Course Title**	**Windows and Linux Hardening**
3	**Credits**	4
4	**Contact Hours (L-T-P-SL)**	3-0-2-3
5	**Course Status**	Core

6	**Course Objective**	Students will gain practical experience in Windows and Linux operating system hardening through hands-on laboratories, focusing on secure configuration, authentication, access control, firewall and service hardening, kernel security, logging, auditing, vulnerability assessment, and compliance with industry security standards such as CIS Benchmarks and DISA STIGs while following ethical and professional cybersecurity practices.
7	**Course Outcomes (COs)**	**After successful completion of this course, the student will be able to:** **THEORY COs — Assessed via MTE + ETE:** **CO1 (Remember – L1):** Explain the fundamental concepts of operating system security, security principles, Windows and Linux security architectures, authentication, authorization, access control models, and common operating system threats and vulnerabilities. **CO2 (Understand – L2):** Describe Windows and Linux hardening techniques, including user and group management, password policies, file permissions, security policies, Group Policy, and operating system security features. **CO3 (Apply – L3):** Apply operating system hardening techniques to configure secure Windows and Linux systems by implementing authentication mechanisms, access controls, firewall configurations, SSH security, PAM, SELinux/AppArmor, and kernel protection. **CO4 (Analyze – L4):** Analyze operating system security using logging, auditing, vulnerability assessment tools, and security monitoring techniques to identify vulnerabilities and recommend appropriate remediation measures. **CO5 (Evaluate – L5):** Evaluate Windows and Linux systems against security standards and best practices, including CIS Benchmarks, DISA STIGs, Microsoft Security Baselines, and secure configuration guidelines, and recommend comprehensive hardening strategies to improve organizational security posture. **LAB COs — Assessed via Laboratory Assessment only:** **CO7 (Apply – L3):**

		Demonstrate the use of Windows and Linux security tools to configure secure user accounts, implement access controls, harden operating systems, and secure network services in controlled laboratory environments. **CO8 (Create – L5/L6):** Perform vulnerability assessments and security compliance evaluations using operating system hardening tools, and prepare structured technical reports documenting security findings, risk analysis, and recommended remediation measures. **CO9 (Apply – L2/L3):** Collaborate effectively in operating system security and hardening activities by configuring security policies, analyzing audit logs, interpreting vulnerability assessment results, and recommending secure system configurations. **CO10 (Apply – L3):** Demonstrate professional and ethical practices in operating system administration by implementing secure configurations, adhering to organizational security policies, ensuring regulatory compliance, and following industry standards such as CIS Benchmarks and DISA STIGs.
8	**Teaching & Learning**	Classroom Instructions (CI) 45 hrs + Lab Instructions (LI) 30 hrs + Self Learning (SL) 45 hrs = 120 hrs
9	**Mode of Examination**	Lab (40 marks) + MTE (10 marks) + ETE (50 marks) = 100 marks. Theory COs: MTE + ETE only. Lab COs: Lab only.
10	**Self Learning (SL: 45 hrs)**	4. Explore and practice operating system security and hardening tools such as Microsoft Security Compliance Toolkit, Group Policy Editor, PowerShell, Sysinternals Suite, Lynis, OpenSCAP, auditd, and SELinux/AppArmor tools to perform system analysis, security configuration, vulnerability identification, and hardening assessment in controlled laboratory environments. Prepare a technical report documenting tools used, hardening procedures, security findings, compliance status, and recommended remediation measures. 5. Perform a simulated end-to-end operating system hardening exercise involving Windows and Linux system assessment, user and permission configuration, service hardening, firewall configuration, authentication security, logging and auditing, vulnerability assessment, compliance checking, and preparation of a professional system hardening report for a mock organizational environment. 6. Study emerging trends in operating system and infrastructure security including zero trust architecture, secure boot technologies, container security, cloud workload protection, endpoint detection and response (EDR), automated compliance management, AI-assisted security operations, and modern system defense mechanisms. Prepare a technical presentation and summary report analyzing current challenges, security approaches, industry standards, and recommended hardening practices..

11	**References**	8. Christopher Negus, Linux Bible, 11th Edition, Wiley, 2025. 9. Ben Clark, Linux Hardening in Hostile Networks: Protecting Linux Servers from Attack, Apress, 2020. 10. William Panek, Microsoft Security, Compliance, and Identity Fundamentals (SC-900) Study Guide, Wiley Sybex, 2022.

3. Outline Syllabus — Theory Units with CO Mapping (CO1–CO6)

Unit CO mappings refer to Theory COs (CO1–CO6) only. Lab experiments reinforce these units but are assessed under Lab COs (CO7–CO10).

	Topic / Activity	CO Mapping
Unit 1	**Fundamentals of Operating System Security: (8-0-0-6 = 14hrs)**	
A	Security Principles (CIA Triad, Least Privilege, Defense in Depth) Authentication, Authorization, and Accountability (AAA) Access Control Models (DAC, MAC, RBAC)	CO1, CO2, CO3
B	Windows Security Architecture: SRM, LSASS, SAM,UAC	
C	Linux Security Architecture: Linux Kernel Security, User Space and Kernel Space, File System Hierarchy, LSM, Process and Memory Protection	
Tools Used	Windows Security PowerShell Sysinternals Process Explorer Linux Terminal (Bash) systeminfo / uname	
Activities	**Objective:** • Understand Windows and Linux security architectures. • Identify system security components and operating system configurations. • Examine user accounts, processes, and system information. • Compare Windows and Linux security mechanisms. • Analyze the operating system attack surface.	
Unit 2	**Windows Operating System Hardening: (10-0-0-9= 19 hrs)**	

A	User and Group Management, Password and Account Policies, NTFS Permissions and Access Control	CO1, CO2,CO3,CO5
B	Windows Services and Service Hardening, Windows Defender Security Features, Windows Firewall Configuration, BitLocker Drive Encryption	
C	Windows Event Logging and Auditing, Group Policy Objects (GPO), Microsoft Security Baselines, Windows Update and Patch Management	
Tools Used	Local Group Policy Editor (gpedit.msc) Microsoft Security Compliance Toolkit Windows Defender Firewall Windows Event Viewer PowerShell	
Activities	**Objective:** • Configure secure user and password policies. • Apply Microsoft security baselines and Group Policy settings. • Harden Windows services and firewall configurations. • Enable and review Windows security auditing. • Implement secure Windows operating system configurations	
Unit 3	**Linux Operating System Hardening (9-0-0-10 = 19 hrs)**	
A	Linux User and Group Management, File Permissions and Ownership, Special Permissions (SUID, SGID, Sticky Bit)	CO2, CO3, CO4, CO5, CO6
B	Access Control Lists (ACLs), Sudo Configuration Pluggable Authentication Modules (PAM)	
C	Password Policies, SSH Hardening, Firewall Configuration, SELinux and AppArmor Kernel and Process Hardening	
Tools Used	OpenSSH UFW (or firewalld) SELinux (or AppArmor) auditd Linux Terminal (Bash	

Activities	**Objective:** • Configure secure Linux user accounts and file permissions. • Implement PAM authentication and password policies. • Harden SSH services and firewall configurations. • Configure SELinux/AppArmor access control policies. • Apply kernel and process hardening techniques.	
Unit 4	**Logging, Auditing, and Vulnerability Assessment (9-0-0-10 = 19 hrs)**	
A	Security Logging Concepts, Windows Event Viewer, Windows Audit Policy Linux Audit Framework (auditd)	CO3, CO4, CO5
B	journald and rsyslog, Log Analysis, Security Monitoring, Vulnerability Assessment Concepts, CVE and CVSS	
C	OpenSCAP, Lynis, Patch and Update Management, Security Reporting	
Tools Used	OpenSCAP Lynis auditd Windows Event Viewer Sysinternals Autoruns	
Activities	**Objective:** • Assess web server and web application security using ethical testing techniques. • Identify common web vulnerabilities, including those listed in the OWASP Top 10. • Demonstrate SQL Injection and Cross-Site Scripting (XSS) attacks in a safe laboratory environment. • Analyze wireless network security mechanisms and authentication protocols. • Explore fundamental mobile application security concepts and common mobile threats.	
Unit 5	**Security Compliance and System Hardening for Industry (9-0-0-10 = 19 hrs)**	

A	CIS Benchmarks, DISA STIG Guidelines, Microsoft Security Baselines	CO2, CO3, CO4, CO5, CO6
B	Secure Configuration Management, Compliance Auditing Incident Response Basics	
C	Documentation of Security Configurations, Hardening Windows and Linux Systems, Case Studies	
Tools Used	CIS Benchmarks Microsoft Security Compliance Toolkit OpenSCAP	
Activities	**Objective:** • Assess Windows and Linux systems against CIS Benchmarks. • Verify compliance with security configuration standards. • Implement comprehensive operating system hardening. • Document secure configuration and remediation measures. • Develop and validate a complete Windows and Linux hardening project.	

4. Topic-wise Bloom's Taxonomy Level Mapping (Theory)

S.No	Topic	L1	L2	L3	L4	L5	L6
1	1.A	□	□				
2	1.B		□	□			
3	1.C		□	□			
4	2.A			□			
5	2.B			□			
6	2.C			□	□		
7	3.A			□	□		□

8	3.B		□	□		□	
9	3.C			□	□		
10	4.A			□	□		
11	4.B			□	□	□	
12	4.C			□			
13	5.A		□	□		□	□
14	5.B			□	□		□
15	5.C			□	□	□	□

5. CO vs Bloom's Taxonomy — All Three Domains (Updated for 10 COs)

□ *Only strong/dominant alignments are mapped. Lab COs (CO7–CO10) extend into Psychomotor and Affective domains, reflecting the skill-based nature of lab and project work.*

CO	Cognitive Domain (L1–L6)						Affective (A1–A5)					Psychomotor (P1–P7)						
CO	L1	L2	L3	L4	L5	L6	A1	A2	A3	A4	A5	P1	P2	P3	P4	P5	P6	P7
CO1	□																	
CO2		□																
CO3			□											□				
CO4				□											□			
CO5					□											□		
CO6						□			□							□	□	
CO7			□					□						□	□			
CO8					□	□			□						□	□	□	

CO9			□							□	□						
CO10			□					□			□			□			

Legend: □ = Strong / Dominant mapping only. Theory COs: primarily Cognitive. Lab COs: span all three domains.

6. Lecture Plan Outline (Theory — 45 Lectures)

Date	Topics to be Covered/Title	UNIT	Total Lectures
DD/MM/YY	Introduction to Operating System Security and Security Principles (CIA Triad, Least Privilege, Defense in Depth)	UNIT-1	9
DD/MM/YY	Authentication, Authorization, Accountability (AAA) and Access Control Models (DAC, MAC, RBAC)		
DD/MM/YY	Threats, Vulnerabilities, Attack Surface, and Threat Modeling		
DD/MM/YY	Windows Security Architecture: Kernel, Security Reference Monitor (SRM), LSASS		
DD/MM/YY	Windows Security Components: SAM, UAC, Registry, NTFS Security		
DD/MM/YY	Linux Security Architecture: Kernel, User Space, Process Model		
DD/MM/YY	Linux File System Security and Linux Security Modules (LSM)		
DD/MM/YY	Comparison of Windows		
DD/MM/YY	Linux Security Architectures		
DD/MM/YY	Windows User and Group Management	UNIT-2	9
DD/MM/YY	Password Policies, Account Lockout, and Local Security Policy		
DD/MM/YY	NTFS Permissions and Access Control		
DD/MM/YY	Windows Services and Service Hardening		
DD/MM/YY	Windows Defender, BitLocker, and Windows Firewall		
DD/MM/YY	Group Policy Objects (GPO): Concepts and Configuration		

DD/MM/YY	Microsoft Security Baselines and Security Compliance Toolkit		
DD/MM/YY	Windows Event Logging, Auditing, and Patch Management		
DD/MM/YY	Windows User and Group Management		
DD/MM/YY	Linux User and Group Management	UNIT-3	9
DD/MM/YY	File Permissions, Ownership, SUID, SGID, Sticky Bit		
DD/MM/YY	Access Control Lists (ACLs) and sudo Configuration		
DD/MM/YY	Pluggable Authentication Modules (PAM) and Password Policies		
DD/MM/YY	SSH Hardening and Secure Remote Access		
DD/MM/YY	Linux Firewall Configuration (UFW, firewalld, nftables/iptables)		
DD/MM/YY	SELinux and AppArmor Configuration		
DD/MM/YY	Kernel and Process Hardening (sysctl, Secure Boot, Capabilities)		
DD/MM/YY	Linux Hardening Case Study and Best Practices		
DD/MM/YY	Security Logging Concepts and Windows Event Viewer	UNIT-4	9
DD/MM/YY	Windows Audit Policy and Security Monitoring		
DD/MM/YY	Linux Logging: journald, rsyslog, and Log Management		
DD/MM/YY	Linux Auditing using auditd, ausearch, and aureport		
DD/MM/YY	Vulnerability Assessment Concepts, CVE, and CVSS		
DD/MM/YY	OpenSCAP: Installation, Configuration, and Compliance Scanning		
DD/MM/YY	Lynis: Security Auditing and Hardening Recommendations		
DD/MM/YY	Patch Management and Security Reporting		
DD/MM/YY	Vulnerability Assessment Case Study		
DD/MM/YY	Introduction to CIS Benchmarks and Secure Configuration Standards	UNIT-5	9
DD/MM/YY	DISA STIGs and Microsoft Security Baselines		

DD/MM/YY	Compliance Auditing and Security Configuration Assessment		
DD/MM/YY	Secure Configuration Management and Documentation		
DD/MM/YY	Incident Response Basics for Operating Systems		
DD/MM/YY	Windows Hardening Project: Planning and Implementation		
DD/MM/YY	Linux Hardening Project: Planning and Implementation		
DD/MM/YY	Integrated Windows Hardening Case Study		
DD/MM/YY	Integrated Linux Hardening Case Study		

7. Lab Session Plan — List of Experiments (Updated CO7–CO10)

W1–W12: All experiments develop CO7 skills (professional implementation, tool usage, documentation). W13–W15 (teal rows): CO8 (design/real-world), CO9 (ethics/reflection), CO10 (teamwork/presentation). Theory knowledge is applied but NOT re-evaluated in lab.

Week	Session	Experiment	Lab CO	Marks
W1	S-1	Study of Windows and Linux Security Architecture and System Information Analysis	CO7	3.0
W2	S-2	User Account Management and Access Control Analysis in Windows and Linux	CO7	3.0
W3	S-3	Process, Service, and Startup Security Analysis	CO7	3.0
W4	S-4	Windows User, Password Policy, and Account Security Hardening.	CO7	3.0

W5	S-5	Windows NTFS Permission and Access Control Hardening.	**CO7**	3.0
W6	S-6	Windows Firewall and Network Service Hardening	**CO7**	3.0
W7	S-7	Windows Security Baseline Implementation Using Group Policy	**CO7**	3.0
W8	S-8	Linux File Permission and User Security Hardening	**CO8/CO9**	3.0
W9	S-9	Linux SSH Service Hardening and Secure Remote Administration	**CO8/CO10**	3.0
W10	S-10	Linux Firewall Configuration and Network Hardening	**CO9/CO10**	3.0
W11	S-11	Linux Mandatory Access Control Using SELinux/AppArmor	**CO7**	3.0
W12	S-12	Linux Kernel and Process Hardening	**CO7**	3.0

W13	S-13	Windows and Linux Security Logging and Auditing	CO8	3.0
W14	S-14	Operating System Vulnerability Assessment and Security Audi	CO8/CO9	3.0
W15	S-15	Windows and Linux Hardening Compliance check	CO8/CO9	3.0

Instructions: Write C programs, compile, execute and test with suitable test cases. Lab record (aim, algorithm, code, output, result) must be submitted before the next session.

PART II

THEORY ASSESSMENT FRAMEWORK

Theory Skill Dimensions, MTE & ETE Structure for Theory COs (CO1–CO6)

8. Theory Skill Dimensions (TS1–TS6) — CO1 through CO6

THEORY COs (CO1–CO6) — Assessed exclusively via MTE and ETE only

Six theory skill dimensions — one per Bloom's level L1–L6 — correspond directly to CO1–CO6. They define the competency measured in each section of MTE and ETE, providing a clear NBA-auditable assessment rationale.

ID	Dimension	What is Measured	CO / BTL	Assessment

TS1	**Operating System Security Fundamentals**	Recall operating system security concepts, security principles, Windows and Linux security architecture, authentication, authorization, access control models, threats, vulnerabilities, and attack surface.	CO1 | L1–L2	MTE Sec A | ETE Sec A
TS2	**Windows and Linux Operating System Hardening**	Explain and apply Windows hardening (users, NTFS, services, Group Policy, security baselines) and Linux hardening (permissions, PAM, SELinux/AppArmor, SSH, firewall, kernel hardening) techniques to secure operating systems	CO2 | L2	MTE Sec A | ETE Sec A
TS3	**Logging, Auditing, Vulnerability Assessment & Compliance**	Apply logging, auditing, vulnerability assessment, CIS Benchmarks, DISA STIG compliance, and secure configuration management to assess and harden Windows and Linux systems	CO3 | L3	MTE Sec B | ETE Sec B
TS4	**Windows and Linux Hardening Techniques**	Analyze Windows and Linux hardening mechanisms, including user and permission management, Group Policy, PAM, SELinux/AppArmor, SSH security, firewall configuration, and kernel protection, and recommend appropriate system hardening measures.	CO4 | L4	MTE Sec B | ETE Sec B
TS5	**Security Monitoring, Auditing & Vulnerability Assessment**	Evaluate operating system security using logging, auditing, vulnerability assessment tools, patch management, and security monitoring techniques, and justify suitable remediation and mitigation strategies.	CO5 | L5	ETE Sec B/C
TS6	**Security Compliance & Secure System Administration**	Design and implement secure operating system configurations using CIS Benchmarks, DISA STIGs, Microsoft Security Baselines, compliance auditing, and security documentation while integrating ethical, legal, and professional cybersecurity practices.	CO6 | L6	ETE Sec C

9. Theory Assessment Structure — MTE and ETE

9.1 Mid Term Examination (MTE) — 10 Marks (CO1–CO4 only)

Section	Marks	Skill Dimensions	COs	Question Type
Sec A	**4**	TS1 — Operating System Security Fundamentals TS2 — Windows and Linux Operating System Hardening	**CO1, CO2**	Short-answer: definitions.
Sec B	**6**	TS3 — Logging, Auditing, Vulnerability Assessment & Security Compliance TS4 — Windows and Linux Hardening Techniques	**CO3, CO4**	Long and descriptive answers
TOTAL	**10**	TS1–TS4	**CO1–CO4**	Units 1–3 covered; CO5 and CO6 assessed only in ETE

9.2 End Term Examination (ETE) — 100 Marks (Scaled to 50) (CO1–CO6)

Section	Marks	Skill Dimensions	COs	Question Type
Sec A	**25**	TS1 — Operating System Security Fundamentals TS2 — Windows and Linux Operating System Hardening	**CO1, CO2**	Short questions: definitions.
Sec B	**50**	TS3 — Logging, Auditing, Vulnerability Assessment & Security Compliance TS4 — Windows and Linux Hardening Techniques	**CO3, CO4, CO5**	Medium questions: Comparison, Tools and Techniques
Sec C	**25**	TS5 — Security Monitoring, Auditing & Vulnerability Assessment TS6 — Security Compliance & Secure System Administration	**CO5, CO6**	Long/design questions: Applications, working principles/

TOTAL	**100**	TS1–TS6 (all)	**CO1–CO6**	Scaled to 50 marks. Minimum 20/50 required to pass.

PART III

LABORATORY ASSESSMENT FRAMEWORK

Evaluation Scheme, CA Rubric, Mini Project Rubric, Skill Dimensions for Lab COs (CO7–CO10)

10. Evaluation Scheme — Overview

Component	Weightage	Marks	COs Assessed
Laboratory Assessment	40%	**40**	Lab COs only: CA experiments
Mid Semester Examination (MTE)	10%	**10**	Theory COs only: CO1, CO2, CO3, CO4
End Semester Examination (ETE)	50%	**50**	Theory COs only: CO1, CO2, CO3, CO4, CO5, CO6
TOTAL	**100%**	**100**	Strict separation — no cross-assessment

11. Laboratory Assessment (40 Marks)

LAB COs (CO7–CO10) — Assessed exclusively via Laboratory Assessment only (CA)

11.1 Component Breakdown

Sub-Component	Quantum	Marks	Remarks
Lab Experiments (CA)	Best 10 of 12	**30**	3.0 marks each — assesses CO7, CO8, CO9
Mini Project/Case Study	1 Project	**10**	Design, implementation, demo & reflection — all 4 Lab COs (CO7–CO10)
TOTAL	—	**40**	

11.2 Per-Experiment CA Rubric (3.0 Marks each — Assesses CO7, CO8, CO9)

Criterion	Marks	CA Skill Dimensions Covered	Marking Guide	Lab CO
Problem Definition & Experimental Design	**1.0**	CA1 — Problem identification, forensic objective, scope definition CA2 — Investigation planning, tool/environment selection CA7 — Methodology, workflow, attack/defense analysis plan	1.0: Well-defined with design | 0.5: Partial | 0: Missing	CO7, CO8
Code Execution & Computational Efficiency	**1.0**	CA3 — Correct execution of scanning/sniffing/auditing/crypto tasks CA4 — Efficient and optimized use of tools/scripts	1.0: Correct & efficient | 0.5: Correct, not optimized | 0: Fails	CO7
Output Analysis, Outcome & Lab Documentation	**0.75**	CA5 — Packet/log/result analysis and interpretation CA6 — Evidence validation, screenshots, observations and conclusion documentation	0.75: Thorough | 0.5: Adequate | 0.25: Partial | 0: Absent	CO8, CO9
Professional Attitude & Ethical Conduct	**0.25**	CA6 — Structured report, screenshots, references, conclusion CA8 — Viva-voce understanding and communication PO7/CO9 — Ethical and responsible cybersecurity practices	0.25: Consistent | 0.10: Occasional | 0: Absent	CO9
Total	**3.0**	All 8 CA skill dimensions covered		

11.3 Best-10-of-N Scoring Scheme

Conducted	Best N Counted	Max Score	Note
> (10 + x)	Best 10	**30 Marks**	x worst dropped
10	All 10	**30 Marks**	No drop
< 10	All	**≤ 30 Marks**	Deficit = zero

11.4 Mini Project Evaluation Rubric (10 Marks — All 4 Lab COs)

Criterion	Marks	Project Skill Dimensions	Marking Guide	Lab CO / PO
SDG Alignment & Problem Scoping	**1.5**	P1 — SDG mapping; societal relevance P2 — Problem scope and stakeholder requirements P4 — Innovative solution proposal with alternatives	1.5: Comprehensive | 1.0: Adequate | 0.5: Partial | 0: Absent	CO8 / PO3, PO6
Project Planning & Financial Awareness	**1.5**	P2 — Timeline, milestones, resource planning P11 — Financial feasibility and cost estimation	1.5: Detailed | 1.0: Adequate | 0.5: Basic | 0: Absent	CO10 / PO10
End-to-End Implementation & System Operation	**2.0**	P5 — Professional toolchain selection P6 — Complete project build and integration P7 — System commissioning and operational testing	2: Fully operational | 1–1.5: Partial | 0–0.5: Non-functional	CO7, CO8 / PO3, PO5
Impact Assessment & Critical Reporting	**2.0**	P8 — Measurable outcome vs stated goals P9 — Statistical/comparative analysis; technical report	2: Rigorous | 1.5: Good | 1: Basic | 0: Absent	CO8, CO10 / PO6
Communication, Presentation & Teamwork	**2.0**	P3 — Communication plan and testing strategy P10 — Professional presentation quality and delivery	2: Excellent | 1.5: Good | 1: Adequate | 0: Poor	CO10 / PO8, PO9
Skill Reflection, Ethics & Professional Attitudes	**1.0**	P12 — Skill growth mapping (pre/post project) P13 — Professional attitudes and ethical conduct	1.0: Reflective & honest | 0.5: Partial | 0: Absent	CO9 / PO7, PO11
Total	**10**	All 13 Project skill dimensions; all 4 Lab COs (CO7–CO10)		

12. CA Skill Dimensions (8 Dimensions — Lab COs only)

ID	Dimension	What is Measured	Lab CO Anchor

CA1	**Problem Definition & Metrics**	Define forensic/security problem; identify measurable attributes, attack indicators, objectives, scope, and success criteria	CO7, CO8
CA2	**Experimental Design & Tool Setup**	Plan experiment/investigation; configure tools and environments such as VirtualBox, Wine, Nmap, Wireshark, IPCop, cryptographic utilities, Linux CLI, and network settings	CO7
CA3	**Code Implementation & Execution**	Correctly execute scanning, sniffing, auditing, fingerprinting, firewall, and cryptographic experiments to obtain expected outputs	CO7
CA4	**Computational Efficiency & Optimization**	Analyze efficiency of scans/captures/configurations; identify bottlenecks, security gaps, and optimization techniques	CO7
CA5	**Output Analysis & Result Interpretation**	Analyze captured packets, logs, scans, fingerprints, and cryptographic outputs; explain findings and derive evidence-based conclusions	CO8
CA6	**Documented Outcome with Verification**	Record experiment results formally with screenshots/logs/output verification and validate against objectives	CO7, CO8
CA7	**Algorithmic Design & Solution Planning**	Design investigation workflow/steps; prepare procedures, attack-defense methodology, flowcharts, or security audit plans before execution	CO7, CO8
CA8	**Lab Record Maintenance & Viva-Voce**	Maintain complete lab records, observations, ethical practices, and demonstrate conceptual understanding during viva	CO7, CO9

13. Project Skill Dimensions (13 Dimensions — Lab COs only)

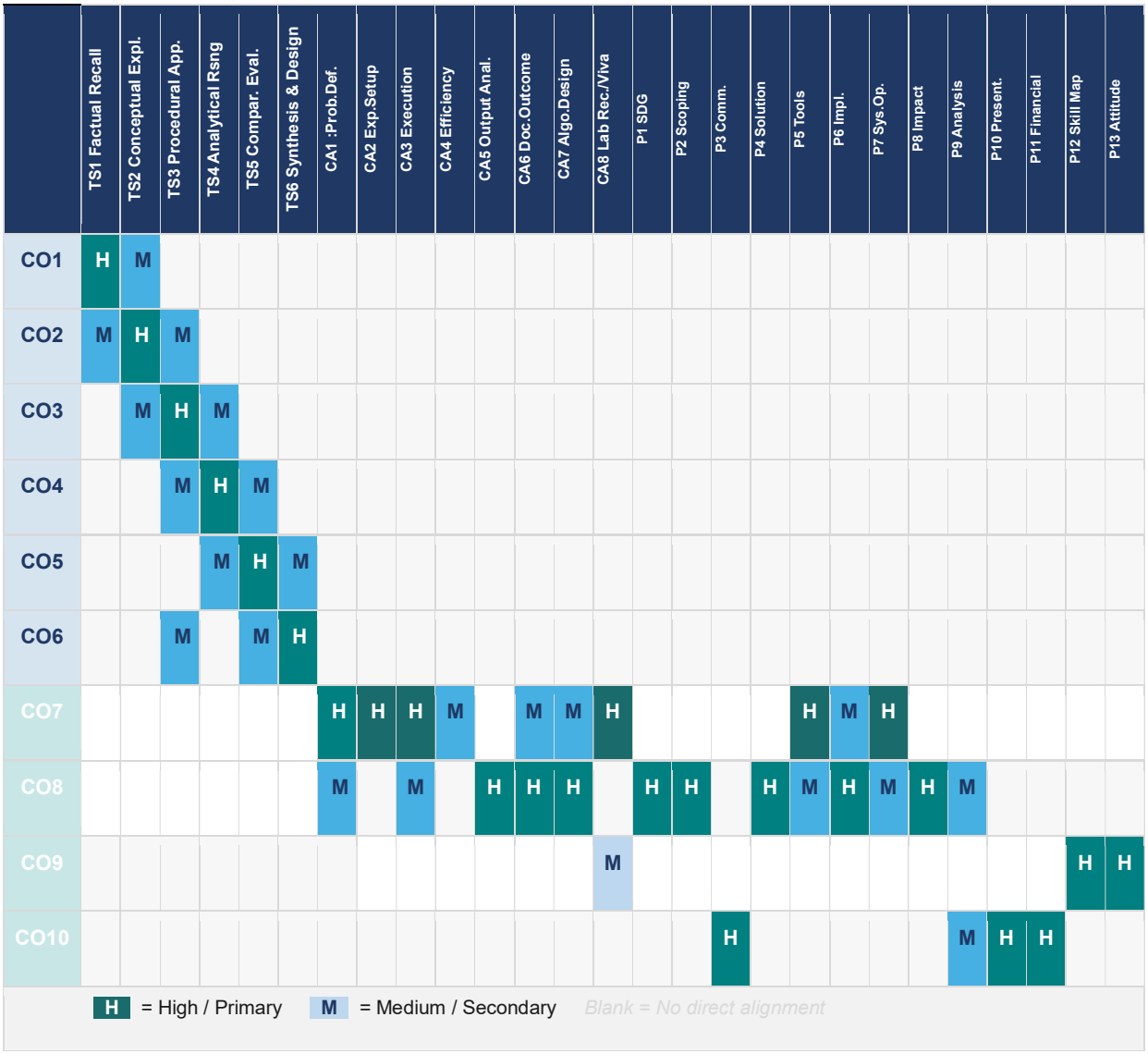
ID	Dimension	What is Measured	Lab CO / PO Anchor
P1	**SDG Alignment & Social Relevance**	Map project to relevant SDGs; articulate societal value and intended impact	CO8 | PO6
P2	**Problem Scoping & Requirements**	Define boundaries; produce formal problem statement with measurable goals	CO8 | PO2
P3	**Communication & Testing Strategy**	Develop communication plan; design testing strategy; coordinate group activities	CO10 | PO9
P4	**Innovative Solution Proposal**	Propose solution with alternatives; justify selection using design criteria	CO8 | PO3

P5	**Professional Toolchain**	Select and justify development tools; configure professional project environment	CO7 | PO5
P6	**End-to-End Implementation**	Build complete integrated solution incorporating at least 3 syllabus topics	CO7, CO8 | PO3
P7	**System Commissioning & Testing**	Deploy and operate system; conduct edge-case and stress tests	CO7, CO8 | PO5
P8	**Measurable Impact & Outcome**	Evaluate actual outcomes against goals; quantify impact using defined metrics	CO8 | PO6
P9	**Critical Analysis & Reporting**	Perform comparative/statistical analysis; produce structured technical report	CO8, CO10 | PO2, PO4
P10	**Professional Presentation & Teamwork**	Deliver professional presentation; evidence team collaboration and role differentiation	CO10 | PO8, PO9
P11	**Financial Feasibility & Planning**	Estimate project cost; justify resource allocation; discuss cost-effectiveness	CO10 | PO10
P12	**Individual Skill Growth Mapping**	Document pre/post skill gaps; map personal contributions to project dimensions	CO9 | PO11
P13	**Professional Attitude, Ethics & Responsibility**	Demonstrate integrity, ethical conduct, and responsible use of tools/data throughout	CO9 | PO7

14. CO × Skill Dimensions Mapping (10 COs × [6 Theory+ 8 CA + 13 Project Dimensions])

- *Theory COs (CO1–CO6) are fully mapped. Lab COs (CO7–CO10) intentionally have no TS mapping — confirming strict assessment separation.*
- *Theory COs (CO1–CO6) have NO CA alignment — confirms they are NOT evaluated in lab. All CA alignments confined to Lab COs (CO7–CO10).*
- *Theory COs (CO1–CO6) have NO project alignment — confirms strict lab-only assessment. All 13 Project dimensions anchored exclusively to Lab COs (CO7–CO10).*

CO	Theory Skill Dimensions	CA Skill Dimensions	Project Skill Dimensions



	TS1 Factual Recall	TS2 Conceptual Expl.	TS3 Procedural App.	TS4 Analytical Rsng	TS5 Compar. Eval.	TS6 Synthesis & Design	CA1 :Prob.Def.	CA2 Exp.Setup	CA3 Execution	CA4 Efficiency	CA5 Output Anal.	CA6 Doc.Outcome	CA7 Algo.Design	CA8 Lab Rec./Viva	P1 SDG	P2 Scoping	P3 Comm.	P4 Solution	P5 Tools	P6 Impl.	P7 Sys.Op.	P8 Impact	P9 Analysis	P10 Present.	P11 Financial	P12 Skill Map	P13 Attitude
CO1	H	M																									
CO2	M	H	M																								
CO3		M	H	M																							
CO4			M	H	M																						
CO5				M	H	M																					
CO6			M		M	H																					
CO7							H	H	H	M		M	M	H					H	M	H						
CO8							M		M		H	H	H		H	H		H	M	H	M	H	M				
CO9														M												H	H
CO10																	H						M	H	H		

H = High / Primary M = Medium / Secondary *Blank = No direct alignment*

PART IV

COMBINED MAPPINGS & REFERENCE

CO–PO Matrix, SDG Mapping, Bloom's Taxonomy Reference, Attendance & Pass/Fail

15. CO–PO and CO–PSO Mapping Matrix (All 10 COs)

Strength Scale: 3 = Substantial (High) | 2 = Moderate | 1 = Slight (Low) | – = Not Applicable. Column averages computed over non-zero entries only.

CO/PO	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PSO1	PSO2	PSO3
CO1	3	2	-	2	2	2	3	1	1	1	2	3	2	2
CO2	3	3	2	2	3	-	2	2	-	1	2	3	3	2
CO3	2	3	3	3	3	-	2	-	-	1	2	3	3	3
CO4	3	2	2	3	3	-	2	-	1	-	2	3	3	2
CO5	2	3	-	2	2	2	2	-	1	2	3	2	3	2
CO6	2	2	-	-	-	1	-	-	3	2	2	2	2	2
CO7	–	–	1	–	3	1	–	–	–	–	–	2	3	3
CO8	–	1	3	1	2	3	–	–	–	–	–	2	3	3
CO9	–	–	–	–	–	–	3	–	–	–	3	–	1	2
CO10	–	–	–	–	–	1	–	3	3	3	2	2	2	2
Avg	2.50	2.29	2.20	2.17	2.57	1.67	2.33	2.00	1.80	1.67	2.25	2.44	2.50	2.30

PO7 (Ethics) now receives mapping from CO9 (strength 3). PO11 (Life-Long Learning) is addressed by both Theory COs and CO9. Lab COs (CO7–CO10) extend coverage to POs 3, 5, 6, 7, 8, 9, 10, 11.

16. CO × PO Alignment Map (H/M Indicators — All 10 COs × 11 POs)

CO	PO1 Eng.Know.	PO2 Prob.Analysis	PO3 Design	PO4 Investigation	PO5 Tool Usage	PO6 Engineer & World	PO7 Ethics	PO8 Teamwork	PO9 Comm.	PO10 Proj.Mgmt	PO11 Lifelong
CO1	H	M	-	M	M	M	H				M
CO2	H	H	M	M	H	-	M	M	-		M
CO3	M	H	H	H	H	-	M	-	-		M
CO4	H	M	M	H	H	-	M	-		-	M
CO5	M	H	-	M	M	M	M	-		M	H
CO6	M	M	-	-	-		-	-	H	M	M
CO7	–	–		–	H		–	–	–	–	–
CO8	–		H		M	H	–	–	–	–	–
CO9	–	–	–	–	–	–	H	–	–	–	H
CO10	–	–	–	–	–		–	H	H	H	M

H = High / Primary **M** = Medium / Secondary *Blank = No direct alignment*

17. Course-to-SDG Mapping Matrix

SDG Goal	Description	Mapping	Justification
SDG 4	**Quality Education**	**3 (High)**	Builds strong foundation in computational thinking and structured programming; aligned with lifelong learning (CO1–CO6, CO9).

SDG 8	Decent Work & Economic Growth	3 (High)	Develops industry-relevant programming and professional tool skills (CO7) directly applicable to employment in technology sectors.
SDG 9	Industry, Innovation & Infrastructure	3 (High)	Enables development of efficient software solutions; fosters innovation through real-world application design (CO6, CO8) and team-based projects (CO10).
SDG 12	Responsible Consumption & Production	2 (Moderate)	Promotes efficient, optimized coding; encourages ethical coding and responsible use of computational resources (CO9, CO7).

18. Bloom's Taxonomy — Domain Level Reference

Cognitive Domain (6 Levels)	Affective Domain (5 Levels)	Psychomotor Domain — Simpson (7 Levels)
L1 — Remember: Recall facts, definitions, basic concepts L2 — Understand: Explain ideas, concepts, principles L3 — Apply: Use knowledge to solve new problems L4 — Analyze: Break down information, examine patterns L5 — Evaluate: Judge, justify, assess, make decisions L6 — Create: Design, develop, produce new solutions	A1 — Receiving: Awareness, willingness to attend A2 — Responding: Active participation and reaction A3 — Valuing: Showing commitment, assigning value A4 — Organizing: Integrating values into personal system A5 — Characterizing: Internalized value system	P1 — Perception: Sensory cues guide motor activity P2 — Set: Mental, physical readiness to act P3 — Guided Response: Basic practice through imitation P4 — Mechanism: Habitual correct performance P5 — Complex Overt Response: Skilled performance P6 — Adaptation: Modify skills for special situations P7 — Origination: Create new solution patterns

OBE Compliance Statement: Theory COs (CO1–CO6) are primarily mapped to the Cognitive domain (L1–L6). Lab COs (CO7–CO10) span all three domains — Cognitive (L2–L6), Psychomotor (P3–P7), and Affective (A2–A5) — reflecting the skill-based nature of laboratory and project assessment.

19. Attendance Policy & Pass/Fail Criteria

19.1 Attendance Policy

Component	Minimum	Applicable To	Consequence
Theory Classes	**70%**	All lecture sessions	Debarred from ETE
Practical / Lab	**70%**	All lab sessions	Debarred from ETE
Combined (Theory + Lab)	**75%**	Combined sessions	Debarred from ETE

Both theory and practical attendance must independently meet 70%. The combined must be 75%. Satisfying one does NOT compensate for a shortfall in the other.

19.2 Pass / Fail Criteria

Condition	Threshold	Status	Remarks
ETE Score (scaled)	**≥ 20 / 50**	**MANDATORY**	40% of ETE; equivalent to ≥ 40/100 on the full paper
Overall Total	**≥ 40 / 100**	**Must pass overall**	Lab 40 + MTE 10 + ETE 50 = 100; 40% overall minimum required

PPS INTEGRATED COURSE PLAN — MEASUREMENT ARCHITECTURE

11 AICTE Programme Outcomes → 10 COs (6 Theory + 4 Lab) → 3 Assessment Instruments → 27 Skill Dimensions (6 TS + 8 CA + 13 Project)

Theory Tier CO1–CO6 (MTE + ETE): PO1, PO2, PO3, PO4, PO9 | 6 Theory Skill Dims (TS1–TS6)

Lab Tier CO7–CO10 (Lab only): PO3, PO5, PO6, PO7, PO8, PO9, PO10, PO11 | 8 CA Dims + 13 Project Dims

Marks: Lab 40 (Experiments 30 @ 3.0 each + Project 10) + MTE 10 + ETE 50 = Total 100

COURSE PLAN

Web Application Security (CSCF3202)

Sharda School of Computing Science & Engineering | B.Tech CSE | Semester VI | Batch 2026–2030

Theory-Only Course Plan — All 6 COs (CO1–CO6) | Theory Skill Dimensions TS1–TS6 | CA + MTE + ETE Assessment

PART I

COURSE SYLLABUS

Course Identification, Details, Outcomes, BTL Mapping & Lecture Plan

1. Course Identification

School:	SSCSE- Sharda School of Computing Science & Engineering	**Batch:**	2026 – 2030
Program:	B. Tech	**Current Academic Year:**	2028-29
Branch:	Cyber Security & Forensics	**Semester:**	VI
Course Code:	**CSCF3202**	**Course Type:**	Core — Theory Only

2. Course Details

 THEORY-ONLY COURSE — All 6 COs (CO1–CO6) are assessed exclusively via Continuous Assessment (CA), MTE, and ETE. No laboratory component.

S.No	Attribute	Details
1	**Course Code**	**CSCF3202**
2	**Course Title**	**Web Application Security**
3	**Credits**	3

4	**Contact Hours (L-T-P-SL)**	3-0-0-3 (Theory: 45 hrs. Classroom + 45 hrs. Self-Learning = 90 hrs. total)
5	**Course Status**	**Core — Theory Only (No Laboratory Component)**
6	**Course Objectives**	1. Understand the fundamentals of web application security and common web vulnerabilities. 2. Develop practical skills to identify and mitigate security threats in web applications. 3. Apply digital forensics techniques for investigating web-based security incidents. 4. Enhance hands-on skills in secure web application development and testing.
7	**Course Outcomes (COs)**	**After successful completion of this course, students will be able to:** CO1 (Understand – L1/L2): Understand and enhance communication and problem-solving skills in the context of web application security. CO2 (Apply – L2/L3): Identify, explain, and demonstrate insecure coding practices and apply appropriate methods to rectify vulnerabilities in web applications. CO3 (Understand – L1/L2): Understand the IT infrastructure and foundational concepts associated with web application security. CO4 (Analyze – L3/L4): Analyze the challenges, limitations, and effectiveness of application security techniques. CO5 (Design – L4/L5): Design and apply data mining-based solutions for addressing security issues in web applications. CO6 (Examine – L3/L4): Examine database security concerns and web-specific input validation issues in secure web applications.
8	**Course Description**	This course introduces advanced aspects of Cyber Crime, encompassing the Laws and its domains comprising many activities such as data breaches and all, and choose the relevant countermeasures.
9	**Teaching & Learning Scheme**	Classroom Instructions (CI): 45 hrs. | Self Learning (SL): 45 hrs. | Total: 90 hrs.
10	**Mode of Examination**	**Theory Only. CA: 25% | MTE: 15% | ETE: 60% | Total: 100 marks**
11	**Textbook**	Bryan Sullivan and Vincent Liu, Web Application Security: A Beginner's Guide, 1st Edition, McGraw-Hill Education, 2011, ISBN: 978-0071776165.
12	**References**	1. Andrew Hoffman, Web Application Security: Exploitation and Countermeasures for Modern Web Applications, 1st Edition, O'Reilly Media, 2020, ISBN: 978-1492053118. 2. Dafydd Studdard and Marcus Pinto, The Web Application Hacker's Handbook: Finding and Exploiting Security Flaws, 2nd Edition, Wiley, 2011, ISBN: 978-1118026472. 3. Michal Zalewski, The Tangled Web: A Guide to Securing Modern Web Applications, No Starch Press, 2011, ISBN: 978-1593273880.

3. Outline Syllabus with CO Mapping

All CO mappings in this section refer to Theory COs (CO1–CO6). This is a theory-only course; all assessment is via CA, MTE, and ETE.

	Topic	CO Mapping
Unit 1	**Introduction to Web Application Security**	
A	Need for secure web systems, evolution of web security threats, security goals and attack surface analysis	**CO1, CO3, CO4**
B	Proactive security development lifecycle, secure software development process, risk assessment methodologies	**CO1, CO3, CO5**
C	Fundamental security principles, threat modeling concepts, attacker mindset, vulnerability classification	**CO1, CO3, CO4**
Unit 2	**Secure Coding Practices and Common Vulnerabilities using C**	
A	Secure coding fundamentals, input validation, authentication basics, insecure coding practices	**CO2**
B	Common web vulnerabilities: buffer overflows, injection flaws, improper error handling	**CO2, CO4**
C	Vulnerability mitigation strategies, secure coding standards, defensive programming practices	**CO2, CO5**
Unit 3	**Secure Coding in C++ and Java for Web Applications**	
A	Dynamic memory management in web applications, common memory handling errors, secure resource management	**CO2, CO4**
B	Memory managers, double free vulnerabilities, memory corruption issues affecting web application security	**CO2, CO4**
C	Integer security vulnerabilities, insecure input handling, exception handling, and mitigation strategies for secure web applications	**CO2, CO5**
Unit 4	**Database and Web-Specific Input Security**	
A	Quoting user input, secure input validation, encoding and sanitization techniques	**CO2, CO6**
B	Use of stored procedures, building SQL statements securely, prepared statements and secure database interaction	**CO5, CO6**

C	SQL Injection, Cross-Site Scripting (XSS), Cross-Site Request Forgery (CSRF), attacks and remedies	CO2, CO4, CO6
Unit 5	**Software Security Engineering for Web Applications**	
A	Security requirements engineering, misuse cases, abuse cases, secure architecture principles	CO3, CO5
B	QUARE (Quality Requirements Engineering) process model, secure software design methodologies, threat analysis and risk mitigation approaches	CO4, CO5
C	Software security practices, architectural and design security knowledge, code review and deployment security considerations	CO1, CO2, CO3, CO6

4. Topic-wise Bloom's Taxonomy Level Mapping

S.No	Topic	L1 Remember	L2 Understand	L3 Apply	L4 Analyze	L5 Evaluate	L6 Create
1	1.A	□	□		□		
2	1.B		□	□	□		□
3	1.C	□	□		□	□	
4	2.A	□	□	□			
5	2.B	□	□	□	□		
6	2.C		□	□	□	□	
7	3.A	□	□	□			
8	3.B	□	□	□	□		
9	3.C		□	□	□	□	
10	4.A	□	□	□			
11	4.B	□	□	□	□		
12	4.C	□	□	□	□	□	
13	5.A	□	□		□		□
14	5.B		□	□	□	□	

15	5.C		□	□	□	□	□

5. CO vs Bloom's Taxonomy — All Three Domains

ℹ *Only strong/dominant alignments are mapped. This is a theory-only course; Psychomotor mapping is limited to Guided Response (P3) for algorithm implementation in CO3. Affective domain appears at A3 (Valuing) for efficiency analysis in CO4 and CO5.*

CO	Cognitive Domain (L1–L6)						Affective (A1–A5)					Psychomotor (P1–P7)						
CO	L1	L2	L3	L4	L5	L6	A1	A2	A3	A4	A5	P1	P2	P3	P4	P5	P6	P7
CO1	□	□					□											
CO2		□	□	□				□					□	□				
CO3		□	□	□			□						□	□				
CO4				□	□				□									
CO5			□	□	□	□			□					□	□			
CO6		□	□	□	□			□					□	□				

Legend: □ = Strong / Dominant mapping. Theory-only course: Cognitive domain is primary. Psychomotor (P3) limited to CO3 (algorithm implementation). Affective (A3) for CO4 and CO5 (valuing efficiency).

6. Lecture Plan Outline (Theory — 45 Lectures / 45 Hours)

ℹ *Total classroom contact: 45 hours across 5 units. Self-Learning activities (45 hrs.) are structured separately in Section 11.*

Date	Topics to be Covered/Title	UNIT	Total Lectures
DD/MM/YYYY	Introduction to Web Application Security and Course Overview	Unit 1	10
DD/MM/YYYY	Need for Secure Web Systems		
DD/MM/YYYY	Evolution of Web Security Threats		
DD/MM/YYYY	Security Goals: Confidentiality, Integrity, Availability		

DD/MM/YYYY	Attack Surface Analysis in Web Applications		
DD/MM/YYYY	Secure Software Development Lifecycle (SSDLC)		
DD/MM/YYYY	Proactive Security Development Process		
DD/MM/YYYY	Risk Assessment Methodologies		
DD/MM/YYYY	Security Principles and Best Practices		
DD/MM/YYYY	Threat Modeling Concepts and Vulnerability Classification		
DD/MM/YYYY	Introduction to Secure Coding Practices	**Unit 2**	**10**
DD/MM/YYYY	Common Insecure Coding Practices		
DD/MM/YYYY	Input Validation Principles		
DD/MM/YYYY	Buffer Overflow Vulnerabilities		
DD/MM/YYYY	Injection Flaws and Exploits		
DD/MM/YYYY	Improper Error Handling		
DD/MM/YYYY	Defensive Programming Concepts		
DD/MM/YYYY	Secure Coding Standards		
DD/MM/YYYY	Vulnerability Mitigation Techniques		
DD/MM/YYYY	Dynamic Memory Management in Web Applications	**Unit 3**	**9**
DD/MM/YYYY	Memory Allocation and Deallocation Errors		
DD/MM/YYYY	Secure Resource Management		
DD/MM/YYYY	Memory Managers and Secure Handling		
DD/MM/YYYY	Double Free Vulnerabilities		
DD/MM/YYYY	Memory Corruption in Web Applications		
DD/MM/YYYY	Integer Overflow and Underflow Issues		
DD/MM/YYYY	Input Handling and Exception Security		
DD/MM/YYYY	Mitigation Strategies for Secure Web Applications		
DD/MM/YYYY	Secure Input Validation and Sanitization	**Unit 4**	**8**
DD/MM/YYYY	Quoting User Input Securely		
DD/MM/YYYY	Stored Procedures and Secure Database Access		
DD/MM/YYYY	Building SQL Statements Securely		
DD/MM/YYYY	Prepared Statements and Parameterized Queries		
DD/MM/YYYY	SQL Injection Attacks		
DD/MM/YYYY	Cross-Site Scripting (XSS)		

DD/MM/YYYY	Cross-Site Request Forgery (CSRF)		
DD/MM/YYYY	Security Requirements Engineering	Unit 5	9
DD/MM/YYYY	Misuse Cases in Secure Software Design		
DD/MM/YYYY	Abuse Cases in Security Engineering		
DD/MM/YYYY	QUARE Process Model		
DD/MM/YYYY	Secure Design Methodologies		
DD/MM/YYYY	Threat Analysis and Risk Mitigation		
DD/MM/YYYY	Software Security Practices		
DD/MM/YYYY	Architectural Security Principles		
DD/MM/YYYY	Code Review and Deployment Security		

PART II

THEORY ASSESSMENT FRAMEWORK

Theory Skill Dimensions, CO × TS Mapping, CA / MTE / ETE Structure

7. Theory Skill Dimensions (TS1–TS6)

THEORY-ONLY COURSE — All 6 COs (CO1–CO6) are assessed exclusively via Continuous Assessment (CA), MTE, and ETE. No laboratory component.

Six Theory Skill Dimensions — one per Bloom's progression (L1–L4) — correspond directly to the six COs. They define precisely what competency is being measured in each section of the CA, MTE, and ETE, providing a clear NBA-auditable assessment rationale.

ID	Dimension	What is Measured	CO / BTL	Assessment
TS1	**Conceptual Recall & Security Fundamentals**	Recall fundamental web security terminology, security principles, threat categories, attack surface concepts, and secure development lifecycle fundamentals	CO1 | L1–L2	CA | MTE Sec A | ETE Sec A
TS2	**Secure Coding Interpretation & Vulnerability Identification**	Explain secure coding principles, identify insecure coding practices, interpret vulnerability scenarios including buffer overflow, memory misuse, and unsafe input handling	CO2 | L2–L3	CA | MTE Sec A | ETE Sec A

TS3	**Security Application & Secure Implementation**	Apply secure coding practices, database security techniques, secure input validation, and mitigation strategies in web application contexts	CO3 / CO6 | L3	CA | MTE Sec B | ETE Sec B
TS4	**Threat Analysis & Security Evaluation**	Analyze attack scenarios, vulnerability exploitability, limitations of security mechanisms, and compare mitigation effectiveness across techniques	CO4 | L4–L5	MTE Sec B | ETE Sec B
TS5	**Secure Design & Software Security Engineering**	Evaluate secure architecture principles, threat modeling outputs, QUARE model usage, and software security engineering practices for robust application design	CO5 | L4–L5	ETE Sec B/C
TS6	**Database & Web Attack Investigation**	Analyze web-specific attack vectors such as SQL Injection, XSS, CSRF, database vulnerabilities, and assess remediation strategies through case-based evaluation	CO6 | L3–L5	ETE Sec C

8. CO × Theory Skill Dimension Mapping (6 COs × 6 Dimensions)

ℹ *Each CO maps primarily to one TS dimension (H) with adjacent dimensions receiving secondary mapping (M), reflecting the progressive Bloom's structure of this course.*

CO	TS1 Conceptual Recall	TS2 Process Interpretation	TS3 Algorithmic Application	TS4 Performance Evaluation	TS5 Memory System Analysis	TS6 File & Disk Evaluation
CO1	**H**	**M**				
CO2	**M**	**H**	**M**			
CO3	**M**		**H**	**M**		
CO4			**M**	**H**	**M**	
CO5				**M**	**H**	**M**
CO6		**M**	**M**	**M**		**H**

H = High / Primary alignment **M** = Medium / Secondary alignment *Blank = No direct alignment*

9. Continuous Assessment (CA) — 25 Marks

CA is formative and covers COs progressively as the syllabus is taught. It includes numerical-based assignments, a technical video learning report, and a real-world case study — mirroring TS1 through TS6.

9.1 CA Component Breakdown (Sample)

Component	Quantum	Marks	COs Assessed	Skill Dimensions
Assignments 1–5 (Problem-based / Vulnerability Analysis / Secure Coding Tasks)	5 Assignments	15	CO1, CO2, CO3, CO6	TS1, TS2, TS3, TS4
Technical Video Learning Report + Presentation	1 Report + Presentation	5	CO1, CO3, CO4	TS2, TS3, TS4
Real-World Case Study (Security Incident / Web Attack Analysis Report)	1 Report	5	CO4, CO5, CO6	TS4, TS5, TS6
TOTAL	—	25	CO1–CO6	TS1–TS6

9.2 Assignment-wise CO & TS Mapping

Item	Topic / Focus	COs	TS Dims	SL Hours	Evaluation Criteria
Assignment 1	Unit 1 concepts: web security fundamentals, threat landscape, security goals, threat modeling	**CO1, CO3**	**TS1, TS2**	**5h SL**	Conceptual problem-solving, short analytical report, vulnerability identification
Assignment 2	Secure coding practices: insecure coding examples, buffer overflow, input validation issues	**CO2**	**TS2, TS3**	**5h SL**	Code analysis, vulnerability identification, mitigation strategy explanation
Assignment 3	Secure coding in C++/Java: memory vulnerabilities, integer overflow, secure resource handling	**CO2, CO4**	**TS2, TS3**	**5h SL**	Secure coding exercises, vulnerability tracing, comparative mitigation analysis
Assignment 4	Database and web-specific attacks: SQL Injection, XSS, CSRF, secure query building	**CO4, CO6**	**TS3, TS4**	**5h SL**	Attack scenario analysis, remediation design, secure implementation recommendations

Assignment 5	Software security engineering: misuse cases, abuse cases, QUARE model, secure design practices	**CO5, CO6**	**TS4, TS5**	**5h SL**	Secure architecture/design solution, threat analysis, justification of design choices
Video Learning Report	Technical video on web security tools/secure coding practices/OWASP Top 10 (minimum 3 hrs); structured report + class presentation	**CO1, CO3, CO4**	**TS2, TS3, TS4**	**9h SL**	Report covering learning outcomes, concepts understood, vulnerability insights, self-reflection; Presentation (10 min)
Case Study Report	Real-world web application security incident (e.g., SQL injection breach, XSS exploit, authentication bypass, major web attack case); detailed technical analysis	**CO4, CO5, CO6**	**TS4, TS5, TS6**	**6h SL**	Technical depth, incident analysis, attack vector identification, mitigation recommendations, comparative evaluation

10. Mid Term Examination (MTE) — 15 Marks (Units 1–3)

ℹ *MTE covers Units 1–3 (CO1, CO2, CO3, CO4). CO5 and CO6 are assessed in ETE only. MTE maps to TS1–TS4.*

Section	Marks	Theory Skill Dimensions	COs Assessed	Question Type & Guidance
Section A	**10**	TS1 — Conceptual Recall & Security Fundamentals TS2 — Secure Coding Interpretation & Vulnerability Identification	**CO1, CO2, CO3**	**Short-answer:** define web security concepts, explain security principles, threat modeling, secure development lifecycle, identify common vulnerabilities, explain secure coding practices, memory handling/security flaws
Section B	**15**	TS3 — Security Application & Secure Implementation TS4 — Threat Analysis & Security Evaluation	**CO2, CO3, CO4**	**Analytical/application questions:** analyze vulnerability scenarios, identify insecure code and suggest remediation, apply secure coding principles, compare mitigation techniques, evaluate attack scenarios and security mechanisms
TOTAL	**25**	**TS1–TS4**	**CO1–CO4**	**Units 1–3 only. CO5 and CO6 assessed in ETE only.**

11. End Term Examination (ETE) — 60 Marks (All Units, All COs)

ℹ *ETE is comprehensive — all 5 units and all 6 COs. Full progression from TS1 (recall) through TS6 (evaluation). Minimum 20/50 required to pass.*

Section	Marks	Theory Skill Dimensions	COs Assessed	Question Type & Guidance
Section A	15	TS1 — Conceptual Recall & Security Fundamentals TS2 — Secure Coding Interpretation & Vulnerability Identification	CO1, CO2, CO3	Short questions (all units): definitions of web security concepts, threat identification, security principles, secure development lifecycle, secure coding concepts, vulnerability identification, threat modeling, memory/security flaw concepts
Section B	25	TS3 — Security Application & Secure Implementation TS4 — Threat Analysis & Security Evaluation TS5 — Secure Design & Software Security Engineering	CO3, CO4, CO5	Medium questions: secure coding analysis, vulnerability mitigation design, SQL injection/XSS attack analysis, secure database implementation, threat analysis, QUARE model application, software security engineering case-based questions
Section C	10	TS5 — Secure Design & Software Security Engineering TS6 — Database & Web Attack Investigation	CO5, CO6	Long/evaluation questions: secure architecture evaluation, software security practices, database security analysis, SQL injection/XSS/CSRF case study analysis, mitigation strategy evaluation, real-world web security incident analysis
TOTAL	50	TS1–TS6 (all)	CO1–CO6	Scaled from 100-mark paper if needed. Minimum 20/50 to pass.

11.1 CO-wise Assessment Instrument Summary

CO	CO Statement (Short)	CA (25)	MTE (25)	ETE (50)	TS	PO Primary
CO1	Understand fundamental concepts, principles, and threats in web application security	□	□	□	TS1	PO1, PO2, PO8
CO2	Identify insecure coding practices and apply mitigation techniques in web applications	□	□	□	TS2	PO1, PO2, PO3, PO5
CO3	Understand IT infrastructure and foundational web application security mechanisms	□	□	□	TS3	PO1, PO2, PO5
CO4	Analyze challenges, threats, vulnerabilities, and limitations of security techniques	□	□	□	TS4	PO2, PO4, PO8

CO5	Design and apply secure software engineering and web security solutions	□	—	□	TS5	PO3, PO4, PO5, PO12
CO6	Examine database security and web-specific attack vectors and mitigation strategies	□	—	□	TS6	PO2, PO4, PO5

□ *CO5 and CO6 are NOT assessed in MTE (only Units 1–3 are covered at mid-semester). They are assessed in CA (self-learning activities) and ETE.*

PART III

COMBINED MAPPINGS & REFERENCE

CO–PO Matrix, CO–PO Alignment, Self-Learning Activities, Bloom's Reference, Attendance & Pass/Fail

12. CO–PO and CO–PSO Mapping Matrix (Original Framework)

ℹ *Strength Scale: 3 = Substantial (High) | 2 = Moderate | 1 = Slight (Low) | - = Not Applicable. Averages computed over non-zero entries only. PO framework as per the original course design.*

CO	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PO12	PSO1	PSO2	PSO3
CO1	3	3	-	-	2	-	-	3	-	-	-	3	-	-	3
CO2	3	3	2	-	-	-	-	-	-	-	-	-	-	-	3
CO3	3	3	2	-	2	-	-	-	2	-	-	2	3	-	3
CO4	3	3	-	3	2	3	-	2	-	-	-	-	-	3	3
CO5	3	2	3	-	-	-	-	3	3	-	-	-	-	3	3
CO6	3	3	-	3	3	3	3	-	-	3	3	-	3	-	3
Avg	3.00	2.83	2.33	3.00	2.25	3.00	3.00	2.67	2.50	3.00	3.00	2.50	3.00	3.00	3.00

13. CO × PO Alignment Map (H/M Indicators — All 6 COs)

CO	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PSO1	PSO2	PSO3
CO1	H	H			M			H				H		
CO2	H	H	M											
CO3	H	H	M		M				M			M	H	
CO4	H	H		H	M	H		M						H
CO5	H	M	H					H	H					H
CO6	H	H		H	H	H	H			H	H		H	

= High / Primary alignment **M** = Medium / Secondary alignment *Blank = No direct alignment*

14. Self-Learning Activities (SL: 45 Hours)

S.No	Activity	Hours	COs / TS	Evaluation Criteria
1	**Assignment Writing (5 assignments, one per unit focus area covering web security concepts, secure coding, vulnerability analysis, database/web attacks, software security engineering)**	5 assignments × 5 hrs. each Total = 25 hrs.	CO1–CO6 TS1–TS5	Evaluated based on assignment submission, conceptual clarity, vulnerability identification, mitigation strategy design, secure coding correctness, analytical justification
2	**Technical Video-Based Learning related to Web Application Security (e.g., OWASP Top 10, secure coding practices, SQL Injection/XSS prevention, threat modeling, software security engineering)**	Video viewing: 3 hrs. Report preparation: 3 hrs. Presentation: 3 hrs. Total = 9 hrs.	CO2, CO3, CO4 TS2, TS3, TS4	Report + presentation based on technical understanding, learning outcomes, secure development insights, vulnerability interpretation, and self-reflection
3	**Real-World Web Security Case Studies (e.g., Equifax breach, SQL injection attacks, XSS exploitation, authentication bypass incidents, web application vulnerability disclosures)**	Data collection / study: 4 hrs. Report preparation: 4 hrs. Presentation / discussion: 3 hrs. Total = 11 hrs.	CO4, CO5, CO6 TS4, TS5, TS6	Evaluated based on technical depth, attack analysis, factual investigation, security weakness identification, mitigation recommendations, comparative evaluation
	TOTAL Self-Learning Hours	45 Hours	CO1–CO6	All activities are compulsory. Submission deadlines communicated at the start of the semester.

15. Bloom's Taxonomy — Domain Level Reference

Cognitive Domain (6 Levels)	Affective Domain (5 Levels)	Psychomotor Domain — Simpson (7 Levels)
L1 — Remember: Recall facts, definitions, basic concepts L2 — Understand: Explain ideas, concepts, and principles L3 — Apply: Use knowledge to solve problems in new situations L4 — Analyze: Break down information, examine relationships L5 — Evaluate: Judge, justify, assess, and make decisions L6 — Create: Design, develop, and produce new artefacts	A1 — Receiving: Awareness and willingness to attend A2 — Responding: Active participation and reaction A3 — Valuing: Commitment and assigning value to content A4 — Organizing: Integrating values into a personal system A5 — Characterizing: Internalized value system	P1 — Perception: Sensory cues guide motor activity P2 — Set: Mental, physical readiness to act P3 — Guided Response: Practice through imitation/trial P4 — Mechanism: Habitual correct performance P5 — Complex Overt Response: Skilled performance P6 — Adaptation: Modify skills for special situations P7 — Origination: Create new solution patterns

 OBE Compliance Statement: This is a theory-only course. All 6 COs are mapped primarily to the Cognitive domain (L1–L5). Psychomotor domain (P3) appears only for CO3 (algorithm implementation as mental tracing). Affective domain (A3) appears for CO4 and CO5, reflecting valuing of algorithmic efficiency.

16. Attendance Policy & Pass / Fail Criteria

16.1 Attendance Policy

Component	Minimum	Applicable To	Consequence
Theory Classes	**75%**	All lecture sessions	Debarred from ETE if below threshold
Self-Learning / Assignment Submission	**All activities**	SL activities (45 hrs.)	Incomplete SL affects CA score directly

 Theory attendance must meet 75% minimum. Missing SL activities (assignments, video report, case study) directly impacts CA marks and is not compensable by exam performance.

16.2 Pass / Fail Criteria

Condition	Threshold	Status	Remarks
ETE Score	≥ 24 / 60	**MANDATORY**	40% of ETE paper required; failing ETE means failing the course regardless of CA + MTE
Overall Total (CA + MTE + ETE)	≥ 40 / 100	**Must pass overall**	CA 25 + MTE 25 + ETE 50 = 100; 40% overall minimum required

CSCF3202— MEASUREMENT ARCHITECTURE SUMMARY

Theory-Only Course | 6 COs (CO1–CO6) | 3 Assessment Instruments | 6 Theory Skill Dimensions (TS1–TS6)

CO1–CO2: Conceptual / Understand → TS1, TS2 → CA + MTE Sec A + ETE Sec A

CO3–CO4: Apply / Analyze → TS3, TS4 → CA + MTE Sec B + ETE Sec B

CO5–CO6: Analyze / Evaluate → TS5, TS6 → CA + ETE Sec B/C

CA 25 marks + MTE 25 marks + ETE 50 marks = Total 100 marks

COURSE PLAN

Malware Analysis (CSCF3203)

Sharda School of Computing Science & Engineering | B.Tech CSE | Semester VI | Batch 2026–2030

Theory-Only Course Plan — All 6 COs (CO1–CO6) | Theory Skill Dimensions TS1–TS6 | CA + MTE + ETE Assessment

PART I

COURSE SYLLABUS

Course Identification, Details, Outcomes, BTL Mapping & Lecture Plan

1. Course Identification

School:	SSCSE-Sharda School of Computing Science & Engineering	**Batch:**	2026-2030
Program:	B.Tech	**Current Academic Year:**	2026-27
Branch:	CSE	**Semester:**	VI
Course Code:	CSCF3203	**Course Type:**	Theory Only

2. Course Details

 THEORY-ONLY COURSE — All 6 COs (CO1–CO6) are assessed exclusively via Continuous Assessment (CA), MTE, and ETE. No laboratory component.

S.No	Attribute	Details
1	**Course Code**	**CSCF3203**
2	**Course Title**	**Malware Analysis**
3	**Credits**	3

4	**Contact Hours (L-T-P-SL)**	3-0-0-3 (Theory: 45 hrs Classroom + 45 hrs Self Learning = 90 hrs total)
5	**Course Status**	**Core — Theory Only (No Laboratory Component) Elective**
6	**Course Objectives**	7. Introduce the fundamentals of malware, operating system security concepts, and the challenges posed by evolving malware threats. 8. Provide knowledge of different malware types, malware analysis methodologies, and techniques for static and dynamic malware analysis. 9. Develop the ability to use malware analysis tools and virtualized environments for examining malicious software behavior and system impact. 10. Enable students to analyze malware functionality including persistence mechanisms, privilege escalation, rootkits, and code injection techniques. 11. Familiarize students with modern malware detection approaches including signature-based, behavior-based, and machine learning techniques through practical case studies.
7	**Course Outcomes (COs)**	**After successful completion of this course, students will be able to:** CO1 (Understand – L1/L2) Identify and understand the fundamental concepts of malware, operating system security principles, malware evolution, threats, and different categories of malicious software. CO2 (Explore – L2/L3) Explore various malware analysis methodologies including static and dynamic analysis techniques, malware structures, and analysis environments. CO3 (Apply – L3) Apply static malware analysis techniques using antivirus scanning, hashing, string analysis, PE file examination, packed malware identification, and virtual machine configuration. CO4 (Analyze – L4) Analyze malware behavior using dynamic analysis tools such as sandboxes, process monitoring, registry analysis, packet sniffing, and network simulation tools. CO5 (Analyze – L4/L5) Analyze malware functionality including persistence mechanisms, privilege escalation, rootkits, process injection, covert launching techniques, and credential stealing methods. CO6 (Evaluate – L5) Evaluate and compare malware detection techniques including signature-based, similarity-based, machine learning approaches, and mobile malware case studies for application security. I/O management techniques, and analyze their comparative efficiency.
8	**Course Description**	This course introduces the fundamental concepts of malware analysis, malware behavior, and system security principles. It covers various types of malware, static and dynamic malware analysis techniques, malware functionality, persistence mechanisms, and covert attack methods. The course also provides hands-on exposure to malware analysis tools, virtualized analysis environments, network monitoring, and malware detection techniques including signature-based and machine learning approaches. Real-world malware case studies and smartphone application security are also discussed to develop practical skills in malware investigation and defense mechanisms.

9	**Teaching & Learning Scheme**	Classroom Instructions (CI): 45 hrs | Self Learning (SL): 45 hrs | Total: 90 hrs
10	**Mode of Examination**	**Theory Only. CA: 25% | MTE: 15% | ETE: 60% | Total: 100 marks**
11	**Textbook**	Michael Sikorski and Andrew Honig, "Practical Malware Analysis : The Hands-On Guide to Dissecting Malicious Software", No Starch Press,2012.
12	**References**	1. Jamie Butler and Greg Hoglund, "Rootkits: Subverting the Windows Kernel", Addison-Wesley, 2005. 2. Dang, Gazet, Bachaalany, "Practical Reverse Engineering", Wiley, 2014. 3. Reverend Bill Blunden, "The Rootkit Arsenal: Escape and Evasion in the Dark Corners of the System" Second Edition, Jones & Bartlett, 2012.

3. Outline Syllabus with CO Mapping

All CO mappings in this section refer to Theory COs (CO1–CO6). This is a theory-only course; all assessment is via CA, MTE, and ETE.

	Topic	CO Mapping
	Unit 1: Introduction	
A	The Goals of Malware Analysis, Introduction to malware, OS security concepts, malware threats, evolution of malware, General Rules for Malware Analysis	**CO1**
B	Malware types, viruses, worms, rootkits, Trojans, bots, spyware, adware, logic bombs	**CO2**
C	Malware analysis, Malware Analysis Techniques: Basic Static Analysis, Basic Dynamic Analysis, Advanced Static Analysis, Advanced Dynamic Analysis	**CO1**
	Unit 2: Static Analysis	
A	Antivirus Scanning: A Useful First Step, Hashing: A Fingerprint for Malware, Finding Strings, Packed and Obfuscated Malware, Portable Executable File Format, Linked Libraries and Functions	**CO2, CO6**

B	Static Analysis in Practice, PotentialKeylogger.exe: An Unpacked Executable, PackedProgram.exe: A Dead End, The PE File Headers and Sections	CO2, CO6
C	Malware analysis in virtual machines: The Structure of a Virtual Machine, Creating Your Malware Analysis Machine, Configuring VMware, Using Your Malware Analysis Machine	CO2, CO6
	Unit 3: Dynamic Analysis	
A	Sandboxes: The Quick-and-Dirty Approach, Using a Malware Sandbox, Sandbox Drawbacks, Running Malware, Monitoring with Process Monitor, The Procmon Display, Filtering in Procmon	CO3, CO6
B	Viewing Processes with Process Explorer: The Process Explorer Display, Using the Verify Option, Comparing Strings, Using Dependency Walker, Analyzing Malicious Documents. Comparing Registry Snapshots with Regshot, Faking a Network : Using ApateDNS, Monitoring with Netcat	CO3, CO6
C	Packet Sniffing with Wireshark, Using INetSim, Basic Dynamic Tools in Practice	CO3, CO6
	Unit 4: Malware Functionality	
A	Downloaders and Launchers, Backdoors, Credential Stealers	CO4
B	Persistence Mechanisms, Privilege Escalation, Covering Its Tracks—User-Mode Rootkits	CO4
C	Covert malware launching- Launchers, Process Injection, Process Replacement, Hook Injection, Detours, APC injection	CO4
	Unit 5: Malware Detection Techniques	
A	Signature-based techniques: malware signatures, packed malware signature, metamorphic and polymorphic malware signature	CO5, CO6
B	Non-signaturebased techniques: similarity-based techniques, machine-learning methods, invariant inferences	CO5, CO6
C	Case Studies – Plankton, DroidKungFu, AnserverBot, Smartphone (Apps) Security	CO5, CO6

4. Topic-wise Bloom's Taxonomy Level Mapping

S.No	Topic	L1 Remember	L2 Understand	L3 Apply	L4 Analyze	L5 Evaluate	L6 Create
1	1.A	□	□				
2	1.B	□	□				
3	1.C		□				
4	2.A		□	□			
5	2.B		□	□			
6	2.C			□	□		
7	3.A	□	□	✓			
8	3.B		✓	□	□		
9	3.C			□	□	□	
10	4.A		□				
11	4.B		✓	□	□		
12	4.C			□	□	□	□
13	5.A		□	□			
14	5.B		✓	□	□		□
15	5.C		□	□	□		□

5. CO vs Bloom's Taxonomy — All Three Domains

□ *Only strong/dominant alignments are mapped. This is a theory-only course; Psychomotor mapping is limited to Guided Response (P3) for algorithm implementation in CO3. Affective domain appears at A3 (Valuing) for efficiency analysis in CO4 and CO5.*

CO	Cognitive Domain (L1–L6)						Affective (A1–A5)					Psychomotor (P1–P7)						
CO	L1	L2	L3	L4	L5	L6	A1	A2	A3	A4	A5	P1	P2	P3	P4	P5	P6	P7
CO1	□	□																
CO2		□	□															
CO3			□	□											□			
CO4				□	□				□									
CO5				□	□			□										
CO6		□	□	□														

Legend: □ = Strong / Dominant mapping. Theory-only course: Cognitive domain is primary. Psychomotor (P3) limited to CO3 (algorithm implementation). Affective (A3) for CO4 and CO5 (valuing efficiency).

6. Lecture Plan Outline (Theory — 45 Lectures / 45 Hours)

□ *Total classroom contact: 45 hours across 5 units. Self-Learning activities (45 hrs) are structured separately in Section 11.*

Date	Topics to be Covered/Title	UNIT	Total Lectures
DD/MM/YY	Introduction to Malware Analysis and Cyber Threat Landscape	UNIT-1	9
DD/MM/YY	Goals and Importance of Malware Analysis		
DD/MM/YY	Operating System Security Concepts		
DD/MM/YY	Malware Threats and Evolution of Malware		
DD/MM/YY	General Rules and Safety Practices for Malware Analysis		
DD/MM/YY	Malware Types: Viruses and Worms		
DD/MM/YY	Malware Types: Rootkits, Trojans, Bots		

DD/MM/YY	Spyware, Adware, Logic Bombs		
DD/MM/YY	Malware Analysis Techniques: Static vs Dynamic Analysis Overview		
DD/MM/YY	Introduction to Static Malware Analysis	UNIT-2	9
DD/MM/YY	Antivirus Scanning and Malware Hashing		
DD/MM/YY	Finding Strings and Indicators in Malware		
DD/MM/YY	Packed and Obfuscated Malware		
DD/MM/YY	Portable Executable (PE) File Format		
DD/MM/YY	Linked Libraries and API Functions		
DD/MM/YY	Static Analysis in Practice: Unpacked Executables		
DD/MM/YY	PE Headers, Sections, and Packed Programs		
DD/MM/YY	Malware Analysis in Virtual Machines and VMware Configuratio		
DD/MM/YY	Introduction to Dynamic Malware Analysis	UNIT-3	9
DD/MM/YY	Malware Sandboxes and Their Limitations		
DD/MM/YY	Running Malware Safely in Controlled Environments		
DD/MM/YY	Monitoring Malware with Process Monitor (Procmon)		
DD/MM/YY	Process Explorer and Dependency Walker		
DD/MM/YY	Registry Monitoring using Regshot		
DD/MM/YY	Network Monitoring using ApateDNS and Netcat		
DD/MM/YY	Packet Sniffing with Wireshark and INetSim		
DD/MM/YY	Dynamic Analysis Tools in Practice and Case Demonstration		
DD/MM/YY	Malware Functionalities Overview	UNIT-4	9
DD/MM/YY	Downloaders and Launchers		
DD/MM/YY	Backdoors and Credential Stealers		

DD/MM/YY	Persistence Mechanisms in Malware		
DD/MM/YY	Privilege Escalation Techniques		
DD/MM/YY	User-Mode Rootkits and Covering Tracks		
DD/MM/YY	Covert Malware Launching Techniques		
DD/MM/YY	Process Injection, Process Replacement, Hook Injection		
DD/MM/YY	APC Injection and Detours Techniques		
DD/MM/YY	Introduction to Malware Detection Techniques	UNIT-5	9
DD/MM/YY	Signature-Based Malware Detection		
DD/MM/YY	Packed, Metamorphic, and Polymorphic Malware Signatures		
DD/MM/YY	Similarity-Based Detection Techniques		
DD/MM/YY	Machine Learning Methods for Malware Detection		
DD/MM/YY	Invariant Inference Techniques		
DD/MM/YY	Case Study: Plankton and DroidKungFu		
DD/MM/YY	Case Study: AnserverBot and Smartphone App Security		
DD/MM/YY	Course Review, Emerging Malware Trends, and Revision		

PART II

THEORY ASSESSMENT FRAMEWORK

Theory Skill Dimensions, CO × TS Mapping, CA / MTE / ETE Structure

7. Theory Skill Dimensions (TS1–TS6)

THEORY-ONLY COURSE — All 6 COs (CO1–CO6) are assessed exclusively via Continuous Assessment (CA), MTE, and ETE. No laboratory component.

Six Theory Skill Dimensions — one per Bloom's progression (L1–L4) — correspond directly to the six COs. They define precisely what competency is being measured in each section of the CA, MTE, and ETE, providing a clear NBA-auditable assessment rationale.

ID	Dimension	What is Measured	CO / BTL	Assessment
TS1	**Taxonomy & Fundamentals**	Recall malware types (rootkits, trojans, etc.) and evolution; identify general rules for analysis and OS security concepts.	CO1 | L1–L2	CA | MTE Sec A | ETE Sec A
TS2	**Interpretation Static Analysis Interpretation**	Explain PE file structures, hashing, and the role of linked libraries; interpret strings and headers to identify packed/obfuscated malware.	CO2 | L2–L3	CA | MTE Sec A | ETE Sec A
TS3	**Dynamic Analysis Application**	Apply sandboxing, Procmon filtering, and Regshot snapshots to trace malware behavior; execute basic network faking with ApateDNS.	CO3 | L3	CA | MTE Sec B | ETE Sec B
TS4	**Evaluation Behavioral Analysis & Trafficking**	Analyze network traffic using Wireshark/INetSim; evaluate differences between static and dynamic results to determine malware intent.	CO4 | L4–L5	MTE Sec B | ETE Sec B
TS5	**Advanced Persistence & Injection**	Analyze covert launching mechanisms (Process Injection, APC injection, Hooking); evaluate privilege escalation and user-mode rootkit stealth.	CO5 | L4–L5	ETE Sec B/C

TS6	**Detection Strategy & Case Evaluation**	Evaluate signature-based vs. non-signature (ML) techniques; apply detection theory to case studies like DroidKungFu or Plankton.	CO6 | L2–L4	ETE Sec C

8. CO × Theory Skill Dimension Mapping (6 COs × 6 Dimensions)

Each CO maps primarily to one TS dimension (H) with adjacent dimensions receiving secondary mapping (M), reflecting the progressive Bloom's structure of this course.

CO	TS1 Conceptual Recall	TS2 Process Interpretation	TS3 Algorithmic Application	TS4 Performance Evaluation	TS5 Memory System Analysis	TS6 File & Disk Evaluation
CO1	H	M				
CO2	M	H	M			
CO3		M	H	M		
CO4			M	H	M	
CO5				M	H	M
CO6		M		M	M	H

H = High / Primary alignment **M** = Medium / Secondary alignment *Blank = No direct alignment*

9. Continuous Assessment (CA) — 25 Marks

CA is formative and covers COs progressively as the syllabus is taught. It includes numerical-based assignments, a technical video learning report, and a real-world case study — mirroring TS1 through TS6.

9.1 CA Component Breakdown (Sample)

Component	Quantum	Marks	COs Assessed	Skill Dimensions

Assignments 1–5 (Analysis Problem-based)	5 assignments	**15**	CO1, CO2, CO3, CO4	TS1, TS2, TS3, TS4
Technical Video Learning Report	1 Report + Presentation	**5**	CO2, CO3	TS2, TS3
Real-World Case Study (Report)	1 Report	**5**	CO4, CO5, CO6	TS4, TS5, TS6
TOTAL	—	**25**	CO1–CO6	TS1–TS6

9.2 Assignment-wise CO & TS Mapping

Item	Topic / Focus	COs	TS Dims	SL Hours	Evaluation Criteria
Assignment 1	Unit 1 Fundamentals: Malware taxonomy, evolution, and analysis goals.	CO1	TS1	8h SL	Report submission + conceptual evaluation
Assignment 2	Static Analysis: PE file headers, hashing, and finding strings in PotentialKeylogger.exe.	CO2	TS2	8h SL	Technical report on PE structure & obfuscation
Assignment 3	Dynamic Analysis: Filtering Procmon logs and Regshot comparisons for behavior tracing.	CO3	TS3	8h SL	Log interpretation + behavioral trace analysis
Assignment 4	Network Analysis: Wireshark PCAP analysis and INetSim traffic simulation.	CO3, CO4	TS3, TS4	8h SL	Packet analysis report + traffic evaluation
Assignment 5	Covert Mechanisms: Analyzing Process Injection, Hooking, and APC injection logic.	CO4, CO5	TS4, TS5	8h SL	Comparative analysis of stealth mechanisms
Video Learning Report	Technical video on Malware Persistence or Detection (min 3 hrs); structured report + presentation.	CO5, CO6	TS5, TS6	5h SL	Report: learning outcomes, key concepts, self-reflection. Presentation: 10 min

10. Mid Term Examination (MTE) — 15 Marks (Units 1–3)

MTE covers Units 1–3 (CO1, CO2, CO3, CO4). CO5 and CO6 are assessed in ETE only. MTE maps to TS1–TS4.

Section	Marks	Theory Skill Dimensions	COs Assessed	Question Type & Guidance
Section A	10	TS1 — Malware Taxonomy & FundamentalsTS2 — Static Analysis & PE Interpretation	CO1, CO2	Short-answer: Define malware types (Rootkits/Trojans), explain the role of PE headers, describe hashing logic for fingerprints, and identify packed malware indicators.
Section B	15	TS3 — Dynamic Analysis ApplicationTS4 — Behavioral Analysis & Trafficking	CO2, CO3, CO4	Analytical problems: Interpret Procmon filter results; trace registry changes via Regshot; analyze Wireshark packet captures for malicious C2 traffic; compare sandbox results with basic dynamic tool output.
TOTAL	25	TS1–TS4	CO1–CO4	Units 1–3 only. CO5 (Covert Functionality) and CO6 (Detection Strategies) assessed in ETE only.

11. End Term Examination (ETE) — 60 Marks (All Units, All COs)

ETE is comprehensive — all 5 units and all 6 COs. Full progression from TS1 (recall) through TS6 (evaluation). Minimum 20/50 required to pass.

Section	Marks	Theory Skill Dimensions	COs Assessed	Question Type & Guidance
Section A	15	TS1 — Malware TaxonomyTS2 — Static Analysis Interpretation	CO1, CO2	Short questions (all units): definitions of malware types, PE file header components, hashing logic, identification of packed vs. obfuscated malware.
Section B	35	TS3 — Dynamic ApplicationTS4 — Behavioral AnalysisTS5 — Covert Functionality	CO3, CO4, CO5	Medium questions: Interpreting Procmon/Regshot logs, Wireshark packet analysis, tracing process injection steps (APC/Hooking), and analyzing persistence mechanisms.

Section C	10	TS5 — Stealth AnalysisTS6 — Detection & Case Evaluation	CO5, CO6	Long/evaluation questions: Comparing signature vs. ML detection methods, evaluating rootkit stealth techniques, and case study analysis (e.g., DroidKungFu).
TOTAL	60	TS1–TS6 (all)	CO1–CO6	Scaled from 100-mark paper if needed. Covers full course lifecycle from basic static analysis to advanced detection.

11.1 CO-wise Assessment Instrument Summary

CO	CO Statement (Short)	CA (25)	MTE (25)	ETE (50)	TS	PO Primary
CO1	Understand malware taxonomy, types, evolution, and analysis goals	✓	✓	✓	TS1	PO1, PO2, PO3, PO4
CO2	Interpret static analysis results, PE headers, and obfuscation methods	✓	✓	✓	TS2	PO1, PO3, PO4
CO3	Apply dynamic analysis tools to trace behavior and network activity	✓	✓	✓	TS3	PO1, PO2, PO3, PO4
CO4	Analyze and evaluate behavioral traces and traffic patterns	✓	✓	✓	TS4	PO9, PO10, PO11
CO5	Analyze advanced persistence and covert injection mechanisms	✓	—	✓	TS5	PO1, PO2, PO8, PO9, PO10
CO6	Evaluate detection techniques and modern malware case studies	✓	—	✓	TS6	PO1, PO2, PO10, PO11

CO5 and CO6 are NOT assessed in MTE (only Units 1–3 are covered at mid-semester). They are assessed in CA (self-learning activities) and ETE.

PART III

COMBINED MAPPINGS & REFERENCE

CO–PO Matrix, CO–PO Alignment, Self-Learning Activities, Bloom's Reference, Attendance & Pass/Fail

12. CO–PO and CO–PSO Mapping Matrix (Original Framework)

Strength Scale: 3 = Substantial (High) | 2 = Moderate | 1 = Slight (Low) | – = Not Applicable. Averages computed over non-zero entries only. PO framework as per the original course design.

CO	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PSO1	PSO2	PSO3
CO1	3	3	-	-	2	1	-	3	1	1	3	1	-	3
CO2	3	3	2	-	-	1	3	1	-	-	-	-	-	3
CO3	3	3	2	-	2	-	3	-	2	3	2	3	-	-
CO4	3	3	-	3	2	3	-	2	3	3	3	3	3	-
CO5	3	2	3	-	-	-	2	3	3	3	1	-	3	2
CO6	3	3	-	3	3	3	3	3	-	3	3	3	3	-
Avg	***3***	***2.88***	***1.16***	***1***	***1.5***	***1.33***	***1.83***	***2.0***	***1.5***	***2.16***	***2.0***	***1.66***	***1.5***	***1.33***

13. CO × PO Alignment Map (H/M Indicators — All 6 COs)

CO	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PSO1	PSO2	PSO3
CO1	H	H			M			H			H			H
CO2	H	H	M				H							H
CO3	H	H	M		M		H		M	H	M	H		

CO4	H	H		H	M	H		M	H	H	H	H	H	
CO5	H	M	H				M	H	H	H			H	M
CO6	H	H		H	H	H	H	H		H	H	H	H	

H = High / Primary alignment M = Medium / Secondary alignment Blank = No direct alignment

14. Self-Learning Activities (SL: 45 Hours)

S.No	Activity	Hours	COs / TS	Evaluation Criteria
1	Technical Video based learning related to the subject	Duration of video = 5h Report preparation & Presentation = 10h Total = 15h	CO1–CO4TS1–TS4	Report /presentation based on the video learning outcomes.
2	Mini Literature Review on a Technical Topic	Reading articles=10 h; Summary report= 5 h, Total=15 h	CO2, CO3, CO5TS2, TS3, TS5	Depth of literature review, comparison of approaches, referencing quality
3	Open-Source Project Contribution (GitHub based)	Repository study=5 h; Contribution/bug fix=10 h, Total=15 h	CO4, CO5, CO6TS4, TS5, TS6	Actual contribution, code quality, documentation and submission proof
	TOTAL Self-Learning Hours	45	CO1–CO6	All activities are compulsory. Submission deadlines communicated at the start of the semester.

15. Bloom's Taxonomy — Domain Level Reference

Cognitive Domain (6 Levels)	Affective Domain (5 Levels)	Psychomotor Domain — Simpson (7 Levels)
L1 — Remember: Recall facts, definitions, basic concepts	A1 — Receiving: Awareness and willingness to attend	P1 — Perception: Sensory cues guide motor activity

L2 — Understand: Explain ideas, concepts, and principles L3 — Apply: Use knowledge to solve problems in new situations L4 — Analyze: Break down information, examine relationships L5 — Evaluate: Judge, justify, assess, and make decisions L6 — Create: Design, develop, and produce new artefacts	A2 — Responding: Active participation and reaction A3 — Valuing: Commitment and assigning value to content A4 — Organizing: Integrating values into a personal system A5 — Characterizing: Internalized value system	P2 — Set: Mental, physical readiness to act P3 — Guided Response: Practice through imitation/trial P4 — Mechanism: Habitual correct performance P5 — Complex Overt Response: Skilled performance P6 — Adaptation: Modify skills for special situations P7 — Origination: Create new solution patterns

OBE Compliance Statement: This is a theory-only course. All 6 COs are mapped primarily to the Cognitive domain (L1–L5). Psychomotor domain (P3) appears only for CO3 (algorithm implementation as mental tracing). Affective domain (A3) appears for CO4 and CO5, reflecting valuing of algorithmic efficiency.

16. Attendance Policy & Pass / Fail Criteria

16.1 Attendance Policy

Component	Minimum	Applicable To	Consequence
Theory Classes	**75%**	All lecture sessions	Debarred from ETE if below threshold
Self-Learning / Assignment Submission	**All activities**	SL activities (45 hrs)	Incomplete SL affects CA score directly

Theory attendance must meet 75% minimum. Missing SL activities (assignments, video report, case study) directly impacts CA marks and is not compensable by exam performance.

16.2 Pass / Fail Criteria

Condition	Threshold	Status	Remarks
ETE Score	**≥ 24 / 60**	**MANDATORY**	40% of ETE paper required; failing ETE means failing the course regardless of CA + MTE
Overall Total (CA + MTE + ETE)	**≥ 40 / 100**	**Must pass overall**	CA 25 + MTE 25 + ETE 50 = 100; 40% overall minimum required

(…….)— MEASUREMENT ARCHITECTURE SUMMARY

Theory-Only Course | 6 COs (CO1–CO6) | 3 Assessment Instruments | 6 Theory Skill Dimensions (TS1–TS6)

CO1–CO2: Conceptual / Understand → TS1, TS2 → CA + MTE Sec A + ETE Sec A

CO3–CO4: Apply / Analyze → TS3, TS4 → CA + MTE Sec B + ETE Sec B

CO5–CO6: Analyze / Evaluate → TS5, TS6 → CA + ETE Sec B/C

CA 25 marks + MTE 25 marks + ETE 50 marks = Total 100 marks

COURSE PLAN

Cryptography and Network Defense (CSCF3303)

School of Computing Science & Engineering (SSCSE) | B.Tech CSE | Semester VI | Batch 2026–2030

Integrated Course Plan — Theory COs (CO1–CO6) + Lab COs (CO7–CO10) | New AICTE 11-PO Framework | Full Skill Mapping

PART I

COURSE SYLLABUS

Course Identification, Details, Outcomes, BTL Mapping & Lecture/Lab Plans

1. Course Identification

School:	SSCSE	**Batch:**	2026–2030
Program:	B.Tech	**Current Academic Year:**	2026–27
Branch:	CSE	**Semester:**	VI

2. Course Details

Integrated theory + laboratory model. 10 COs in two tiers: Theory COs (CO1–CO6) via MTE + ETE; Lab COs (CO7–CO10) via Laboratory Assessment only. No cross-evaluation.

S.No	Attribute	Details
1	**Course Code**	CSCF3303
2	**Course Title**	Cryptography and Network Defense / Cryptography and Network Defense Lab
3	**Credits**	4

4	**Contact Hours (L-T-P-SL)**	3-0-2-3
5	**Course Status**	Core
6	**Course Objective**	To provide students with an overview of Cryptography and essential security algorithms used in data communication across computer networks, forming the foundation of modern organizations worldwide, while enabling understanding of techniques like Advanced Encryption Standard and RSA algorithm to ensure secure and reliable information exchange.
7	**Course Outcomes (COs)**	**After successful completion of this course, the student will be able to:** **THEORY COs — Assessed via MTE + ETE:** CO1 (Remember– L1):Analyze the conventional Network security technique which are basically designed to maintain confidentiality. CO2 (Understand – L2):Compare the techniques of algorithms developed in modern cryptographic era. CO3 (Apply– L3):Explain the tools and methodologies used to perform Security analysis CO4 (Analyze – L4):Summarize the working knowledge of the Crytography application during Network Security to maintain security. CO5 (Evaluate – L5):Examine security at application layer, transport layer and network layer. CO6 (Create – L6): Interpret use of cryptographic data integrity algorithms and user authentication protocols **LAB COs — Assessed via Laboratory Assessment only:** CO7 (L4 – Analyze): Identify and analyze security vulnerabilities and attacks in cryptographic systems and networks. CO8 (L5/L6 – Create):Prepare and present structured security analysis reports for cryptographic and network security findings. CO9 (L3 – Apply):Collaborate with stakeholders to implement secure cryptographic and network security solutions. CO10 (L3 – Apply):Demonstrate ethical, legal, and professional conduct in Cryptography and Network Defense practices.
8	**Teaching & Learning**	Classroom Instructions (CI) 45 hrs + Lab Instructions (LI) 30 hrs + Self Learning (SL) 45 hrs = 120 hrs

9	**Mode of Examination**	Lab (40 marks) + MTE (10 marks) + ETE (50 marks) = 100 marks. Theory COs: MTE + ETE only. Lab COs: Lab only.
10	**Self Learning (SL: 45 hrs)**	4. Perform Network Scanning and Vulnerability Mapping using Nmap 5. Open Source Intelligence (OSINT) and Footprinting Analysis using Maltego 6. Packet Inspection and Traffic Analysis using Wireshark
11	**References**	Textbook: 3. Behrouz A. Forouzan, "Cryptography and Network Defense"- McGraw Hill. 4. **Cryptography and Network Defense: Principles and Practice** Author: William Stallings 5. Introduction to Modern Cryptography Authors: Jonathan Katz, Yehuda Lindell Edition: 4th Edition (2025) 6. Cryptography: Theory and Practice Author: Douglas R. Stinson, Maura Paterson Edition: 4th Edition

3. Outline Syllabus — Theory Units with CO Mapping (CO1–CO6)

Unit CO mappings refer to Theory COs (CO1–CO6) only. Lab experiments reinforce these units but are assessed under Lab COs (CO7–CO10).

	Topic / Activity	CO Mapping
Unit 1	**Introduction to Network Security & Ethics (8-0-0-6 = 14hrs)**	
A	Computer Security Concepts- OSI security Architecture, Security attacks, Services, mechanism, model of network security	CO1, CO2, CO3
B	Classical encryption techniques- Substitution Cipher (Mono-alphabetic, Poly-alphabetic), Transposition cipher, Steganography	

C	Block Cipher- Encryption Principles, DES & strength of DES	
Tools Used	NA	
Activities	**Objective:** • Understand computer security concepts, OSI security architecture, and network security models. • Learn classical encryption techniques including substitution, transposition, and steganography. • Apply block cipher principles and analyze Data Encryption Standard and its strength.	
Unit 2	**Mathematics of Cryptography (10-0-0-9= 19 hrs)**	
A	Euclidean, Extended Euclidean Algorithm, Euler's Totient Function, Ferment little Theorem, Euler's Theorem	CO3, CO4
B	Primality Testing-Miller Rabin test, Chinese Remainder Theorem	
C	Exponential- square and multiply method, Discrete Logarithm	
Tools Used	NA	
Activities	**Objective:** • Understand number theory concepts including Euclidean and Extended Euclidean algorithms, Euler's Totient function, Fermat's Little Theorem, and Euler's Theorem. • Learn primality testing methods such as Miller–Rabin test and apply the Chinese Remainder Theorem. • Apply modular exponentiation using square-and-multiply method and analyze discrete logarithm problems.	
Unit 3	**Asymmetric Cryptography & Key Exchange (9-0-0-10 = 19 hrs)**	
A	Public Key cryptography-RSA, Cryptanalysis of RSA	CO2, CO3, CO4

B	Key management & distribution: KDC	
C	Diffie Hellman key exchange	
Tools Used	NA	
Activities	**Objective:** • Understand public key cryptography concepts and implementation of RSA algorithm along with its cryptanalysis. • Learn key management and secure key distribution using Key Distribution Centers (KDC). • Apply secure key exchange mechanisms such as Diffie-Hellman key exchange.	
Unit 4	**Digital Signatures and MAC (9-0-0-10 = 19 hrs)**	
A	User Authentication protocol- Kerberos, Digital Signature –RSA, Elgamal	CO3, CO4, CO6
B	DSS, Data integrity algorithms-Hash Functions, MD5,SHA512	
C	Message Authentication Code, HMAC	
Tools Used	NA	
Activities	**Objective:** • Understand public key cryptography concepts and implementation of RSA algorithm along with its cryptanalysis. • Learn key management and secure key distribution using Key Distribution Centers (KDC).	
Unit 5	**Quantum Cryptography (9-0-0-10 = 19 hrs)**	
A	Classical vs Quantum systems , Qubits and state representation ,Superposition , Measurement and collapse, Heisenberg uncertainty principle , Quantum entanglement	CO5, CO6

B	Mathematical Model for Quantum Mechanics, Single and multi-qubit quantum gates and circuits	
C	Quantum Key Distribution (QKD), Types of Quantum Key Distribution, QKD attack methods	
Tools Used	NA	
Activities	**Objective:** • Understand fundamental concepts of quantum mechanics applied to cryptography. • Analyze quantum principles like superposition and entanglement for secure communication. • Implement and evaluate Quantum Key Distribution (QKD) protocols.	

4. Topic-wise Bloom's Taxonomy Level Mapping (Theory)

S.No	Topic	L1	L2	L3	L4	L5	L6
1	1.A	□	□				
2	1.B		□	□			
3	1.C		□	□			
4	2.A			□			
5	2.B			□			
6	2.C			□	□		
7	3.A			□	□		□
8	3.B		□	□		□	
9	3.C			□	□		
10	4.A			□	□		

11	4.B			□	□	□	
12	4.C			□			
13	5.A		□	□		□	□
14	5.B			□	□		
15	5.C			□	□	□	

5. CO vs Bloom's Taxonomy — All Three Domains (Updated for 10 COs)

□ *Only strong/dominant alignments are mapped. Lab COs (CO7–CO10) extend into Psychomotor and Affective domains, reflecting the skill-based nature of lab and project work.*

CO	Cognitive Domain (L1–L6)						Affective (A1–A5)					Psychomotor (P1–P7)						
CO	L1	L2	L3	L4	L5	L6	A1	A2	A3	A4	A5	P1	P2	P3	P4	P5	P6	P7
CO1	□																	
CO2		□																
CO3			□											□				
CO4				□											□			
CO5					□											□		
CO6						□			□							□	□	
CO7			□		✓			□					✓	□	□			
CO8					□	□			□						□	□	□	
CO9			□							□	□							
CO10			□					□			□			□			✓	

Legend: □ = Strong / Dominant mapping only. Theory COs: primarily Cognitive. Lab COs: span all three domains.

6. Lecture Plan Outline (Theory — 45 Lectures)

Date	Topics to be Covered	Unit	Total Lectures
DD/MM/YY	Computer Security Concepts- OSI security Architecture	**UNIT-1**	**8**
DD/MM/YY	Security attacks		
DD/MM/YY	Services, mechanism,		
DD/MM/YY	model of network security		
DD/MM/YY	Classical encryption techniques- Substitution Cipher (Mono-alphabetic, Poly-alphabetic)		
DD/MM/YY	Transposition cipher, Steganography		
DD/MM/YY	Block Cipher- Encryption Principles		
DD/MM/YY	DES & strength of DES		
DD/MM/YY	Mathematics in Cryptography	**UNIT-2**	**10**
DD/MM/YY	Euclidean		
DD/MM/YY	Extended Euclidean Algorithm		
DD/MM/YY	Euler's Totient Function		
DD/MM/YY	Ferment little Theorem		
DD/MM/YY	Euler's Theorem		
DD/MM/YY	Primality Testing-		
DD/MM/YY	Miller Rabin test,		
DD/MM/YY	Chinese Remainder Theorem		
DD/MM/YY	Exponential- square and multiply method,		
DD/MM/YY	Discrete Logarithm		
DD/MM/YY	Public Key cryptography	**UNIT-3**	**9**
DD/MM/YY	RSA		
DD/MM/YY	Cryptanalysis of RSA		
DD/MM/YY	Key management & distribution		
DD/MM/YY	KDC		
DD/MM/YY	Key Management		
DD/MM/YY	Diffie Hellman key exchange		
DD/MM/YY	Attacks on Diffie-Hellman		
DD/MM/YY	Applications of Diffie-Hellman		
DD/MM/YY	User Authentication protocol	**UNIT-4**	**9**

DD/MM/YY	Kerberos		
DD/MM/YY	Digital Signature –RSA		
DD/MM/YY	Elgamal		
DD/MM/YY	DSS, Data integrity algorithms-Hash Functions		
DD/MM/YY	MD5,SHA512		
DD/MM/YY	Message Authentication Code		
DD/MM/YY	HMAC		
DD/MM/YY	Classical vs Quantum systems	**UNIT-5**	**9**
DD/MM/YY	Qubits and state representation		
DD/MM/YY	Superposition		
DD/MM/YY	Measurement and collapse		
DD/MM/YY	Heisenberg uncertainty principle , Quantum entanglement		
DD/MM/YY	Mathematical Model for Quantum Mechanics,		
DD/MM/YY	Single and multi-qubit quantum gates and circuits		
DD/MM/YY	Quantum Key Distribution (QKD)		
DD/MM/YY	Types of Quantum Key Distribution		
DD/MM/YY	QKD attacks		

7. Lab Session Plan — List of Experiments (Updated CO7–CO10)

W1–W12: All experiments develop CO7 skills (professional implementation, tool usage, documentation). W13–W15 (teal rows): CO8 (design/real-world), CO9 (ethics/reflection), CO10 (teamwork/presentation). Theory knowledge is applied but NOT re-evaluated in lab.

Week	Session	Experiment	Lab CO	Marks
W1	S-1	Perform the following implementation Encryption and Decryption with Ceaser cipher	**CO7**	3.0
		.		
W2	S-2	Perform the following implementation Encryption and Decryption with Playfair cipher	**CO7**	3.0
W3	S-3	Perform the following implementation	**CO7**	3.0

		Encryption and Decryption with Vigenere cipher		
W4	S-4	Perform the following implementation Encryption and Decryption with Hill cipher	**CO7**	3.0
W5	S-5	Perform the following implementation encryption and decryption Transposition using Rail Fence Cipher	**CO7**	3.0
W6	S-6	Perform the following implementation encryption and decryption Transposition using Columnar Transposition	**CO7**	3.0
W7	S-7.	Perform the following implementation encryption and decryption Implement Euclidean Algorithm to compute GCD of two number	**CO7**	3.0
W8	S-8	Perform the following implementation: Encryption and Decryption with DES	**CO8/CO9**	3.0
W9	S-9	Perform the following implementation: Encryption and Decryption with 3-DES	**CO8/CO10**	3.0
W10	S-10	Perform the following implementation: Encryption and Decryption with AES	**CO9/CO10**	3.0
W11	S-11	Perform the following implementation Encryption and Decryption with RSA	**CO7**	3.0

W12	S-12	Perform the following implementation Encryption and Decryption with Diffie-Hellman	**CO7**	3.0
W13	S-13	Perform the following implementation Digital signature of data using RSA	**CO8**	3.0
W14	S-14	Perform the following implementation Digital signature of data using Diffie-Hellman	**CO8/CO9**	3.0
W15	S-15	Implement ElGamal Digital Signature Algorithm.	**CO8/CO9**	3.0

Instructions: Write C programs, compile, execute and test with suitable test cases. Lab record (aim, algorithm, code, output, result) must be submitted before the next session.

PART II

THEORY ASSESSMENT FRAMEWORK

Theory Skill Dimensions, MTE & ETE Structure for Theory COs (CO1–CO6)

8. Theory Skill Dimensions (TS1–TS6) — CO1 through CO6

THEORY COs (CO1–CO6) — Assessed exclusively via MTE and ETE only

Six theory skill dimensions — one per Bloom's level L1–L6 — correspond directly to CO1–CO6. They define the competency measured in each section of MTE and ETE, providing a clear NBA-auditable assessment rationale.

ID	Dimension	What is Measured	CO / BTL	Assessment
TS1	**Factual Recall & Conceptual Recognition**	Recall cryptography terminology, security principles, encryption techniques, network security models, cipher types, authentication concepts, and hashing algorithms	CO1 | L1–L2	MTE Sec A | ETE Sec A
TS2	**Conceptual Explanation & Logical Interpretation**	Explain classical and modern cryptographic algorithms, security attacks, authentication protocols, key exchange mechanisms, and interpret cryptographic workflows logically	CO2 | L2	MTE Sec A | ETE Sec A
TS3	**Procedural Application & Problem Solving**	Apply mathematical cryptographic techniques such as RSA, Diffie–Hellman, DES operations, modular arithmetic, primality testing, hashing, and security analysis methodologies	CO3 | L3	MTE Sec B | ETE Sec B
TS4	**Analytical Reasoning & Program Tracing**	Analyze cryptographic applications in network security, evaluate vulnerabilities, compare encryption strengths, assess authentication methods, and interpret security outcomes	CO4 | L4	MTE Sec B | ETE Sec B
TS5	**Comparative Evaluation & Algorithmic Justification**	Compare cryptographic protocols, evaluate security at application/transport/network layers, assess efficiency of MAC and hash algorithms, and justify security mechanisms	CO5 | L5	ETE Sec B/C
TS6	**Synthesis & Holistic Design**	Design secure communication frameworks using cryptographic integrity algorithms, authentication protocols, digital signatures, and integrated network security practices	CO6 | L6	ETE Sec C

9. Theory Assessment Structure — MTE and ETE

9.1 Mid Term Examination (MTE) — 10 Marks (CO1–CO4 only)

Section	Marks	Skill Dimensions	COs	Question Type
Sec A	**4**	TS1 — Factual Recall TS2 — Conceptual Explanation	**CO1, CO2**	Short-answer: definitions.
Sec B	**6**	TS3 — Procedural Application TS4 — Analytical Reasoning	**CO3, CO4**	Long and descriptive answers

TOTAL	**10**	TS1–TS4	**CO1–CO4**	Units 1–3 covered; CO5 and CO6 assessed only in ETE

9.2 End Term Examination (ETE) — 100 Marks (Scaled to 50) (CO1–CO6)

Section	Marks	Skill Dimensions	COs	Question Type
Sec A	**25**	TS1 — Factual Recall TS2 — Conceptual Explanation	**CO1, CO2**	Short questions: definitions.
Sec B	**50**	TS3 — Procedural Application TS4 — Analytical Reasoning TS5 — Comparative Evaluation	**CO3, CO4, CO5**	Medium questions: Comparison, Tools and Techniques, Algorithms
Sec C	**25**	TS5 — Comparative Evaluation TS6 — Synthesis & Design	**CO5, CO6**	Long/design questions: Applications, working principles/
TOTAL	**100**	TS1–TS6 (all)	**CO1–CO6**	Scaled to 50 marks. Minimum 20/50 required to pass.

PART III

LABORATORY ASSESSMENT FRAMEWORK

Evaluation Scheme, CA Rubric, Mini Project Rubric, Skill Dimensions for Lab COs (CO7–CO10)

10. Evaluation Scheme — Overview

Component	Weightage	Marks	COs Assessed
Laboratory Assessment	40%	**40**	Lab COs only: CA experiments
Mid Semester Examination (MTE)	10%	**10**	Theory COs only: CO1, CO2, CO3, CO4
End Semester Examination (ETE)	50%	**50**	Theory COs only: CO1, CO2, CO3, CO4, CO5, CO6

TOTAL	**100%**	**100**	Strict separation — no cross-assessment

11. Laboratory Assessment (40 Marks)

LAB COs (CO7–CO10) — Assessed exclusively via Laboratory Assessment only (CA)

11.1 Component Breakdown

Sub-Component	Quantum	Marks	Remarks
Lab Experiments (CA)	Best 10 of 12	**30**	3.0 marks each — assesses CO7, CO8, CO9
Mini Project/Case Study	1 Project	**10**	Design, implementation, demo & reflection — all 4 Lab COs (CO7–CO10)
TOTAL	—	**40**	

11.2 Per-Experiment CA Rubric (3.0 Marks each — Assesses CO7, CO8, CO9)

Criterion	Marks	CA Skill Dimensions Covered	Marking Guide	Lab CO
Problem Definition & Experimental Design	**1.0**	**CA1** — Identification of cryptographic/security problem, objective definition, scope identification **CA2** — Experiment planning, cipher/algorithm selection, tool and environment configuration **CA7** — Cryptographic methodology, workflow planning, attack-defense/security analysis approach	1.0: Well-defined with design | 0.5: Partial | 0: Missing	CO7, CO8
Code Execution & Computational Efficiency	**1.0**	**CA3** — Correct execution of encryption/decryption, hashing, digital signature, key exchange, and authentication tasks **CA4** — Efficient and optimized use of cryptographic tools, scripts, and implementations	1.0: Correct & efficient | 0.5: Correct, not optimized | 0: Fails	CO7

Output Analysis, Outcome & Lab Documentation	**0.75**	**CA5** — Analysis and interpretation of ciphertexts, hashes, authentication outputs, packet/log results **CA6** — Evidence validation, screenshots, observations, report preparation, and conclusion documentation	0.75: Thorough | 0.5: Adequate | 0.25: Partial | 0: Absent	CO8, CO9
Professional Attitude & Ethical Conduct	**0.25**	CA6 — Structured report, screenshots, references, conclusion CA8 — Viva-voce understanding and communication PO7/CO9 — Ethical and responsible cybersecurity practices	0.25: Consistent | 0.10: Occasional | 0: Absent	CO9
Total	**3.0**	All 8 CA skill dimensions covered		

11.3 Best-10-of-N Scoring Scheme

Conducted	Best N Counted	Max Score	Note
> (10 + x)	Best 10	**30 Marks**	x worst dropped
10	All 10	**30 Marks**	No drop
< 10	All	**≤ 30 Marks**	Deficit = zero

11.4 Mini Project Evaluation Rubric (10 Marks — All 4 Lab COs)

Criterion	Marks	Project Skill Dimensions	Marking Guide	Lab CO / PO
SDG Alignment & Problem Scoping	**1.5**	P1 — SDG mapping; societal relevance P2 — Problem scope and stakeholder requirements P4 — Innovative solution proposal with alternatives	1.5: Comprehensive | 1.0: Adequate | 0.5: Partial | 0: Absent	CO8 / PO3, PO6
Project Planning & Financial Awareness	**1.5**	P2 — Timeline, milestones, resource planning P11 — Financial feasibility and cost estimation	1.5: Detailed | 1.0: Adequate | 0.5: Basic | 0: Absent	CO10 / PO10

End-to-End Implementation & System Operation	**2.0**	P5 — Professional toolchain selection P6 — Complete project build and integration P7 — System commissioning and operational testing	2: Fully operational | 1–1.5: Partial | 0–0.5: Non-functional	CO7, CO8 / PO3, PO5
Impact Assessment & Critical Reporting	**2.0**	P8 — Measurable outcome vs stated goals P9 — Statistical/comparative analysis; technical report	2: Rigorous | 1.5: Good | 1: Basic | 0: Absent	CO8, CO10 / PO6
Communication, Presentation & Teamwork	**2.0**	P3 — Communication plan and testing strategy P10 — Professional presentation quality and delivery	2: Excellent | 1.5: Good | 1: Adequate | 0: Poor	CO10 / PO8, PO9
Skill Reflection, Ethics & Professional Attitudes	**1.0**	P12 — Skill growth mapping (pre/post project) P13 — Professional attitudes and ethical conduct	1.0: Reflective & honest | 0.5: Partial | 0: Absent	CO9 / PO7, PO11
Total	**10**	All 13 Project skill dimensions; all 4 Lab COs (CO7–CO10)		

12. CA Skill Dimensions (8 Dimensions — Lab COs only)

ID	Dimension	What is Measured	Lab CO Anchor
CA1	**Problem Definition & Metrics**	Define cryptographic problem, objectives, scope, and success criteria	CO7, CO8
CA2	**Experimental Design & Tool Setup**	Configure cryptographic tools, environments, and security utilities	CO7
CA3	**Code Implementation & Execution**	Execute encryption, hashing, authentication, and security experiments	CO7
CA4	**Computational Efficiency & Optimization**	Evaluate performance and optimize cryptographic implementations	CO7
CA5	**Output Analysis & Result Interpretation**	Analyze ciphertexts, logs, packets, and security outputs	CO8

CA6	**Documented Outcome with Verification**	Record observations, screenshots, outputs, and validate results	CO7, CO8
CA7	**Algorithmic Design & Solution Planning**	Design secure workflows and cryptographic methodologies	CO7, CO8
CA8	**Lab Record Maintenance & Viva-Voce**	Maintain lab records and demonstrate conceptual understanding	CO7, CO9

13. Project Skill Dimensions (13 Dimensions — Lab COs only)

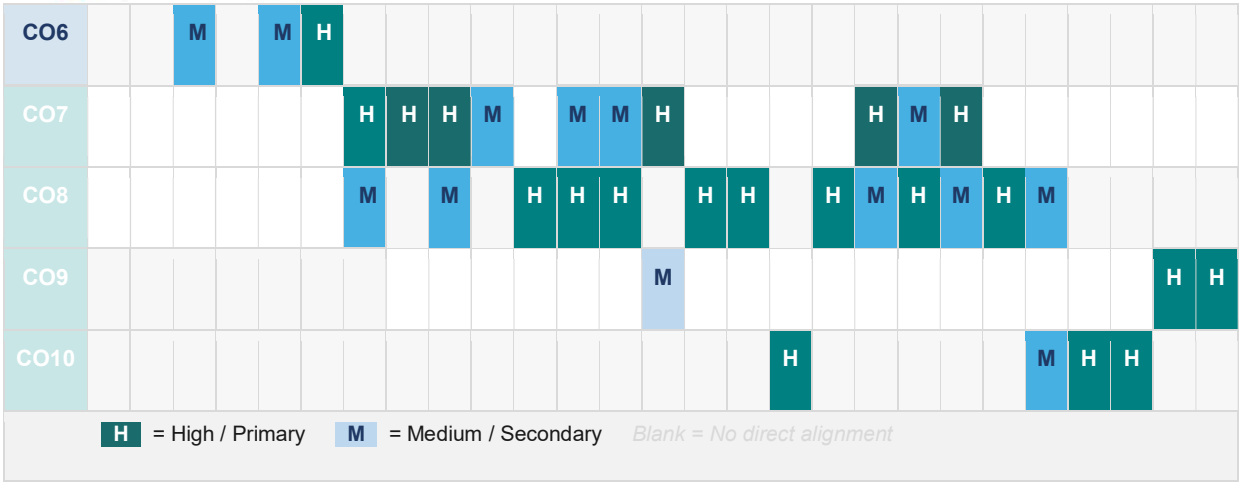
ID	Dimension	What is Measured	Lab CO / PO Anchor
P1	**SDG Alignment & Social Relevance**	Map project to relevant SDGs; articulate societal value and intended impact	CO8 | PO6
P2	**Problem Scoping & Requirements**	Define boundaries; produce formal problem statement with measurable goals	CO8 | PO2
P3	**Communication & Testing Strategy**	Develop communication plan; design testing strategy; coordinate group activities	CO10 | PO9
P4	**Innovative Solution Proposal**	Propose solution with alternatives; justify selection using design criteria	CO8 | PO3
P5	**Professional Toolchain**	Select and justify development tools; configure professional project environment	CO7 | PO5
P6	**End-to-End Implementation**	Build complete integrated solution incorporating at least 3 syllabus topics	CO7, CO8 | PO3
P7	**System Commissioning & Testing**	Deploy and operate system; conduct edge-case and stress tests	CO7, CO8 | PO5
P8	**Measurable Impact & Outcome**	Evaluate actual outcomes against goals; quantify impact using defined metrics	CO8 | PO6
P9	**Critical Analysis & Reporting**	Perform comparative/statistical analysis; produce structured technical report	CO8, CO10 | PO2, PO4
P10	**Professional Presentation & Teamwork**	Deliver professional presentation; evidence team collaboration and role differentiation	CO10 | PO8, PO9

P11	**Financial Feasibility & Planning**	Estimate project cost; justify resource allocation; discuss cost-effectiveness	CO10 | PO10
P12	**Individual Skill Growth Mapping**	Document pre/post skill gaps; map personal contributions to project dimensions	CO9 | PO11
P13	**Professional Attitude, Ethics & Responsibility**	Demonstrate integrity, ethical conduct, and responsible use of tools/data throughout	CO9 | PO7

14. CO × Skill Dimensions Mapping (10 COs × [6 Theory+ 8 CA + 13 Project Dimensions])

- *Theory COs (CO1–CO6) are fully mapped. Lab COs (CO7–CO10) intentionally have no TS mapping — confirming strict assessment separation.*
- *Theory COs (CO1–CO6) have NO CA alignment — confirms they are NOT evaluated in lab. All CA alignments confined to Lab COs (CO7–CO10).*
- *Theory COs (CO1–CO6) have NO project alignment — confirms strict lab-only assessment. All 13 Project dimensions anchored exclusively to Lab COs (CO7–CO10).*

CO	Theory Skill Dimensions						CA Skill Dimensions								Project Skill Dimensions												
	TS1 Factual Recall	TS2 Conceptual Expl.	TS3 Procedural App.	TS4 Analytical Rsng	TS5 Compar. Eval.	TS6 Synthesis & Design	CA1 :Prob.Def.	CA2 Exp.Setup	CA3 Execution	CA4 Efficiency	CA5 Output Anal.	CA6 Doc.Outcome	CA7 Algo.Design	CA8 Lab Rec./Viva	P1 SDG	P2 Scoping	P3 Comm.	P4 Solution	P5 Tools	P6 Impl.	P7 Sys.Op.	P8 Impact	P9 Analysis	P10 Present.	P11 Financial	P12 Skill Map	P13 Attitude
CO1	H	M																									
CO2	M	H	M																								
CO3		M	H	M																							
CO4			M	H	M																						
CO5				M	H	M																					



PART IV

COMBINED MAPPINGS & REFERENCE

CO–PO Matrix, SDG Mapping, Bloom's Taxonomy Reference, Attendance & Pass/Fail

15. CO–PO and CO–PSO Mapping Matrix (All 10 COs)

Strength Scale: 3 = Substantial (High) | 2 = Moderate | 1 = Slight (Low) | – = Not Applicable. Column averages computed over non-zero entries only.

CO/PO	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PSO1	PSO2	PSO3
CO1	3	3	3	-	2	2	-	-	3	-	-	-	3	-
CO2	3	3	3	2	2	-	-	-	-	-	-	-	-	-
CO3	3	3	3	2	2	2	3	-	-	2	-	3	2	3
CO4	3	3	3	-	3	2	3	-	2	-	2	3	-	-
CO5	3	3	2	3	2	-	2	-	3	3	3	2	2	2
CO6	2	3	3	2	3	3	3	3	-	-	3	3	2	3
CO7	–	2	1	–	3	2	–	–	–	–	–	2	3	3

CO8	–	1	3	1	2	3	–	–	–	–	–	2	3	3
CO9	–	–	2	–	–	2	3	–	–	1	3	–	1	2
CO10	2	–	–	–	–	1	–	3	3	3	2	2	2	2
Avg	2.71	2.63	2.56	2.00	2.38	2.13	2.80	3.00	2.75	2.25	2.60	2.43	2.25	2.57

PO7 (Ethics) now receives mapping from CO9 (strength 3). PO11 (Life-Long Learning) is addressed by both Theory COs and CO9. Lab COs (CO7–CO10) extend coverage to POs 3, 5, 6, 7, 8, 9, 10, 11.

16. CO × PO Alignment Map (H/M Indicators — All 10 COs × 11 POs)

CO	PO1 Eng.Know.	PO2 Prob.Analysis	PO3 Design	PO4 Investigation	PO5 Tool Usage	PO6 Engineer & World	PO7 Ethics	PO8 Teamwork	PO9 Comm.	PO10 Proj.Mgmt	PO11 Lifelong
CO1	H	H	H	-	M	M	-	-	H	-	-
CO2	H	H	H	M	M	-	-	-	-	-	-
CO3	H	H	H	M	M	M	H	-	-	M	-
CO4	H	H	H	-	H	M	H	-	M	-	M
CO5	H	H	M	H	M	-	M	-	H	H	H
CO6	M	H	H	M	H	H	H	H	-	-	H
CO7	–	M		–	H	M	–	–	–	–	–
CO8	–		H		M	H	–	–	–	–	–
CO9	–	–	M	–	–	M	H	–	–		H
CO10	M	–	–	–	–		–	H	H	H	M

H = High / Primary **M** = Medium / Secondary *Blank = No direct alignment*

17. Course-to-SDG Mapping Matrix

SDG Goal	Description	Mapping	Justification
SDG 4	Quality Education	3 (High)	Builds strong foundation in computational thinking and structured programming; aligned with lifelong learning (CO1–CO6, CO9).
SDG 8	Decent Work & Economic Growth	3 (High)	Develops industry-relevant programming and professional tool skills (CO7) directly applicable to employment in technology sectors.
SDG 9	Industry, Innovation & Infrastructure	3 (High)	Enables development of efficient software solutions; fosters innovation through real-world application design (CO6, CO8) and team-based projects (CO10).
SDG 12	Responsible Consumption & Production	2 (Moderate)	Promotes efficient, optimized coding; encourages ethical coding and responsible use of computational resources (CO9, CO7).

18. Bloom's Taxonomy — Domain Level Reference

Cognitive Domain (6 Levels)	Affective Domain (5 Levels)	Psychomotor Domain — Simpson (7 Levels)
L1 — Remember: Recall facts, definitions, basic concepts L2 — Understand: Explain ideas, concepts, principles L3 — Apply: Use knowledge to solve new problems L4 — Analyze: Break down information, examine patterns L5 — Evaluate: Judge, justify, assess, make decisions L6 — Create: Design, develop, produce new solutions	A1 — Receiving: Awareness, willingness to attend A2 — Responding: Active participation and reaction A3 — Valuing: Showing commitment, assigning value A4 — Organizing: Integrating values into personal system A5 — Characterizing: Internalized value system	P1 — Perception: Sensory cues guide motor activity P2 — Set: Mental, physical readiness to act P3 — Guided Response: Basic practice through imitation P4 — Mechanism: Habitual correct performance P5 — Complex Overt Response: Skilled performance P6 — Adaptation: Modify skills for special situations P7 — Origination: Create new solution patterns

OBE Compliance Statement: Theory COs (CO1–CO6) are primarily mapped to the Cognitive domain (L1–L6). Lab COs (CO7–CO10) span all three domains — Cognitive (L2–L6), Psychomotor (P3–P7), and Affective (A2–A5) — reflecting the skill-based nature of laboratory and project assessment.

19. Attendance Policy & Pass/Fail Criteria

19.1 Attendance Policy

Component	Minimum	Applicable To	Consequence
Theory Classes	**70%**	All lecture sessions	Debarred from ETE
Practical / Lab	**70%**	All lab sessions	Debarred from ETE
Combined (Theory + Lab)	**75%**	Combined sessions	Debarred from ETE

Both theory and practical attendance must independently meet 70%. The combined must be 75%. Satisfying one does NOT compensate for a shortfall in the other.

19.2 Pass / Fail Criteria

Condition	Threshold	Status	Remarks
ETE Score (scaled)	**≥ 20 / 50**	**MANDATORY**	40% of ETE; equivalent to ≥ 40/100 on the full paper
Overall Total	**≥ 40 / 100**	**Must pass overall**	Lab 40 + MTE 10 + ETE 50 = 100; 40% overall minimum required

PPS INTEGRATED COURSE PLAN — MEASUREMENT ARCHITECTURE

11 AICTE Programme Outcomes → 10 COs (6 Theory + 4 Lab) → 3 Assessment Instruments → 27 Skill Dimensions (6 TS + 8 CA + 13 Project)

Theory Tier CO1–CO6 (MTE + ETE): PO1, PO2, PO3, PO4, PO9 | 6 Theory Skill Dims (TS1–TS6)

Lab Tier CO7–CO10 (Lab only): PO3, PO5, PO6, PO7, PO8, PO9, PO10, PO11 | 8 CA Dims + 13 Project Dims

Marks: Lab 40 (Experiments 30 @ 3.0 each + Project 10) + MTE 10 + ETE 50 = Total 100

COURSE PLAN

Secure Internet of Things (IOT) systems (CSCF4101)

S Sharda School of Computing Science & Engineering (SSCSE) | B.Tech CSE | Semester VII | Batch 2026–2030

Theory-Only Course Plan — All 6 COs (CO1–CO6) | Theory Skill Dimensions TS1–TS6 | CA + MTE + ETE Assessment

PART I

COURSE SYLLABUS

Course Identification, Details, Outcomes, BTL Mapping & Lecture Plan

1. Course Identification

School:	SSCSE- Sharda School of Computing Science & Engineering	**Batch:**	2026-2030
Program:	B.Tech	**Current Academic Year:**	2026–27
Branch:	CSE	**Semester:**	VII
Course Code:	**CSCF4101**	**Course Type:**	Core

2. Course Details

 THEORY-ONLY COURSE — All 6 COs (CO1–CO6) are assessed exclusively via Continuous Assessment (CA), MTE, and ETE. No laboratory component.

S.No	Attribute	Details
1	**Course Code**	**CSCF4100**
2	**Course Title**	**Introduction to IoT and It's Security**
3	**Credits**	3

4	**Contact Hours (L-T-P-SL)**	3-0-0-3 (Theory: 45 hrs Classroom + 45 hrs Self Learning = 90 hrs total)
5	**Course Status**	**Core — Theory Only (No Laboratory Component)**
6	**Course Objectives**	1. Understand the fundamentals of ethical hacking, cybersecurity, and system security. 2. Explore hacking methodologies, tools, and attack techniques. Analyze vulnerabilities in networks, systems, and IoT environments. 3. Apply security mechanisms and ethical practices to protect systems.
7	**Course Outcomes (COs)**	**After successful completion of this course, students will be able to:** After the completion of this course students will be able to: CO1 (Remember – L1): Define ethical hacking concepts, cybersecurity principles, and system components. CO2 (Understand – L2): Explain hacking phases, attack vectors, and security mechanisms. CO3 (Apply – L3): Use ethical hacking tools for scanning, enumeration, and vulnerability analysis. CO4 (Analyze – L4): Analyze systems and IoT environments for security threats and weaknesses. CO5 (Evaluate – L5): Evaluate security frameworks and mitigation strategies. CO6 (Create – L6): Design secure systems and penetration testing strategies.
8	**Course Description**	This course provides a comprehensive understanding of ethical hacking and cybersecurity, focusing on identifying vulnerabilities in systems including IoT environments. It covers hacking methodologies, tools, and defensive mechanisms, enabling students to design secure systems and apply ethical practices in cybersecurity.
9	**Teaching & Learning Scheme**	Classroom Instructions (CI): 45 hrs | Self Learning (SL): 45 hrs | Total: 90 hrs
10	**Mode of Examination**	**Theory Only. CA: 25% | MTE: 15% | ETE: 60% | Total: 100 marks**
11	**Textbook**	1. Sunil Cheruvu, Anil Kumar, Ned Smith, David M. Wheeler “Demystifying Internet of Things Security”
12	**References**	Reference: 1. Maciej Kranz, Building the Internet of Things - Comprehensive, Business Focused, Well-articulated coverage of IoT, WILEY 2. Brian Russell and Drew Van Duren, Practical Internet of Things Security, PACKT

3. Outline Syllabus with CO Mapping

All CO mappings in this section refer to Theory COs (CO1–CO6). This is a theory-only course; all assessment is via CA, MTE, and ETE.

	Topic	CO Mapping
	Unit 1: Introduction to Ethical Hacking & IoT Security	
A	Overview of Ethical Hacking, Cybersecurity Concepts, CIA Triad	CO1, CO2
B	IoT Fundamentals, Devices, Gateways, and Network Architecture	CO1, CO2, CO4
C	Threats, Vulnerabilities, Risk Management in IoT	CO3, CO4, CO5, CO6
	Unit 2: Ethical Hacking Methodology & Architecture	
A	Hacking Phases, Reconnaissance, Scanning, Enumeration	CO2, CO3
B	IoT Reference Architecture and Security Models	CO2, CO4, CO5
C	Design Constraints, Data Handling, and Remote Access Risks	CO4, CO5, CO6
	Unit 3: Secure Systems & Cyber Attacks	
A	Case Studies (BadUSB, Stuxnet, Air-gap attacks)	CO2, CO4, CO5
B	Secure Cyber-Physical Systems Design	CO4, CO5, CO6
C	Network Security, Edge Computing, Trusted Networks	CO3, CO4, CO5, CO6
	Unit 4: System & Hardware Security	
A	Security Terminology and Concepts	CO1, CO2
B	Device Identity, Boot Integrity, Data Protection	CO2, CO4, CO5
C	Runtime Protection and Threat Mitigation	CO3, CO4, CO5, CO6

	Unit 5: Software Security & Defensive Techniques	
A	OS Security, Virtualization, and Isolation	CO2, CO4, CO5
B	Network Stack Security and Device Management	CO3, CO4, CO5
C	Firmware Security, Root of Trust, Secure Updates	CO4, CO5, CO6

4. Topic-wise Bloom's Taxonomy Level Mapping

S.No	Topic	L1 Remember	L2 Understand	L3 Apply	L4 Analyze	L5 Evaluate	L6 Create
1	1.A	✓	✓				
2	1.B		✓	✓			
3	1.C			✓	✓	✓	✓
4	2.A		✓	✓			
5	2.B		✓		✓	✓	
6	2.C				✓	✓	✓
7	3.A		✓		✓	✓	
8	3.B				✓	✓	✓
9	3.C			✓	✓	✓	✓
10	4.A	✓	✓				
11	4.B		✓		✓	✓	
12	4.C			✓	✓	✓	✓
13	5.A		✓		✓	✓	
14	5.B			✓	✓	✓	

15	5.C				✓	✓	✓

5. CO vs Bloom's Taxonomy — All Three Domains

Only strong/dominant alignments are mapped. This is a theory-only course; Psychomotor mapping is limited to Guided Response (P3) for algorithm implementation in CO3. Affective domain appears at A3 (Valuing) for efficiency analysis in CO4 and CO5.

CO	Cognitive Domain (L1–L6)						Affective (A1–A5)					Psychomotor (P1–P7)						
CO	L1	L2	L3	L4	L5	L6	A1	A2	A3	A4	A5	P1	P2	P3	P4	P5	P6	P7
CO1	✓																	
CO2		✓																
CO3			✓											✓	✓			
CO4				✓					✓						✓	✓		
CO5					✓				✓	✓						✓		
CO6						✓				✓	✓					✓	✓	✓

Legend: ✓ = Strong / Dominant mapping. Theory-only course: Cognitive domain is primary. Psychomotor (P3) limited to CO3 (algorithm implementation). Affective (A3) for CO4 and CO5 (valuing efficiency).

6. Lecture Plan Outline (Theory — 45 Lectures / 45 Hours)

Total classroom contact: 30 hours across 5 units. Self-Learning activities (30 hrs) are structured separately in Section 11.

Lecture No.	Date	Topics to be Covered / Title	Unit	Total Lectures
1	DD/MM/YY	Introduction to Ethical Hacking	UNIT-1	9
2	DD/MM/YY	Introduction to IoT Security		
3	DD/MM/YY	Overview of Cybersecurity Concepts		
4	DD/MM/YY	CIA Triad and Security Principles		
5	DD/MM/YY	IoT Architecture Overview		

6	DD/MM/YY	IoT Devices and Sensors		
7	DD/MM/YY	IoT Gateways and Communication Models		
8	DD/MM/YY	Threats, Vulnerabilities and Risk Management		
9	DD/MM/YY	Unit Review and Discussion		
10	DD/MM/YY	Introduction to Hacking Phases and Methodology	UNIT-2	9
11	DD/MM/YY	Footprinting and Reconnaissance Techniques		
12	DD/MM/YY	Active and Passive Reconnaissance		
13	DD/MM/YY	Scanning Techniques and Tools		
14	DD/MM/YY	Enumeration Methods		
15	DD/MM/YY	IoT Reference Architecture		
16	DD/MM/YY	IoT Design Constraints		
17	DD/MM/YY	Data Handling in IoT Systems		
18	DD/MM/YY	Secure System Design Concepts		
19	DD/MM/YY	Case Study: Stuxnet Attack	UNIT-3	9
20	DD/MM/YY	Case Study: BadUSB Attack		
21	DD/MM/YY	Air-gap Attacks and Analysis		
22	DD/MM/YY	Secure Cyber-Physical Systems		
23	DD/MM/YY	Networking Basics: TCP/IP Model		
24	DD/MM/YY	Ports, Protocols and Services		
25	DD/MM/YY	Fundamentals of Network Security		
26	DD/MM/YY	Edge Computing Concepts		
27	DD/MM/YY	Trusted Networks and Review Discussion		
28	DD/MM/YY	Network Attack Scenarios	UNIT-4	9
29	DD/MM/YY	Analysis of Common Network Attacks		
30	DD/MM/YY	Defense Mechanisms in Cybersecurity		
31	DD/MM/YY	Security Terminology and Concepts		
32	DD/MM/YY	Device Identity Management		
33	DD/MM/YY	Authentication Techniques for IoT Devices		
34	DD/MM/YY	Secure Boot Mechanisms		
35	DD/MM/YY	Integrity Verification Techniques		
36	DD/MM/YY	Data Protection and Runtime Protection		
37	DD/MM/YY	Threat Mitigation Strategies	UNIT-5	9
38	DD/MM/YY	Operating System Security Concepts		
39	DD/MM/YY	Virtualization and Hypervisor Security		
40	DD/MM/YY	Isolation Techniques and Container Security		

41	DD/MM/YY	Network Stack Security		
42	DD/MM/YY	Device Management and Monitoring		
43	DD/MM/YY	Firmware Security Concepts		
44	DD/MM/YY	Root of Trust and Secure Update Mechanisms		
45	DD/MM/YY	Final Review, Case Studies and Discussion		

PART II

THEORY ASSESSMENT FRAMEWORK

Theory Skill Dimensions, CO × TS Mapping, CA / MTE / ETE Structure

7. Theory Skill Dimensions (TS1–TS6)

THEORY-ONLY COURSE — All 6 COs (CO1–CO6) are assessed exclusively via Continuous Assessment (CA), MTE, and ETE. No laboratory component.

Six Theory Skill Dimensions — one per Bloom's progression (L1–L4) — correspond directly to the six COs. They define precisely what competency is being measured in each section of the CA, MTE, and ETE, providing a clear NBA-auditable assessment rationale.

ID	Dimension	What is Measured	CO / BTL	Assessment
TS1	**Cybersecurity Fundamentals & Ethical Hacking Awareness**	Recall IoT terminology, architecture, sensors, actuators, protocols, and security concepts; identify correct IoT components and technologies	CO1 | L1–L2	CA | MTE Sec A | ETE Sec A
TS2	**Ethical Hacking Methodology & IoT Security Interpretation**	Explain IoT architecture, communication models, networking protocols, and security mechanisms; interpret IoT workflows and data exchange processes	CO2 | L2–L3	CA | MTE Sec A | ETE Sec A
TS3	**Secure System Implementation & Attack Analysis**	Apply IoT platforms, sensors, controllers, and security practices to develop solutions for real-world IoT applications	CO3 | L3	CA | MTE Sec B | ETE Sec B
TS4	**Hardware Security & Threat Mitigation Analysis**	Analyze IoT system behaviour, trace communication flow, identify vulnerabilities, detect security threats, and evaluate system performance	CO4 | L4–L5	MTE Sec B | ETE Sec B

TS5	**Software, Firmware & Network Security Evaluation**	Compare IoT communication protocols, cloud/fog architectures, and security approaches; justify suitable technologies based on efficiency, scalability, and security requirements	CO5 | L4–L5	ETE Sec B/C
TS6	**Secure IoT System Design & Defensive Architecture Development**	Design secure, scalable, and modular IoT systems integrating sensors, networks, cloud services, and security mechanisms for complex applications	CO6 | L2–L4	ETE Sec C

8. CO × Theory Skill Dimension Mapping (6 COs × 6 Dimensions)

Each CO maps primarily to one TS dimension (H) with adjacent dimensions receiving secondary mapping (M), reflecting the progressive Bloom's structure of this course.

CO	TS1 Ethical Hacking Concepts & Cybersecurity Principles	TS2 Hacking Phases & Security Mechanisms	TS3 Ethical Hacking Tools & Vulnerability Analysis	TS4 Threat & IoT Security Analysis	TS5 Security Frameworks & Mitigation Evaluation	TS6 Secure System & Penetration Testing Design
CO1	H	H	M		-	-
CO2	H	H	M	M	M	-
CO3	H	H	M	H	H	M
CO4	M	M			M	M
CO5	M	H	M	M	H	H
CO6	H	H	H	M	H	H

H = High / Primary alignment M = Medium / Secondary alignment Blank = No direct alignment

9. Continuous Assessment (CA) — 25 Marks

CA is formative and covers COs progressively as the syllabus is taught. It includes numerical-based assignments, a technical video learning report, and a real-world case study — mirroring TS1 through TS6.

9.1 CA Component Breakdown (Sample)

Component	Quantum	Marks	COs Assessed	Skill Dimensions
Assignments 1–5 (Ethical Hacking / IoT Security Problems & Analysis)	5 Assignments	15	CO1, CO2, CO3, CO4	TS1, TS2, TS3, TS4
Technical Tool Demonstration / Video Learning Report	1 Report + Presentation	5	CO2, CO3, CO5	TS2, TS3, TS5
Real-World Cybersecurity & IoT Attack Case Study (Report)	1 Report	5	CO4, CO5, CO6	TS4, TS5, TS6
TOTAL	—	**25**	**CO1–CO6**	**TS1–TS6**

9.2 Assignment-wise CO & TS Mapping

Item	Topic / Focus	COs	TS Dims	SL Hours	Evaluation Criteria
Assignment 1	Unit 1 concepts: Ethical Hacking overview, Cybersecurity principles, CIA Triad, IoT fundamentals	CO1, CO2	TS1, TS2	5h SL	Conceptual understanding, report submission, terminology accuracy
Assignment 2	Hacking phases, reconnaissance, scanning, enumeration, IoT architecture and security models	CO2, CO3	TS2, TS3	5h SL	Tool-based analysis, workflow explanation, vulnerability identification
Assignment 3	Threats, vulnerabilities, network security, trusted networks, runtime protection techniques	CO3, CO4	TS3, TS4	5h SL	Threat analysis, practical application, security assessment
Assignment 4	Secure cyber-physical system design, OS security,	CO4, CO5	TS4, TS5	5h SL	Comparative analysis, mitigation strategy

	virtualization, isolation, risk mitigation				evaluation, technical reasoning
Assignment 5	Firmware security, root of trust, secure updates, penetration testing strategies	CO5, CO6	TS5, TS6	5h SL	Secure design proposal, penetration testing methodology, defense planning
Video Learning Report	Technical video on Ethical Hacking / IoT Security tools and attack-defense mechanisms (min 3 hrs); structured report + presentation	CO2, CO3, CO5	TS2, TS3, TS5	9h SL	Learning outcomes, technical understanding, self-reflection, 10-minute presentation
Case Study Report	Real-world cybersecurity and IoT attack case study (e.g., Stuxnet, BadUSB, smart device attacks, ransomware on IoT systems)	CO4, CO5, CO6	TS4, TS5, TS6	6h SL	Technical depth, attack analysis, comparative evaluation, mitigation framework recommendation

10. Mid Term Examination (MTE) — 15 Marks (Units 1–3)

MTE covers Units 1–3 (CO1, CO2, CO3, CO4). CO5 and CO6 are assessed in ETE only. MTE maps to TS1–TS4.

Section	Marks	Theory Skill Dimensions	COs Assessed	Question Type & Guidance
Section A	10	TS1 — Ethical Hacking Concepts & Cybersecurity Principles TS2 — Hacking Phases & Security Mechanisms	CO1, CO2	Short-answer questions: define ethical hacking concepts, explain CIA Triad, describe IoT architecture, explain hacking phases, reconnaissance, scanning, enumeration, and security terminology
Section B	15	TS3 — Ethical Hacking Tools & Vulnerability Analysis TS4 — Threat & IoT Security Analysis	CO2, CO3, CO4	Analytical and application-based questions: vulnerability analysis using ethical hacking tools, network and IoT threat assessment, attack vector analysis, risk evaluation, secure architecture interpretation, and case-study-based security analysis
TOTAL	**25**	**TS1–TS4**	**CO1–CO4**	Units 1–3 only. CO5 and CO6 assessed in ETE only.

11. End Term Examination (ETE) — 60 Marks (All Units, All COs)

ETE is comprehensive — all 5 units and all 6 COs. Full progression from TS1 (recall) through TS6 (evaluation). Minimum 20/50 required to pass.

Section	Marks	Theory Skill Dimensions	COs Assessed	Question Type & Guidance
Section A	15	TS1 — Ethical Hacking Concepts & Cybersecurity Principles TS2 — Hacking Phases & Security Mechanisms	CO1, CO2	Short questions (all units): definitions of ethical hacking and cybersecurity concepts, CIA Triad, IoT architecture, security terminology, hacking phases, reconnaissance, scanning, enumeration, and security mechanisms
Section B	25	TS3 — Ethical Hacking Tools & Vulnerability Analysis TS4 — Threat & IoT Security Analysis TS5 — Security Frameworks & Mitigation Evaluation	CO3, CO4, CO5	Medium questions: vulnerability scanning and enumeration analysis, IoT threat assessment, network security analysis, attack vector identification, runtime protection techniques, mitigation strategies, and security framework comparisons
Section C	10	TS5 — Security Frameworks & Mitigation Evaluation TS6 — Secure System & Penetration Testing Design	CO5, CO6	Long/evaluation questions: secure cyber-physical system design, firmware and root of trust analysis, penetration testing strategy design, trusted network evaluation, secure update mechanisms, and real-world cybersecurity case study analysis
TOTAL	**50**	**TS1–TS6 (all)**	**CO1–CO6**	Scaled from 100-mark paper if needed. Minimum 20/50 to pass.

11.1 CO-wise Assessment Instrument Summary

CO	CO Statement (Short)	CA (25)	MTE (25)	ETE (50)	TS	PO Primary
CO1	Understand ethical hacking concepts, cybersecurity principles, and IoT fundamentals	✓	✓	✓	TS1	PO1, PO2, PO3, PO4
CO2	Explain hacking phases, attack vectors, IoT architectures, and security mechanisms	✓	✓	✓	TS2	PO1, PO2, PO3, PO4
CO3	Apply ethical hacking tools for scanning, enumeration, and vulnerability analysis	✓	✓	✓	TS3	PO1, PO2, PO3, PO5
CO4	Analyze systems and IoT environments for threats, vulnerabilities, and security risks	✓	✓	✓	TS4	PO2, PO3, PO4, PO10
CO5	Evaluate security frameworks, mitigation strategies, and protection mechanisms	✓	—	✓	TS5	PO1, PO2, PO8, PO10, PO11
CO6	Design secure systems and penetration testing strategies for cyber-physical environments	✓	—	✓	TS6	PO3, PO4, PO10, PO11, PO12

CO5 and CO6 are NOT assessed in MTE (only Units 1–3 are covered at mid-semester). They are assessed in CA (self-learning activities) and ETE.

PART III

COMBINED MAPPINGS & REFERENCE

CO–PO Matrix, CO–PO Alignment, Self-Learning Activities, Bloom's Reference, Attendance & Pass/Fail

12. CO–PO and CO–PSO Mapping Matrix (Original Framework)

Strength Scale: 3 = Substantial (High) | 2 = Moderate | 1 = Slight (Low) | – = Not Applicable. Averages computed over non-zero entries only. PO framework as per the original course design.

CO	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PO12	PSO1	PSO2	PSO3
CO1	3	3	2	1	-	-	-	-	-	-	2	2	3	2	3
CO2	3	3	2	2	2	-	-	-	-	-	3	3	3	3	3
CO3	3	3	2	3	3	2	-	2	2	2	2	3	2	3	3
CO4	2	2	1	1	2	2	2	2	-	1	2	2	2	2	2
CO5	2	3	2	2	3	3	2	-	2	2	1	2	2	2	2
CO6	3	3	3	2	3	3	3	2	2	3	3	3	3	3	3
Avg	**2.67**	**2.83**	**2.00**	**1.83**	**2.17**	**1.67**	**1.50**	**1.00**	**1.00**	**1.17**	**2.33**	**2.50**	**2.50**	**2.50**	**2.67**

13. CO × PO Alignment Map (H/M Indicators — All 6 COs)

CO	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PO12	PSO1	PSO2	PSO3
CO1	H	H	M		-	-	-	-	-	-	M	M	H	M	H
CO2	H	H	M	M	M	-	-	-	-	-	H	H	H	H	H
CO3	H	H	M	H	H	M	-	M	M	M	M	H	M	H	H

CO4	M	M			M	M	M	M	-		M	M	M	M	M
CO5	M	H	M	M	H	H	M	-	M	M		M	M	M	M
CO6	H	H	H	M	H	H	H	M	M	H	H	H	H	H	H

H = High / Primary alignment M = Medium / Secondary alignment Blank = No direct alignment

14. Self-Learning Activities (SL: 30 Hours)

S.No	Activity	Hours	COs / TS	Evaluation Criteria
1	Assignment Writing (5 assignments based on Ethical Hacking, IoT Security, Vulnerability Analysis, Security Frameworks, and Penetration Testing)	5 assignments × 3 hrs each Total = 15 hrs	CO1–CO4 TS1–TS4	Evaluated based on assignment submission, threat analysis accuracy, vulnerability identification, tool usage, mitigation techniques, and analytical reasoning
2	Technical Video-Based Learning related to Ethical Hacking and IoT Security (e.g., reconnaissance, scanning, malware attacks, IoT vulnerabilities, secure architectures)	Video viewing: 3 hrs Report preparation: 3 hrs Presentation: 3 hrs Total = 9 hrs	CO2, CO3, CO5 TS2, TS3, TS5	Report + Presentation based on learning outcomes; must include security concepts, attack-defense mechanisms, ethical hacking tools, and personal technical reflections
3	Real-World Cybersecurity & IoT Case Studies (e.g., Stuxnet, BadUSB, ransomware attacks, smart device vulnerabilities, secure cyber-physical systems)	Data collection/study: 4 hrs Report preparation: 2 hrs Total = 6 hrs	CO4, CO5, CO6 TS4, TS5, TS6	Evaluated based on technical depth, attack analysis, data collection, fact finding, mitigation strategies, secure design recommendations, and analytical conclusions
	TOTAL Self-Learning Hours	**30 hours**	**CO1–CO6**	All activities are compulsory. Submission deadlines communicated at the start of the semester.

15. Bloom's Taxonomy — Domain Level Reference

Cognitive Domain (6 Levels)	Affective Domain (5 Levels)	Psychomotor Domain — Simpson (7 Levels)

L1 — Remember: Recall facts, definitions, basic concepts L2 — Understand: Explain ideas, concepts, and principles L3 — Apply: Use knowledge to solve problems in new situations L4 — Analyze: Break down information, examine relationships L5 — Evaluate: Judge, justify, assess, and make decisions L6 — Create: Design, develop, and produce new artefacts	A1 — Receiving: Awareness and willingness to attend A2 — Responding: Active participation and reaction A3 — Valuing: Commitment and assigning value to content A4 — Organizing: Integrating values into a personal system A5 — Characterizing: Internalized value system	P1 — Perception: Sensory cues guide motor activity P2 — Set: Mental, physical readiness to act P3 — Guided Response: Practice through imitation/trial P4 — Mechanism: Habitual correct performance P5 — Complex Overt Response: Skilled performance P6 — Adaptation: Modify skills for special situations P7 — Origination: Create new solution patterns

OBE Compliance Statement: This is a theory-only course. All 6 COs are mapped primarily to the Cognitive domain (L1–L5). Psychomotor domain (P3) appears only for CO3 (algorithm implementation as mental tracing). Affective domain (A3) appears for CO4 and CO5, reflecting valuing of algorithmic efficiency.

16. Attendance Policy & Pass / Fail Criteria

16.1 Attendance Policy

Component	Minimum	Applicable To	Consequence
Theory Classes	**75%**	All lecture sessions	Debarred from ETE if below threshold
Self-Learning / Assignment Submission	**All activities**	SL activities (30 hrs)	Incomplete SL affects CA score directly

Theory attendance must meet 75% minimum. Missing SL activities (assignments, video report, case study) directly impacts CA marks and is not compensable by exam performance.

16.2 Pass / Fail Criteria

Condition	Threshold	Status	Remarks
ETE Score	**≥ 24 / 60**	**MANDATORY**	40% of ETE paper required; failing ETE means failing the course regardless of CA + MTE
Overall Total (CA + MTE + ETE)	**≥ 40 / 100**	**Must pass overall**	CA 25 + MTE 25 + ETE 50 = 100; 40% overall minimum required

CSCF4101— MEASUREMENT ARCHITECTURE SUMMARY

Theory-Only Course | 6 COs (CO1–CO6) | 3 Assessment Instruments | 6 Theory Skill Dimensions (TS1–TS6)

CO1–CO2: Conceptual / Understand → TS1, TS2 → CA + MTE Sec A + ETE Sec A

CO3–CO4: Apply / Analyze → TS3, TS4 → CA + MTE Sec B + ETE Sec B

CO5–CO6: Analyze / Evaluate → TS5, TS6 → CA + ETE Sec B/C

CA 25 marks + MTE 25 marks + ETE 50 marks = Total 100 marks

COURSE PLAN

Cloud Security (CSCF4200)

SSCSE-Sharda School of Computing Science & Engineering) | B.Tech CSE | Semester VII | Batch 2026–2030

Theory-Only Course Plan — All 6 COs (CO1–CO6) | Theory Skill Dimensions TS1–TS6 | CA + MTE + ETE Assessment

PART I

COURSE SYLLABUS

Course Identification, Details, Outcomes, BTL Mapping & Lecture Plan

1. Course Identification

School:	SSCSE-Sharda School of Computing Science & Engineering	**Batch:**	2026–2030
Program:	B.Tech	**Current Academic Year:**	2026-27
Branch:	CSE	**Semester:**	VII
Course Code:	CSCF4200	**Course Type:**	Core — Theory Only

2. Course Details

THEORY-ONLY COURSE — All 6 COs (CO1–CO6) are assessed exclusively via Continuous Assessment (CA), MTE, and ETE. No laboratory component.

S.No	Attribute	Details
1	**Course Code**	**CSCF4200**
2	**Course Title**	**Cloud Security**
3	**Credits**	3

4	**Contact Hours (L-T-P-SL)**	3-0-0-3 (Theory: 45 hrs Classroom + 45 hrs Self Learning = 90 hrs total)
5	**Course Status**	**Core — Theory Only (No Laboratory Component)**
6	**Course Objectives**	1.Provide students with an overview of the fundamental concepts of Cloud Computing. 2.Gain insight into the challenges and limitations Models of cloud computing. 3.To learn the various technologies of the cloud computing paradigm and learn about recent advances in Cloud Computing and enabling technologies. 4.Prepare students for research in the area of cloud Computing risks and cloud security challenges.
7	**Course Outcomes (COs)**	**After successful completion of this course, students will be able to:** CO1 (Understand – L1/L2): Identify and understand the fundamental concepts, characteristics, and models of cloud computing. CO2 (Understand/Explore – L2/L3): Explain the evolution of cloud computing and examine the role of enabling technologies, including physical and logical infrastructure. CO3 (Apply – L3): Understand and implement cloud access control methods and security mechanisms in cloud environments. CO4 (Analyze – L4/L5): Analyze cloud monitoring, auditing, and management techniques to evaluate cloud system performance and security. CO5 (Analyze – L4/L5): Compare different types of computer viruses and evaluate their objectives, impacts, and prevention techniques. CO6 (Analyze/Evaluate – L4/L5): Analyze various intrusion detection systems and evaluate firewall design principles for ensuring network and cloud security.
8	**Course Description**	This course introduces advanced aspects of Cloud Computing, encompassing the principles, to analyze the cloud, identify the problems, and choose the relevant models and algorithms to apply.
9	**Teaching & Learning Scheme**	Classroom Instructions (CI): 45 hrs | Self Learning (SL): 45 hrs | Total: 90 hrs
10	**Mode of Examination**	**Theory Only. CA: 25% | MTE: 15% | ETE: 60% | Total: 100 marks**
11	**Textbook**	Thomas Erl & Eric Barcelo Monroy — Cloud Computing: Concepts, Technology, Security, and Architecture (2nd Ed.), Pearson, 2024.
12	**References**	1.Jamuna S. Murthy, Siddesh G. M., & Srinivasa K. G. — Cloud Security: Concepts, Applications and Practices (1st Ed.), Chapman & Hall/CRC Press, 2024. 2.Preeti Mishra, Emmanuel S. Pilli, & R. C. Joshi — Cloud Security: Attacks, Techniques, Tools, and Challenges, CRC Press, 2024. 3. Mark Buckwell, Stefaan Van Daele, & Carsten Horst — Security Architecture for Hybrid Cloud: A Practical Method for Designing Security Using Zero Trust Principles, O'Reilly Media, 2024.

3. Outline Syllabus with CO Mapping

All CO mappings in this section refer to Theory COs (CO1–CO6). This is a theory-only course; all assessment is via CA, MTE, and ETE.

	Topic	CO Mapping
	Unit 1: Introduction Cloud Computing	
A	Introduction to distributed systems, Defining Cloud Computing	CO1, CO2
B	Understanding of Cloud Architecture: Composability, Infrastructure, Platform	CO1, CO2
C	Virtual Appliances, Communication Protocols, Applications, Understanding Services: SaaS, PaaS, IaaS	CO1,CO2
	Unit 2: Secure Isolation of Physical & Logical Infrastructure	
A	Isolation: Compute, Network and Storage	CO1, CO2, CO4
B	Common attack vectors and threats, Secure Isolation Strategies, Multitenancy, Virtualization strategies	CO1, CO2, CO4
C	Inter-tenant network segmentation strategies, Storage isolation strategies	CO1, CO2, CO4
	Unit 3: Data Protection for Cloud Infrastructure and Services	
A	Understand the Cloud based Information Life Cycle, Data protection for Confidentiality and Integrity	CO1, CO2,CO3
B	Common attack vectors and threats, Encryption, Data Redaction, Tokenization, Obfuscation, PKI and Key Management, Assuring data deletion	CO1, CO2, CO3

C	Data retention, deletion and archiving procedures for tenant data, Data Protection Strategies	CO1, CO2, CO3
	Unit 4: Enforcing Access Control for Cloud Infrastructure based Services	
A	Understand the access control requirements for Cloud infrastructure.	CO1, CO3, CO4
B	Authentication and Authorization, Roles-based Access Control, Multi-factor authentication.	CO1, CO2, CO4
C	Securing remote access, Verified and measured boot, Firewalls, IDS, IPS and honeypots	CO1, CO2, CO4
	Unit 5: Monitoring, Auditing and Management	
A	Proactive activity monitoring, Incident Response, Monitoring for unauthorized access, malicious traffic, abuse of system privileges, intrusion detection, events and alerts	CO5, CO6
B	Auditing – Record generation, Reporting and Management, Tamper-proofing audit logs	CO5, CO6
C	Quality of Services, Secure Management, User management, Identity management, Security Information and Event Management	CO5, CO6

4. Topic-wise Bloom's Taxonomy Level Mapping

S.No	Topic	L1 Remember	L2 Understand	L3 Apply	L4 Analyze	L5 Evaluate	L6 Create
1	1.A	✓	✓				
2	1.B	✓	✓				
3	1.C		✓				
4	2.A		✓	✓			
5	2.B		✓	✓			✓

6	2.C			✓	✓		✓
7	3.A	✓	✓				✓
8	3.B			✓	✓		✓
9	3.C			✓	✓	✓	✓
10	4.A		✓				
11	4.B			✓	✓		
12	4.C			✓	✓	✓	
13	5.A		✓	✓			
14	5.B			✓	✓		
15	5.C			✓	✓	✓	

5. CO vs Bloom's Taxonomy — All Three Domains

Only strong/dominant alignments are mapped. This is a theory-only course; Psychomotor mapping is limited to Guided Response (P3) for algorithm implementation in CO3. Affective domain appears at A3 (Valuing) for efficiency analysis in CO4 and CO5.

CO	Cognitive Domain (L1–L6)						Affective (A1–A5)					Psychomotor (P1–P7)						
CO	L1	L2	L3	L4	L5	L6	A1	A2	A3	A4	A5	P1	P2	P3	P4	P5	P6	P7
CO1	✓	✓																
CO2		✓	✓															
CO3			✓	✓										✓				

CO4				✓	✓				✓								
CO5				✓	✓				✓								
CO6		✓	✓	✓	✓								✓				

Legend: ✓= Strong / Dominant mapping. Theory-oriented Cloud Security course: Cognitive domain is primary. Psychomotor domain (P3) is limited to implementation and practical analysis of cloud security mechanisms, intrusion detection, and firewall configuration. Affective domain (A3) reflects valuing security, monitoring, and efficient protection mechanisms in cloud environments.

6. Lecture Plan Outline (Theory — 45 Lectures / 45 Hours)

Total classroom contact: 45 hours across 5 units. Self-Learning activities (45 hrs) are structured separately in Section 11.

Date	Topics to be Covered/Title	UNIT	Total Lectures
DD/MM/YY	Introduction to distributed systems and basic concepts	UNIT-1	10
DD/MM/YY	Defining Cloud Computing and characteristics of cloud computing		
DD/MM/YY	Understanding Cloud Architecture and composability		
DD/MM/YY	Cloud Infrastructure and Platform concepts		
DD/MM/YY	Virtual Appliances and virtualization concepts		
DD/MM/YY	Communication protocols used in cloud environments		
DD/MM/YY	Cloud applications and service delivery models		
DD/MM/YY	Understanding SaaS, PaaS and IaaS		

DD/MM/YY	Cloud deployment models and practical examples		
DD/MM/YY	Revision and discussion on cloud architecture concepts		
DD/MM/YY	Introduction to secure isolation in cloud environments	UNIT-2	8
DD/MM/YY	Isolation techniques for Compute resources		
DD/MM/YY	Network and Storage isolation mechanisms		
DD/MM/YY	Common attack vectors and threats in cloud systems		
DD/MM/YY	Secure Isolation Strategies and multitenancy concepts		
DD/MM/YY	Virtualization strategies and hypervisor security		
DD/MM/YY	Inter-tenant network segmentation strategies		
DD/MM/YY	Storage isolation strategies and practical security measures		
DD/MM/YY	Understanding the Cloud-based Information Life Cycle	UNIT-3	10
DD/MM/YY	Data protection requirements for Confidentiality and Integrity		
DD/MM/YY	Common attack vectors and threats to cloud data		
DD/MM/YY	Encryption techniques and secure data storage		
DD/MM/YY	Data Redaction and Tokenization techniques		
DD/MM/YY	Obfuscation methods and data masking concepts		
DD/MM/YY	PKI and Key Management systems		
DD/MM/YY	Assuring secure data deletion in cloud systems		
DD/MM/YY	Data retention, deletion and archiving procedures for tenant data		

DD/MM/YY	Cloud Data Protection Strategies and case discussions		
DD/MM/YY	Introduction to access control requirements for cloud infrastructure	UNIT-4	10
DD/MM/YY	Authentication concepts and techniques in cloud computing		
DD/MM/YY	Authorization mechanisms and access management		
DD/MM/YY	Role-Based Access Control (RBAC) in cloud environments		
DD/MM/YY	Multi-factor authentication and identity verification		
DD/MM/YY	Securing remote access in cloud systems		
DD/MM/YY	Verified and measured boot mechanisms		
DD/MM/YY	Firewalls and cloud network protection		
DD/MM/YY	Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS)		
DD/MM/YY	Honeypots and advanced cloud security practices		
DD/MM/YY	Introduction to Quality of Services and Secure Management	UNIT-5	8
DD/MM/YY	User management and Identity management concepts		
DD/MM/YY	Security Information and Event Management (SIEM)		
DD/MM/YY	Proactive activity monitoring techniques		
DD/MM/YY	Incident Response planning and management		
DD/MM/YY	Monitoring unauthorized access and malicious traffic		

DD/MM/YY	Monitoring abuse of system privileges, intrusion detection, events and alerts		
DD/MM/YY	Auditing, record generation, reporting, management and tamper-proofing audit logs		

PART II

THEORY ASSESSMENT FRAMEWORK

Theory Skill Dimensions, CO × TS Mapping, CA / MTE / ETE Structure

7. Theory Skill Dimensions (TS1–TS6)

THEORY-ONLY COURSE — All 6 COs (CO1–CO6) are assessed exclusively via Continuous Assessment (CA), MTE, and ETE. No laboratory component.

Six Theory Skill Dimensions — one per Bloom's progression (L1–L4) — correspond directly to the six COs. They define precisely what competency is being measured in each section of the CA, MTE, and ETE, providing a clear NBA-auditable assessment rationale.

ID	Dimension	What is Measured	CO / BTL	Assessment
TS1	Cloud Computing Fundamentals & Identification	Recall fundamental cloud computing concepts, characteristics, service models, and deployment models; identify suitable cloud solutions for different computing environments	CO1 | L1–L2	CA | MTE Sec A | ETE Sec A
TS2	Cloud Infrastructure & Technology Interpretation	Explain the evolution of cloud computing and interpret the role of enabling technologies including virtualization, physical infrastructure, and logical infrastructure	CO2 | L2–L3	CA | MTE Sec A | ETE Sec A
TS3	Cloud Security Mechanisms & Access Control Application	Apply authentication, authorization, and access control techniques in cloud environments; implement basic cloud security mechanisms and policies	CO3 | L3	CA | MTE Sec B | ETE Sec B

TS4	Cloud Monitoring, Auditing & Management Analysis	Analyze cloud monitoring, auditing, and management techniques; evaluate system performance, reliability, and security trade-offs in cloud environments	CO4 | L4–L5	MTE Sec B | ETE Sec B
TS5	Malware & Virus Analysis	Analyze different types of computer viruses, malware objectives, attack methods, and prevention mechanisms; evaluate the effectiveness of security countermeasures	CO5 | L4–L5	ETE Sec B/C
TS6	Intrusion Detection & Firewall Evaluation	Analyze intrusion detection systems, firewall architectures, and network security mechanisms; evaluate comparative efficiency and suitability for cloud security scenarios	CO6 | L2–L5	ETE Sec C

8. CO × Theory Skill Dimension Mapping (6 COs × 6 Dimensions)

Each CO maps primarily to one TS dimension (H) with adjacent dimensions receiving secondary mapping (M), reflecting the progressive Bloom's structure of this course.

CO	TS1 Conceptual Recall	TS2 Process Interpretation	TS3 Algorithmic Application	TS4 Performance Evaluation	TS5 Memory System Analysis	TS6 File & Disk Evaluation
CO1	H	M				
CO2	M	H	M			
CO3		M	H	M		
CO4			M	H	M	
CO5				M	H	M
CO6		M	M	M	M	H

H = High / Primary alignment M = Medium / Secondary alignment Blank = No direct alignment

9. Continuous Assessment (CA) — 25 Marks

CA is formative and covers COs progressively as the syllabus is taught. It includes numerical-based assignments, a technical video learning report, and a real-world case study — mirroring TS1 through TS6.

9.1 CA Component Breakdown (Sample)

Component	Quantum	Marks	COs Assessed	Skill Dimensions
Assignments 1–5	5 assignments	**15**	CO1, CO2, CO3, CO4	TS1, TS2, TS3, TS4
Technical Video Learning Report	1 Report + Presentation	**5**	CO2, CO3	TS2, TS3
Real-World Case Study (Report)	1 Report	**5**	CO4, CO5, CO6	TS4, TS5, TS6
TOTAL	—	**25**	CO1–CO6	TS1–TS6

9.2 Assignment-wise CO & TS Mapping

Item	Topic / Focus	COs	TS Dims	SL Hours	Evaluation Criteria
Assignment 1	Unit 1 concepts: cloud computing fundamentals, characteristics, service and deployment models	CO1	TS1	5h SL	Report submission + conceptual evaluation
Assignment 2	Cloud infrastructure, virtualization, and enabling technologies	CO2	TS2	5h SL	Short-answer and conceptual analysis
Assignment 3	Cloud access control, authentication, and authorization mechanisms	CO2, CO3	TS2, TS3	5h SL	Security mechanism implementation + comparative analysis
Assignment 4	Cloud monitoring, auditing, and management techniques	CO3, CO4	TS3, TS4	5h SL	Analytical report + security evaluation
Assignment 5	Malware, virus prevention, intrusion detection systems, and firewall techniques	CO4, CO5, CO6	TS4, TS5, TS6	5h SL	Threat analysis + comparative performance evaluation
Video Learning Report	Technical video on cloud security, virtualization, IDS, or firewall mechanisms (min 3 hrs);	CO2, CO3	TS2, TS3	10h SL	Report: learning outcomes, key concepts, self-reflection. Presentation: 10 min

	structured report + class presentation				
Case Study Report	Real-world cloud security case study (e.g., AWS security model, Azure monitoring, Google Cloud IAM, enterprise firewall deployment); in-depth analysis report	CO4, CO5, CO6	TS4, TS5, TS6	10h SL	Technical depth, data collection, fact finding, comparative analysis

10. Mid Term Examination (MTE) — 15 Marks (Units 1–3)

MTE covers Units 1–3 (CO1, CO2, CO3, CO4). CO5 and CO6 are assessed in ETE only. MTE maps to TS1–TS4.

Section	Marks	Theory Skill Dimensions	COs Assessed	Question Type & Guidance
Section A	**10**	TS1 — Cloud Fundamentals Recall & Identification TS2 — Infrastructure & Technology Interpretation	CO1, CO2	Short-answer: define cloud computing models, explain cloud characteristics, identify deployment/service models, describe virtualization concepts, and explain enabling technologies and cloud infrastructure
Section B	**15**	TS3 — Security Mechanism Application TS4 — Monitoring, Auditing & Security Performance Evaluation	CO3, CO4	Application and analytical problems: apply authentication and access control techniques, analyze cloud monitoring and auditing mechanisms, evaluate security policies, compare cloud security approaches, and assess performance and reliability of cloud security solutions
TOTAL	**25**	TS1–TS4	**CO1–CO4**	Units 1–3 only. CO5 and CO6 assessed in ETE only.

11. End Term Examination (ETE) — 60 Marks (All Units, All COs)

ETE is comprehensive — all 5 units and all 6 COs. Full progression from TS1 (recall) through TS6 (evaluation). Minimum 20/50 required to pass.

Section	Marks	Theory Skill Dimensions	COs Assessed	Question Type & Guidance
Section A	**20**	TS1 — Cloud Fundamentals Recall TS2 — Infrastructure & Technology Interpretation	CO1, CO2	Short questions (all units): cloud concepts, service/deployment models, virtualization basics, enabling technologies, cloud infrastructure, and security terminology
Section B	**25**	TS3 — Security Mechanism Application TS4 — Monitoring & Management Analysis TS5 — Malware & Virus Analysis	CO3, CO4, CO5	Medium questions: access control techniques, authentication mechanisms, cloud auditing and monitoring, malware classification, virus prevention methods, and comparative security analysis
Section C	**15**	TS5 — Malware & Virus Analysis TS6 — IDS & Firewall Evaluation	CO5, CO6	Long/evaluation questions: malware attack analysis, intrusion detection system comparison, firewall design principles, cloud security case studies, and evaluation of network protection techniques
TOTAL	**60**	TS1–TS6 (all)	**CO1–CO6**	Scaled from 100-mark paper if needed. Minimum 20/50 to pass.

11.1 CO-wise Assessment Instrument Summary

CO	CO Statement (Short)	CA (25)	MTE (25)	ETE (50)	TS	PO Primary
CO1	Understand fundamental concepts, characteristics, and models of cloud computing	✓	✓	✓	TS1	**PO1, PO2, PO3, PO4**
CO2	Explain cloud evolution and enabling physical/logical infrastructure	✓	✓	✓	TS2	**PO1, PO2, PO3, PO4**
CO3	Apply cloud access control methods and security mechanisms	✓	✓	✓	TS3	**PO1, PO3, PO4, PO5**

CO4	Analyze cloud monitoring, auditing, and management techniques	✓	✓	✓	TS4	**PO2, PO4, PO9, PO10**
CO5	Compare computer viruses and evaluate prevention techniques	✓	—	✓	TS5	**PO1, PO2, PO8, PO9, PO10**
CO6	Analyze intrusion detection systems and firewall design principles	✓	—	✓	TS6	**PO1, PO2, PO4, PO10, PO11**

CO5 and CO6 are NOT assessed in MTE (only Units 1–3 are covered at mid-semester). They are assessed in CA (self-learning activities) and ETE.

PART III

COMBINED MAPPINGS & REFERENCE

CO–PO Matrix, CO–PO Alignment, Self-Learning Activities, Bloom's Reference, Attendance & Pass/Fail

12. CO–PO and CO–PSO Mapping Matrix (Original Framework)

Strength Scale: 3 = Substantial (High) | 2 = Moderate | 1 = Slight (Low) | – = Not Applicable. Averages computed over non-zero entries only. PO framework as per the original course design.

CO	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PSO1	PSO2	PSO3
CO1	3	3	2	2	-	-	-	2	2	2	2	1	3	2
CO2	2	2	3	3	2	3	3	2	2	2	1	1	2	3
CO3	3	3	3	3	-	2	3	1	1	1	3	2	3	2
CO4	2	2	1	2	2	3	2	2	3	3	3	1	2	2
CO5	-	-	-	3	2	-	2	2	2	-	-	-	2	-
CO6	-	2	-	-	-	-	-	-	-	2	2	2	2	-

Avg	1.67	2.00	1.50	2.16	1.00	1.33	1.67	1.50	1.67	1.67	1.83	1.16	2.33	1.50

13. CO × PO Alignment Map (H/M Indicators — All 6 COs)

CO	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PO12	PSO1	PSO2	PSO3
CO1	H	H	M	M				M	M	M	M		H	M	H
CO2	M	M	H	H	M	H	H	M	M	M			M	H	M
CO3	H	H	H	H		M	H				H	M	H	M	H
CO4	M	M		M	M	H	M	M	H	H	H		M	M	M
CO5				H	M		M	M	M				M		
CO6		M								M	M	M	M		

H = High / Primary alignment M = Medium / Secondary alignment *Blank = No direct alignment*

14. Self-Learning Activities (SL: 45 Hours)

S.No	Activity	Hours	COs / TS	Evaluation Criteria
1	**Assignment Writing (5 assignments, problem-based, one per unit focus area)**	5 assignments × 3 hrs each Total = 15 hrs	CO1–CO4 TS1–TS4	Evaluated based on the assignment submitted; correctness, steps shown, performance Cloud Deployment
2	**Technical Video-Based Learning related to the subject (e.g.AWS, Cloud Deployment)**	Video viewing: 7 hrs Report preparation: 7 hrs Presentation: 6 hrs Total = 20 hrs	CO2, CO3 TS2, TS3	Report + Presentation based on video learning outcomes; must capture key concepts, Cloud infrastructure, resource making in AWS

3	**Real-World Case Studies (e.g.S3 bucket integration, Load balancer)**	Data collection/study: 5 hrs Report preparation: 5 hrs Total = 10 hrs	CO4, CO5, CO6 TS4, TS5, TS6	Evaluated based on in-depth study, technical depth, data collected, fact finding, and analytical conclusions drawn
	TOTAL Self-Learning Hours	**45 hours**	CO1–CO6	All activities are compulsory. Submission deadlines communicated at the start of the semester.

15. Bloom's Taxonomy — Domain Level Reference

Cognitive Domain (6 Levels)	Affective Domain (5 Levels)	Psychomotor Domain — Simpson (7 Levels)
L1 — Remember: Recall facts, definitions, basic concepts L2 — Understand: Explain ideas, concepts, and principles L3 — Apply: Use knowledge to solve problems in new situations L4 — Analyze: Break down information, examine relationships L5 — Evaluate: Judge, justify, assess, and make decisions L6 — Create: Design, develop, and produce new artefacts	A1 — Receiving: Awareness and willingness to attend A2 — Responding: Active participation and reaction A3 — Valuing: Commitment and assigning value to content A4 — Organizing: Integrating values into a personal system A5 — Characterizing: Internalized value system	P1 — Perception: Sensory cues guide motor activity P2 — Set: Mental, physical readiness to act P3 — Guided Response: Practice through imitation/trial P4 — Mechanism: Habitual correct performance P5 — Complex Overt Response: Skilled performance P6 — Adaptation: Modify skills for special situations P7 — Origination: Create new solution patterns

OBE Compliance Statement: This is a theory-only course. All 6 COs are mapped primarily to the Cognitive domain (L1–L5). Psychomotor domain (P3) appears only for CO3 (algorithm implementation as mental tracing). Affective domain (A3) appears for CO4 and CO5, reflecting valuing of algorithmic efficiency.

16. Attendance Policy & Pass / Fail Criteria

16.1 Attendance Policy

Component	Minimum	Applicable To	Consequence
Theory Classes	**75%**	All lecture sessions	Debarred from ETE if below threshold
Self-Learning / Assignment Submission	**All activities**	SL activities (30 hrs)	Incomplete SL affects CA score directly

Theory attendance must meet 75% minimum. Missing SL activities (assignments, video report, case study) directly impacts CA marks and is not compensable by exam performance.

16.2 Pass / Fail Criteria

Condition	Threshold	Status	Remarks
ETE Score	**≥ 24 / 60**	**MANDATORY**	40% of ETE paper required; failing ETE means failing the course regardless of CA + MTE
Overall Total (CA + MTE + ETE)	**≥ 40 / 100**	**Must pass overall**	CA 25 + MTE 25 + ETE 50 = 100; 40% overall minimum required

CSCF4200— Cloud Security

Theory-Only Course | 6 COs (CO1–CO6) | 3 Assessment Instruments | 6 Theory Skill Dimensions (TS1–TS6)

CO1–CO2: Conceptual / Understand → TS1, TS2 → CA + MTE Sec A + ETE Sec A

CO3–CO4: Apply / Analyze → TS3, TS4 → CA + MTE Sec B + ETE Sec B

CO5–CO6: Analyze / Evaluate → TS5, TS6 → CA + ETE Sec B/C

CA 25 marks + MTE 25 marks + ETE 50 marks = Total 100 marks

COURSE PLAN

Penetration Testing (CSCF4201)

SSCSE-Sharda School of Computing Science & Engineering) | B.Tech CSE | Semester VII | Batch 2026–2030

Theory-Only Course Plan — All 6 COs (CO1–CO6) | Theory Skill Dimensions TS1–TS6 | CA + MTE + ETE Assessment

PART I

COURSE SYLLABUS

Course Identification, Details, Outcomes, BTL Mapping & Lecture Plan

1. Course Identification

School:	SSCSE-Sharda School of Computing Science & Engineering	**Batch:**	2026–2030
Program:	B.Tech	**Current Academic Year:**	2026-27
Branch:	CSE	**Semester:**	VII
Course Code:	CSCF4201	**Course Type:**	Core — Theory Only

2. Course Details

 THEORY-ONLY COURSE — All 6 COs (CO1–CO6) are assessed exclusively via Continuous Assessment (CA), MTE, and ETE. No laboratory component.

S.No	Attribute	Details
1	**Course Code**	**CSCF4201**
2	**Course Title**	**Penetration Testing**
3	**Credits**	3

4	**Contact Hours (L-T-P-SL)**	3-0-0-3 (Theory: 45 hrs Classroom + 45 hrs Self Learning = 90 hrs total)
5	**Course Status**	**Core — Theory Only (No Laboratory Component)**
6	**Course Objectives**	Students will learn fundamentals of penetration testing via lectures and assignments. Students will investigate various problem and regulation of penetration testing through projects and assignments.
7	**Course Outcomes (COs)**	CO1 (Analyze/Evaluate – L4/L5): Identify the core concepts of penetration testing, and essential penetration testing tools. CO2 (Analyze – L4/L5): Illustrate the legal and ethical considerations involved in penetration testing, including major laws and regulatory acts. CO3 (Apply/Analyze – L3/L4): Demonstrate various social engineering techniques by applying various tactics to simulate real-world scenarios. CO4 (Apply – L3): Apply tools and guidelines for effective vulnerability assessment. CO5 (Understand/Analyze – L2/L4): Analyze common network attacks and assess security flaws. CO6 (Create/Evaluate – L5/L6): Evaluate real-world penetration testing case studies and mitigation strategies.
8	**Course Description**	This course provides an in-depth exploration of penetration testing, covering key concepts, methodologies, and tools used to identify vulnerabilities in network systems. Students will gain hands-on experience in ethical hacking, social engineering, and host reconnaissance while understanding the legal and ethical implications of cybersecurity practices.
9	**Teaching & Learning Scheme**	Classroom Instructions (CI): 45 hrs | Self Learning (SL): 45 hrs | Total: 90 hrs
10	**Mode of Examination**	**Theory Only. CA: 25% | MTE: 15% | ETE: 60% | Total: 100 marks**
11	**Textbook**	David Kennedy, Mati Aharoni, Devon Kearns, Jim O'Gorman and Daniel Graham, Metasploit: The Penetration Tester's Guide, 2nd Edition, No Starch Press, 2025
12	**References**	1. Gerald "Tripp" Roybal III, Penetration Testing with Kali NetHunter, BPB Publications, 2024. 2.Rishabh Bhardwaj, Vulnerability Assessment and Penetration Testing (VAPT), BPB Publications, 2025. 3.Richa Gupta, Hands-on Penetration Testing for Web Applications, 2nd Edition, Google Books, 2025

3. Outline Syllabus with CO Mapping

All CO mappings in this section refer to Theory COs (CO1–CO6). This is a theory-only course; all assessment is via CA, MTE, and ETE.

	Topic	CO Mapping
	Unit 1: Understanding Penetration Testing	
A	Defining penetration testing, types of penetration testing	**CO1, CO2**
B	Understanding Web, LAN, WAN MAN.	**CO1, CO2**
C	Introducing penetration testing tools	**CO1,CO2**
	Unit 2: Legal and ethical consideration	
A	Ethics of penetration testing, Laws: US Law, Computer Fraud and abuse act (CFAA), State Laws	**CO1, CO2**
B	Regulatory Laws: Health Insurance Portability and Accountability Act (HIPAA), Graham-Leach-Bliley (GLB)	**CO1, CO2**
C	Federal Information Security Management Act (FISMA), Sarbanes-Oxley Act (SOX)	**CO1, CO2**
	Unit 3: Performing Social Engineering	
A	Human Psychology: conformity persuasion, logic persuasion, need-based persuasion, authority-based persuasion, reciprocation based social engineering, similarity based social engineering, information based social engineering	**CO3, CO4**
B	First Impressions and the social engineer, tech support impersonation, third-party impersonation	**CO3, CO4**
C	E-Mail impersonation, end user impersonation, customer impersonation, Reverse Social engineering	**CO3, CO4**
	Unit 4: Performing Host Reconnaissance	
A	Passive host reconnaissance, active host reconnaissance	**CO4, CO5**
B	OWASP:	**CO4, CO5**

	• OWASP Top 10 • OWASP Testing Guide • OWASP ZAP	
C	Dealing with IDS, IPS, EDR and XDR	**CO4, CO5**
	Unit 5: Attacking the Network	
A	Understanding injection attacks, Dealing with all forms of XSS, CSRF	**CO4,CO5, CO6**
B	Dealing with API based attack: Broken Authentication	**CO4, CO5, CO6**
C	Case Study: Bangladesh SWIFT code-based attack. Case Study: Digital Arrest	**CO4, CO5, CO6**

4. Topic-wise Bloom's Taxonomy Level Mapping

S.No	Topic	L1 Remember	L2 Understand	L3 Apply	L4 Analyze	L5 Evaluate	L6 Create
1	1.A	✓	✓				
2	1.B	✓	✓	✓			
3	1.C	✓	✓	✓			
4	2.A	✓	✓	✓	✓		
5	2.B	✓	✓	✓	✓		
6	2.C	✓	✓	✓	✓	✓	
7	3.A		✓	✓	✓		
8	3.B		✓	✓	✓	✓	
9	3.C		✓	✓	✓	✓	✓
10	4.A	✓	✓	✓	✓		

11	4.B		✓	✓	✓	✓	
12	4.C		✓	✓	✓	✓	✓
13	5.A		✓	✓	✓	✓	✓
14	5.B		✓	✓	✓	✓	✓
15	5.C		✓	✓	✓	✓	✓

5. CO vs Bloom's Taxonomy — All Three Domains

Only strong/dominant alignments are mapped. This is a theory-only course; Psychomotor mapping is limited to Guided Response (P3) for algorithm implementation in CO3. Affective domain appears at A3 (Valuing) for efficiency analysis in CO4 and CO5.

CO	Cognitive Domain (L1–L6)						Affective (A1–A5)					Psychomotor (P1–P7)						
CO	L1	L2	L3	L4	L5	L6	A1	A2	A3	A4	A5	P1	P2	P3	P4	P5	P6	P7
CO1	✓	✓		✓	✓			✓	✓					✓				
CO2	✓	✓		✓	✓			✓		✓				✓				
CO3		✓	✓	✓					✓	✓			✓	✓	✓			
CO4		✓	✓						✓	✓			✓	✓	✓			
CO5		✓	✓	✓	✓			✓	✓				✓	✓		✓		
CO6				✓	✓	✓			✓	✓	✓			✓	✓	✓	✓	

Legend: ✓= Strong / Dominant mapping. Theory-oriented Cloud Security course: Cognitive domain is primary. Psychomotor domain (P3) is limited to implementation and practical analysis of cloud security mechanisms, intrusion detection, and firewall configuration. Affective domain (A3) reflects valuing security, monitoring, and efficient protection mechanisms in cloud environments.

6. Lecture Plan Outline (Theory — 45 Lectures / 45 Hours)

Total classroom contact: 45 hours across 5 units. Self-Learning activities (45 hrs) are structured separately in Section 11.

Date	Topics to be Covered/Title	UNIT	Total Lectures
DD/MM/YY	Introduction to penetration testing, objectives and phases of penetration testing	**UNIT-1**	**10**
DD/MM/YY	Defining penetration testing and understanding ethical hacking concepts		
DD/MM/YY	Understanding Web, LAN, WAN and MAN networking concepts		
DD/MM/YY	Network architecture and communication protocols in penetration testing		
DD/MM/YY	Introducing penetration testing tools and frameworks		
DD/MM/YY	Practical overview of scanning and reconnaissance tools		
DD/MM/YY	Types of penetration testing: Black box, White box and Gray box testing		
DD/MM/YY	Internal and external penetration testing methodologies		
DD/MM/YY	Penetration testing process, reporting and documentation		
DD/MM/YY	Revision and case discussion on penetration testing basics		
DD/MM/YY	Ethics of penetration testing and professional responsibilities		
DD/MM/YY	Laws related to cybersecurity and ethical hacking		
DD/MM/YY	US Law and Computer Fraud and Abuse Act (CFAA)		

DD/MM/YY	State laws and legal implications of unauthorized access	**UNIT-2**	**8**
DD/MM/YY	Health Insurance Portability and Accountability Act (HIPAA)		
DD/MM/YY	Graham-Leach-Bliley (GLB) Act and data privacy regulations		
DD/MM/YY	Federal Information Security Management Act (FISMA)		
DD/MM/YY	Sarbanes-Oxley Act (SOX) and compliance requirements		
DD/MM/YY	Introduction to human psychology in social engineering	**UNIT-3**	**10**
DD/MM/YY	Conformity persuasion and logic persuasion techniques		
DD/MM/YY	Need-based persuasion and authority-based persuasion		
DD/MM/YY	Reciprocation-based social engineering attacks		
DD/MM/YY	Similarity-based and information-based social engineering		
DD/MM/YY	First impressions and behavior analysis in social engineering		
DD/MM/YY	Tech support impersonation and third-party impersonation attacks		
DD/MM/YY	E-mail impersonation and phishing techniques		
DD/MM/YY	End-user impersonation and customer impersonation		
DD/MM/YY	Reverse social engineering and social engineering case studies		
DD/MM/YY	Introduction to reconnaissance and information gathering		
DD/MM/YY	Passive host reconnaissance techniques		

DD/MM/YY	Active host reconnaissance and foot printing methods	**UNIT-4**	**10**
DD/MM/YY	DNS enumeration and network scanning techniques		
DD/MM/YY	Port scanning and service identification		
DD/MM/YY	Vulnerability scanning and enumeration tools		
DD/MM/YY	Introduction to OWASP and OWASP Top 10 vulnerabilities		
DD/MM/YY	OWASP Testing Guide and secure testing methodologies		
DD/MM/YY	Introduction and practical use of OWASP ZAP		
DD/MM/YY	Reconnaissance and vulnerability assessment practical session		
DD/MM/YY	Understanding IDS, IPS, EDR and XDR technologies	**UNIT-5**	**8**
DD/MM/YY	Techniques for dealing with IDS and IPS systems		
DD/MM/YY	Understanding injection attacks and SQL Injection		
DD/MM/YY	Cross Site Scripting (XSS) attacks and mitigation techniques		
DD/MM/YY	Cross Site Request Forgery (CSRF) attacks and prevention		
DD/MM/YY	API-based attacks and Broken Authentication vulnerabilities		
DD/MM/YY	Case Study: Bangladesh SWIFT code-based cyber attack		
DD/MM/YY	Case Study: Digital Arrest and modern cyber fraud techniques		

PART II

THEORY ASSESSMENT FRAMEWORK

Theory Skill Dimensions, CO × TS Mapping, CA / MTE / ETE Structure

7. Theory Skill Dimensions (TS1–TS6)

THEORY-ONLY COURSE — All 6 COs (CO1–CO6) are assessed exclusively via Continuous Assessment (CA), MTE, and ETE. No laboratory component.

Six Theory Skill Dimensions — one per Bloom's progression (L1–L4) — correspond directly to the six COs. They define precisely what competency is being measured in each section of the CA, MTE, and ETE, providing a clear NBA-auditable assessment rationale.

ID	Dimension	What is Measured	CO / BTL	Assessment
TS1	Penetration Testing Concepts & Tool Identification	Identify and analyze the core concepts of penetration testing, penetration testing methodologies, and essential penetration testing tools used in cyber security assessments	CO1 | L4–L5	CA | MTE Sec A | ETE Sec A
TS2	Legal, Ethical & Regulatory Analysis in Penetration Testing	Analyze legal and ethical considerations involved in penetration testing, including cyber laws, compliance requirements, regulatory acts, and professional responsibilities	CO2 | L4–L5	CA | MTE Sec A | ETE Sec B
TS3	Social Engineering Techniques & Scenario Simulation	Apply and analyze social engineering techniques, persuasion tactics, impersonation methods, and phishing simulations in real-world attack scenarios	CO3 | L3–L4	CA | MTE Sec B | Practical
TS4	Vulnerability Assessment & Security Testing Tools	Apply vulnerability assessment tools, penetration testing frameworks, and security testing guidelines to identify and evaluate system and network weaknesses	CO4 | L3	CA | Practical | ETE Sec B
TS5	Network Attack Analysis & Security Flaw Evaluation	Analyze common network attacks, web application attacks, security flaws, and evaluate defensive mechanisms and security countermeasures	CO5 | L2–L4	MTE Sec B | ETE Sec C

TS6	Penetration Testing Case Study & Mitigation Strategy Design	Evaluate real-world penetration testing case studies and design effective mitigation strategies and security improvement plans for organizational cyber defense	CO6 | L5–L6	ETE Sec C | Project/Case Study

8. CO × Theory Skill Dimension Mapping (6 COs × 6 Dimensions)

Each CO maps primarily to one TS dimension (H) with adjacent dimensions receiving secondary mapping (M), reflecting the progressive Bloom's structure of this course.

CO	TS1 Conceptual Recall	TS2 Process Interpretation	TS3 Algorithmic Application	TS4 Performance Evaluation	TS5 Memory System Analysis	TS6 File & Disk Evaluation
CO1	H	M			M	
CO2	M	H	M			
CO3		M	H	M		
CO4			M	H	M	
CO5				M	H	M
CO6	M		M	M	M	H

H = High / Primary alignment **M** = Medium / Secondary alignment *Blank = No direct alignment*

9. Continuous Assessment (CA) — 25 Marks

CA is formative and covers COs progressively as the syllabus is taught. It includes numerical-based assignments, a technical video learning report, and a real-world case study — mirroring TS1 through TS6.

9.1 CA Component Breakdown (Sample)

Component	Quantum	Marks	COs Assessed	Skill Dimensions
Assignments 1–5	5 assignments	**15**	CO1, CO2, CO3, CO4	TS1, TS2, TS3, TS4

Technical Video Learning Report	1 Report + Presentation	**5**	CO2, CO3	TS2, TS3
Real-World Case Study (Report)	1 Report	**5**	CO4, CO5, CO6	TS4, TS5, TS6
TOTAL	—	**25**	CO1–CO6	TS1–TS6

9.2 Assignment-wise CO & TS Mapping

Item	Topic / Focus	COs	TS Dims	SL Hours	Evaluation Criteria
Assignment 1	Core concepts of penetration testing, penetration testing lifecycle, and identification of essential penetration testing tools	CO1	TS1	5h SL	Report submission + conceptual understanding and tool identification
Assignment 2	Legal and ethical considerations in penetration testing including CFAA, HIPAA, SOX, FISMA, and regulatory compliance analysis	CO2	TS2	5h SL	Short-answer assessment + legal and ethical case analysis
Assignment 3	Social engineering techniques including impersonation, phishing, persuasion tactics, and simulated attack scenarios	CO3	TS3	5h SL	Scenario simulation + analytical comparison of social engineering methods
Assignment 4	Vulnerability assessment methodologies, OWASP tools, penetration testing frameworks, and security testing guidelines	CO4	TS4	5h SL	Practical assessment + analytical vulnerability evaluation report
Assignment 5	Network attack analysis including XSS, CSRF, injection attacks, API attacks, and evaluation of security flaws and countermeasures	CO5	TS5	5h SL	Threat analysis + comparative security evaluation
Video Learning Report	Technical video on penetration testing, vulnerability assessment, IDS/IPS, OWASP, social engineering, or ethical hacking tools (minimum	CO3, CO4, CO6	TS3, TS4, TS6	10h SL	Report: learning outcomes, practical insights, and self-reflection. Presentation: 10 min

	3 hrs) with structured report and presentation				
Case Study Report	Real-world penetration testing case studies such as Bangladesh SWIFT attack, phishing campaigns, ransomware attacks, API exploitation, or enterprise vulnerability assessments with mitigation strategies	CO5, CO6	TS5, TS6	10h SL	Technical depth, fact finding, attack analysis, mitigation planning, and comparative evaluation

10. Mid Term Examination (MTE) — 15 Marks (Units 1–3)

MTE covers Units 1–3 (CO1, CO2, CO3, CO4). CO5 and CO6 are assessed in ETE only. MTE maps to TS1–TS4.

Section	Marks	Theory Skill Dimensions	COs Assessed	Question Type & Guidance
Section A	**10**	TS1 — Penetration Testing Concepts & Tool Identification	CO1	Analytical and evaluative questions on penetration testing concepts, penetration testing phases, ethical hacking methodologies, identification and usage of penetration testing tools, and assessment of organizational security weaknesses
Section B	**15**	TS2 — Legal, Ethical & Regulatory Analysis in Penetration Testing	CO2	Scenario-based and analytical questions involving cyber laws, legal compliance, ethical considerations, CFAA, HIPAA, FISMA, SOX regulations, and evaluation of legal implications in penetration testing activities
TOTAL	**25**	TS1–TS4	**CO1–CO4**	Units 1–3 only. CO5 and CO6 assessed in ETE only.

11. End Term Examination (ETE) — 60 Marks (All Units, All COs)

ETE is comprehensive — all 5 units and all 6 COs. Full progression from TS1 (recall) through TS6 (evaluation). Minimum 20/50 required to pass.

Section	Marks	Theory Skill Dimensions	COs Assessed	Question Type & Guidance
Section A	20	TS1 — Penetration Testing Concepts & Tool Identification TS2 — Legal, Ethical & Regulatory Analysis in Penetration Testing	CO1, CO2	Short-answer questions on penetration testing concepts, penetration testing phases, ethical hacking tools, legal and ethical considerations, cyber laws, regulatory acts, compliance requirements, and professional responsibilities in penetration testing
Section B	25	TS3 — Social Engineering Techniques & Scenario Simulation TS4 — Vulnerability Assessment & Security Testing Tools TS5 — Network Attack Analysis & Security Flaw Evaluation	CO3, CO4, CO5	Medium-level analytical and application-based questions involving phishing and impersonation techniques, social engineering tactics, OWASP tools, vulnerability assessment methods, network attacks, XSS, CSRF, API attacks, and evaluation of security flaws and countermeasures
Section C	15	TS5 — Network Attack Analysis & Security Flaw Evaluation TS6 — Penetration Testing Case Study & Mitigation Strategy Design	CO5, CO6	Long analytical and evaluative questions involving real-world penetration testing case studies, attack analysis, security flaw assessment, mitigation planning, enterprise security improvement strategies, and evaluation of defensive mechanisms
TOTAL	60	TS1–TS6 (all)	CO1–CO6	Scaled from 100-mark paper if needed. Minimum 20/50 to pass.

11.1 CO-wise Assessment Instrument Summary

CO	CO Statement (Short)	CA (25)	MTE (25)	ETE (50)	TS	PO Primary
CO1	Identify penetration testing concepts, methodologies, and essential penetration testing tools used in cyber security assessments	✓	✓	✓	TS1	PO1, PO2, PO3, PO4
CO2	Illustrate legal, ethical, and regulatory considerations involved in penetration testing and cyber security compliance	✓	✓	✓	TS2	PO1, PO2, PO3, PO4
CO3	Demonstrate social engineering techniques and apply persuasion tactics to simulate real-world cyber attack scenarios	✓	✓	✓	TS3	PO1, PO3, PO4, PO5
CO4	Apply vulnerability assessment tools, penetration testing frameworks, and security testing guidelines in practical environments	✓	✓	✓	TS4	PO2, PO4, PO9, PO10
CO5	Analyze network attacks, security flaws, and evaluate defensive mechanisms and security countermeasures	✓	—	✓	TS5	PO1, PO2, PO8, PO9, PO10
CO6	Evaluate penetration testing case studies and develop effective mitigation strategies for organizational cyber defense	✓	—	✓	TS6	PO1, PO2, PO4, PO10, PO11

CO5 and CO6 are NOT assessed in MTE (only Units 1–3 are covered at mid-semester). They are assessed in CA (self-learning activities) and ETE.

PART III

COMBINED MAPPINGS & REFERENCE

CO–PO Matrix, CO–PO Alignment, Self-Learning Activities, Bloom's Reference, Attendance & Pass/Fail

12. CO–PO and CO–PSO Mapping Matrix (Original Framework)

Strength Scale: 3 = Substantial (High) | 2 = Moderate | 1 = Slight (Low) | – = Not Applicable. Averages computed over non-zero entries only. PO framework as per the original course design.

CO	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PSO1	PSO2	PSO3
CO1	3	-	-	-	-	2	-	-	-	-	3	3	3	-
CO2	2	-	-	3	2	-	2	-	1	3	3	3	-	3
CO3	3	3	3	-	3	2	-	-	-	-	2	2	3	-
CO4	3	3	3	3	-	2	2	3	2	-	2	-	-	3
CO5	2	3	2	-	2	2	2	-	-	2	1	-	3	-
CO6	3	3	3	3	3	3	3	3	3	2	3	-	-	3
Avg	2.67	2.00	1.83	1.50	1.67	1.83	1.50	1.00	1.00	1.40	2.33	1.33	1.50	1.50

13. CO × PO Alignment Map (H/M Indicators — All 6 COs)

CO	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PO12	PSO1	PSO2	PSO3
CO1	H					M					H	H	H		H
CO2	M			H	M		M			H	H	H		H	M
CO3	H	H	H		H	M					M	M	H		H
CO4	H	H	H	H		M	M	H	M		M			H	H

CO5	M	H	M		M	M	M			M			H		M
CO6	H	H	H	H	H	H	H	H	H	M	H			H	H

H = High / Primary alignment M = Medium / Secondary alignment *Blank = No direct alignment*

14. Self-Learning Activities (SL: 45 Hours)

S.No	Activity	Hours	COs / TS	Evaluation Criteria
1	**Technical Video based learning related to the subject**	5 assignments × 3 hrs each Total = 15 hrs	CO1–CO4 TS1–TS4	Evaluated based on the assignment submitted; analyze software vulnerabilities
2	**Mini Literature Review on a Technical Topic**	Video viewing: 7 hrs Report preparation: 7 hrs Presentation: 6 hrs Total = 20 hrs	CO2, CO3 TS2, TS3	Report + Presentation based on video learning outcomes; Measure the performance and troubleshoot cyber security systems
3	**Open-Source Project Contribution (GitHub based)**	Data collection/study: 5 hrs Report preparation: 5 hrs Total = 10 hrs	CO4, CO5, CO6 TS4, TS5, TS6	Evaluated based on in-depth study, technical depth, data collected, fact finding, and analytical conclusions drawn
	TOTAL Self-Learning Hours	**45 hours**	CO1–CO6	All activities are compulsory. Submission deadlines communicated at the start of the semester.

15. Bloom's Taxonomy — Domain Level Reference

Cognitive Domain (6 Levels)	Affective Domain (5 Levels)	Psychomotor Domain — Simpson (7 Levels)
L1 — Remember: Recall facts, definitions, basic concepts L2 — Understand: Explain ideas, concepts, and principles L3 — Apply: Use knowledge to solve problems in new situations L4 — Analyze: Break down information, examine relationships	A1 — Receiving: Awareness and willingness to attend A2 — Responding: Active participation and reaction A3 — Valuing: Commitment and assigning value to content A4 — Organizing: Integrating values into a personal system	P1 — Perception: Sensory cues guide motor activity P2 — Set: Mental, physical readiness to act P3 — Guided Response: Practice through imitation/trial P4 — Mechanism: Habitual correct performance

L5 — Evaluate: Judge, justify, assess, and make decisions L6 — Create: Design, develop, and produce new artefacts	A5 — Characterizing: Internalized value system	P5 — Complex Overt Response: Skilled performance P6 — Adaptation: Modify skills for special situations P7 — Origination: Create new solution patterns

OBE Compliance Statement: This is a theory-only course. All 6 COs are mapped primarily to the Cognitive domain (L1–L5). Psychomotor domain (P3) appears only for CO3 (algorithm implementation as mental tracing). Affective domain (A3) appears for CO4 and CO5, reflecting valuing of algorithmic efficiency.

16. Attendance Policy & Pass / Fail Criteria

16.1 Attendance Policy

Component	Minimum	Applicable To	Consequence
Theory Classes	**75%**	All lecture sessions	Debarred from ETE if below threshold
Self-Learning / Assignment Submission	**All activities**	SL activities (30 hrs)	Incomplete SL affects CA score directly

Theory attendance must meet 75% minimum. Missing SL activities (assignments, video report, case study) directly impacts CA marks and is not compensable by exam performance.

16.2 Pass / Fail Criteria

Condition	Threshold	Status	Remarks
ETE Score	**≥ 24 / 60**	**MANDATORY**	40% of ETE paper required; failing ETE means failing the course regardless of CA + MTE
Overall Total (CA + MTE + ETE)	**≥ 40 / 100**	**Must pass overall**	CA 25 + MTE 25 + ETE 50 = 100; 40% overall minimum required

CSCF4201— Penetration Testing

Theory-Only Course | 6 COs (CO1–CO6) | 3 Assessment Instruments | 6 Theory Skill Dimensions (TS1–TS6)

CO1–CO2: Conceptual / Understand → TS1, TS2 → CA + MTE Sec A + ETE Sec A
CO3–CO4: Apply / Analyze → TS3, TS4 → CA + MTE Sec B + ETE Sec B
CO5–CO6: Analyze / Evaluate → TS5, TS6 → CA + ETE Sec B/C

CA 25 marks + MTE 25 marks + ETE 50 marks = Total 100 marks

COURSE PLAN

Exploit Writing (CSCF4202)

Sharda School of Computing Science & Engineering | B.Tech CSE | Semester VII | Batch 2026–2030

Theory-Only Course Plan — All 6 COs (CO1–CO6) | Theory Skill Dimensions TS1–TS6 | CA + MTE + ETE Assessment

PART I

COURSE SYLLABUS

Course Identification, Details, Outcomes, BTL Mapping & Lecture Plan

1. Course Identification

School:	SSCSE	SSCSE - Sharda School of Computing Science & Engineering	**Batch:**	2026–2030	2018–2022
Program:	B.Tech	B.Tech	**Current Academic Year:**	2026–27	2018–19
Branch:	CSE	CSE	**Semester:**	VII	
Course Code:	CSCF4202	CSCF4202	**Course Type:**	Elective	Core — Theory Only

2. Course Details

THEORY-ONLY COURSE — All 6 COs (CO1–CO6) are assessed exclusively via Continuous Assessment (CA), MTE, and ETE. No laboratory component.

S.No	Attribute	Details
1	**Course Code**	**CSCF4202**

2	**Course Title**	**Exploit Writing**
3	**Credits**	3
4	**Contact Hours (L-T-P-SL)**	3-0-0-3 (Theory: 45 hrs Classroom + 45 hrs Self Learning = 90 hrs total)
5	**Course Status**	**Core — Theory Only (No Laboratory Component)**
6	**Course Objectives**	4. Understand exploit development concepts and cybersecurity vulnerabilities, analyze memory-level attacks, 5. Learn exploit writing techniques using scripting and debugging tools, evaluate modern protection mechanisms, and develop secure and 6. Ethical practices in penetration testing and exploit development.
7	**Course Outcomes (COs)**	**After successful completion of this course, students will be able to:** After the completion of this course students will be able to: CO1 (Remember– L1) Define exploit development lifecycle, exploit writing concepts, and their role in cybersecurity CO2 (Understand – L2) Explain scripting techniques using PowerShell and Python for exploit automation CO3 (Apply– L3) Apply buffer overflow concepts and memory-level exploitation techniques CO4 (Analyze – L4) Analyze program execution using debugging tools and identify vulnerabilities CO5 (Evaluate – L5) Evaluate protection mechanisms such as DEP, ASLR, and fuzzing techniques CO6 (Create – L6) Design and implement exploits targeting real-world systems in Windows and Linux
8	**Course Description**	This course introduces exploit writing techniques and their role in penetration testing and security research. It focuses on exploit development

		lifecycle, memory vulnerabilities, debugging techniques, and modern protection mechanisms. Students gain practical exposure to exploit development in real-world systems while emphasizing ethical practices and secure system design.
9	**Teaching & Learning Scheme**	Classroom Instructions (CI): 45 hrs | Self Learning (SL): 45 hrs | Total: 90 hrs
10	**Mode of Examination**	**Theory Only. CA: 25% | MTE: 15% | ETE: 60% | Total: 100 marks**
11	**Textbook**	Textbook: 1. The Art of Exploit Development – Josh Luberisse
12	**References**	Other References: 1. A Guide to Kernel Exploitation – Enrico Perla

3. Outline Syllabus with CO Mapping

All CO mappings in this section refer to Theory COs (CO1–CO6). This is a theory-only course; all assessment is via CA, MTE, and ETE.

	Topic	CO Mapping
	Unit 1: Exploit Writing Basics	
A	Overview of Exploit Writing, Lifecycle, Role in Security	CO1, CO2
B	Exploit Writing and Shellcoding	CO2, CO3
C	Types of Exploits (Stack Overflow)	CO3, CO4
	Unit 2: Programming for Exploits	
A	PowerShell Programming for Exploitation	CO2, CO3
B	Python Scripting for Exploit Development	CO2, CO3, CO6
C	Assembly Language Basics for Exploitation	CO3, CO4
	Unit 3: Debugging & Protection Mechanisms	

A	Debugging in Linux (GDB, Automation)	CO4, CO5
B	Address Space Layout Randomization (ASLR)	CO4, CO5
C	DEP and Memory Protection Mechanisms	CO4, CO5
	Unit 4: Exploit Techniques	
A	A Shellcode Techniques (Spawning, Port Binding, Reverse Shell)	CO3, CO4, CO6
B	Exploit Challenges and Antivirus Bypass	CO4, CO5, CO6
C	Advanced Exploitation (SEH, Egg Hunting)	CO4, CO5, CO6
	Unit 5: Advanced Exploit Applications	
A	Windows & Linux Buffer Overflow Exploitation	CO3, CO4, CO6
B	Kernel Exploitation (UAF, Double Free)	CO4, CO5, CO6
C	Remote Code Execution (RCE) Techniques	CO4, CO5, CO6

4. Topic-wise Bloom's Taxonomy Level Mapping

S.No	Topic	L1 Remember	L2 Understand	L3 Apply	L4 Analyze	L5 Evaluate	L6 Create
1	1.A	✓	✓				
2	1.B		✓	✓			
3	1.C			✓	✓		
4	2.A		✓	✓			

5	2.B		✓	✓			✓
6	2.C			✓	✓		
7	3.A				✓	✓	
8	3.B				✓	✓	
9	3.C				✓	✓	
10	4.A			✓	✓		✓
11	4.B				✓	✓	✓
12	4.C				✓	✓	✓
13	5.A			✓	✓		✓
14	5.B				✓	✓	✓
15	5.C				✓	✓	✓

5. CO vs Bloom's Taxonomy — All Three Domains

Only strong/dominant alignments are mapped. This is a theory-only course; Psychomotor mapping is limited to Guided Response (P3) for algorithm implementation in CO3. Affective domain appears at A3 (Valuing) for efficiency analysis in CO4 and CO5.

CO	Cognitive Domain (L1–L6)						Affective (A1–A5)					Psychomotor (P1–P7)						
CO	L1	L2	L3	L4	L5	L6	A1	A2	A3	A4	A5	P1	P2	P3	P4	P5	P6	P7
CO1	✓						✓					✓						
CO2		✓					✓	✓					✓	✓				
CO3			✓					✓	✓					✓	✓			
CO4				✓					✓	✓					✓	✓		
CO5					✓				✓	✓						✓	✓	

CO6						✓				✓	✓					✓	✓	✓

Legend: ✓ = Strong / Dominant mapping. Theory-only course: Cognitive domain is primary. Psychomotor (P3) limited to CO3 (algorithm implementation). Affective (A3) for CO4 and CO5 (valuing efficiency).

6. Lecture Plan Outline (Theory — 45 Lectures / 45 Hours)

Total classroom contact: 30 hours across 5 units. Self-Learning activities (30 hrs) are structured separately in Section 11.

Lecture No.	Date	Topics to be Covered / Title	Unit	Total Lectures
1	DD/MM/YY	Introduction to Exploit Writing	UNIT-1	9
2	DD/MM/YY	Exploit Development Lifecycle		
3	DD/MM/YY	Role of Exploits in Cyber Security		
4	DD/MM/YY	Prerequisites for Exploit Writing		
5	DD/MM/YY	Basics of Shellcoding		
6	DD/MM/YY	Stack Memory Organization		
7	DD/MM/YY	Stack Overflow Exploits		
8	DD/MM/YY	Simple Buffer Overflow Demonstration		
9	DD/MM/YY	Unit Review and Practice Session		
10	DD/MM/YY	Introduction to Programming for Exploit Development	UNIT-2	9
11	DD/MM/YY	PowerShell Programming Basics		
12	DD/MM/YY	PowerShell Scripting Fundamentals		
13	DD/MM/YY	PowerShell Exploitation Scripts		
14	DD/MM/YY	Python Scripting for Exploit Development		
15	DD/MM/YY	Python Libraries for Networking		
16	DD/MM/YY	Networking Libraries: Socket and Scapy		
17	DD/MM/YY	Assembly Language Basics for Exploits		
18	DD/MM/YY	Assembly Instructions and Registers		
19	DD/MM/YY	Introduction to Debugging Concepts in Linux	UNIT-3	9
20	DD/MM/YY	Linux Process and Memory Management		
21	DD/MM/YY	Getting Started with GDB		
22	DD/MM/YY	Breakpoints and Stack Inspection in GDB		
23	DD/MM/YY	Automating Debugging using GDB Scripts		
24	DD/MM/YY	Address Space Layout Randomization (ASLR)		
25	DD/MM/YY	Techniques for Bypassing ASLR		
26	DD/MM/YY	DEP Protection Mechanisms		

27	DD/MM/YY	Memory Protection Techniques and Review		
28	DD/MM/YY	Introduction to Shellcode Development	UNIT-4	9
29	DD/MM/YY	Writing Basic Shellcode		
30	DD/MM/YY	Shell-Spawning Techniques		
31	DD/MM/YY	Port Binding Concepts		
32	DD/MM/YY	Connect-Back Shells		
33	DD/MM/YY	Introduction to Fuzzing Techniques		
34	DD/MM/YY	SPIKE Fuzzer and Vulnerability Discovery		
35	DD/MM/YY	Exploit Challenges: KSTET and GMON		
36	DD/MM/YY	Antivirus Bypass Techniques		
37	DD/MM/YY	Introduction to Windows and Linux Exploitation	UNIT-5	9
38	DD/MM/YY	Buffer Overflow Exploitation in Windows		
39	DD/MM/YY	Buffer Overflow Exploitation in Linux		
40	DD/MM/YY	Kernel Exploitation Concepts		
41	DD/MM/YY	Use-After-Free and Double Free Vulnerabilities		
42	DD/MM/YY	Remote Code Execution (RCE) Concepts		
43	DD/MM/YY	RCE in Linux: Case Studies		
44	DD/MM/YY	RCE in Windows: Case Studies		
45	DD/MM/YY	Secure Coding Practices and Final Review		

PART II

THEORY ASSESSMENT FRAMEWORK

Theory Skill Dimensions, CO × TS Mapping, CA / MTE / ETE Structure

7. Theory Skill Dimensions (TS1–TS6)

THEORY-ONLY COURSE — All 6 COs (CO1–CO6) are assessed exclusively via Continuous Assessment (CA), MTE, and ETE. No laboratory component.

Six Theory Skill Dimensions — one per Bloom's progression (L1–L4) — correspond directly to the six COs. They define precisely what competency is being measured in each section of the CA, MTE, and ETE, providing a clear NBA-auditable assessment rationale.

ID	Dimension	What is Measured	CO / BTL	Assessment
TS1	**Conceptual Recall & Exploit Fundamentals**	Recall exploit writing terminology, exploit lifecycle, shellcoding concepts, memory structures, and cybersecurity fundamentals; identify exploit categories and attack vectors	CO1 | L1–L2	CA | MTE Sec A | ETE Sec A
TS2	**Conceptual Explanation & Scripting Interpretation**	Explain PowerShell, Python scripting, assembly basics, debugging workflows, and exploit automation techniques; interpret exploit execution flow and memory behavior	CO2 | L2–L3	CA | MTE Sec A | ETE Sec A
TS3	**Exploit Development Application & Implementation**	Apply buffer overflow techniques, shellcoding methods, scripting tools, and debugging utilities to develop and test exploits in controlled environments	CO3 | L3	CA | MTE Sec B | ETE Sec B
TS4	**Vulnerability Analysis & Exploit Evaluation**	Analyze program execution, trace vulnerabilities using debugging tools, identify memory corruption issues, and evaluate exploit feasibility and impact	CO4 | L4–L5	MTE Sec B | ETE Sec B
TS5	**Protection Mechanism & Security Evaluation**	Compare DEP, ASLR, fuzzing, antivirus bypass, and memory protection mechanisms; evaluate their effectiveness against modern exploitation techniques	CO5 | L4–L5	ETE Sec B/C
TS6	**Advanced Exploit Design & System-Level Exploitation**	Design and implement secure exploit strategies targeting Windows/Linux systems, kernel vulnerabilities, and remote code execution scenarios	CO6 | L5–L6	ETE Sec C

8. CO × Theory Skill Dimension Mapping (6 COs × 6 Dimensions)

Each CO maps primarily to one TS dimension (H) with adjacent dimensions receiving secondary mapping (M), reflecting the progressive Bloom's structure of this course.

CO	TS1 Exploit Writing Fundamentals & Security Concepts	TS2 Scripting Techniques & Exploit Automation	TS3 Buffer Overflow & Exploit Implementation	TS4 Debugging & Vulnerability Analysis	TS5 Protection Mechanisms & Security Evaluation	TS6 Advanced Exploit Design & System Exploitation

CO 1	H	H	M		-	-
CO 2	H	H	M	M	M	-
CO 3	H	H	M	H	H	M
CO 4	M	M			M	M
CO 5	M	H	M	M	H	H
CO 6	H	H	H	M	H	H

H = High / Primary alignment **M** = Medium / Secondary alignment *Blank = No direct alignment*

9. Continuous Assessment (CA) — 25 Marks

CA is formative and covers COs progressively as the syllabus is taught. It includes numerical-based assignments, a technical video learning report, and a real-world case study — mirroring TS1 through TS6.

9.1 CA Component Breakdown (Sample)

Component	Quantum	Marks	COs Assessed	Skill Dimensions
Assignments 1–5 (Exploit Development, Buffer Overflow, Shellcoding & Debugging Problems)	5 Assignments	15	CO1, CO2, CO3, CO4	TS1, TS2, TS3, TS4

Technical Tool Demonstration / Video Learning Report	1 Report + Presentation	5	CO2, CO3, CO5	TS2, TS3, TS5
Real-World Exploit Analysis & Vulnerability Case Study (Report)	1 Report	5	CO4, CO5, CO6	TS4, TS5, TS6
TOTAL	—	**25**	**CO1–CO6**	**TS1–TS6**

9.2 Assignment-wise CO & TS Mapping

Item	Topic / Focus	COs	TS Dims	SL Hours	Evaluation Criteria
Assignment 1	concepts: Exploit writing overview, exploit lifecycle, shellcoding basics, types of exploits	CO1, CO2	TS1, TS2	5h SL	Conceptual understanding, terminology accuracy, report submission
Assignment 2	PowerShell and Python scripting for exploit automation, assembly language basics	CO2, CO3	TS2, TS3	5h SL	Script development, workflow explanation, exploit implementation accuracy
Assignment 3	Buffer overflow concepts, shellcode techniques, debugging using GDB and automation tools	CO3, CO4	TS3, TS4	5h SL	Vulnerability analysis, practical implementation, debugging effectiveness
Assignment 4	ASLR, DEP, antivirus bypass, exploit mitigation and protection mechanisms	CO4, CO5	TS4, TS5	5h SL	Comparative analysis, security evaluation, mitigation strategy assessment
Assignment 5	Advanced exploitation: kernel exploits, RCE techniques, Windows/Linux exploit development	CO5, CO6	TS5, TS6	5h SL	Exploit design proposal, advanced exploitation methodology, technical justification

Video Learning Report	Technical video on exploit writing, shellcoding, debugging, fuzzing, or exploit mitigation techniques (min 3 hrs); structured report + presentation	CO2, CO3, CO5	TS2, TS3, TS5	9h SL	Learning outcomes, technical understanding, self-reflection, 10-minute presentation
Case Study Report	Real-world exploit and vulnerability case study (e.g., buffer overflow attacks, WannaCry exploitation, kernel exploits, RCE vulnerabilities)	CO4, CO5, CO6	TS4, TS5, TS6	6h SL	Technical depth, exploit analysis, comparative evaluation, mitigation and defense recommendations

10. Mid Term Examination (MTE) — 15 Marks (Units 1–3)

MTE covers Units 1–3 (CO1, CO2, CO3, CO4). CO5 and CO6 are assessed in ETE only. MTE maps to TS1–TS4.

Section	Marks	Theory Skill Dimensions	COs Assessed	Question Type & Guidance
Section A	10	TS1 — Exploit Writing Fundamentals & Security Concepts TS2 — Scripting Techniques & Exploit Automation	CO1, CO2	Short-answer questions: define exploit writing concepts, explain exploit lifecycle, describe shellcoding basics, explain PowerShell/Python scripting techniques, assembly fundamentals, debugging concepts, and exploit automation workflows
Section B	15	TS3 — Buffer Overflow & Exploit Implementation TS4 — Debugging & Vulnerability Analysis	CO2, CO3, CO4	Analytical and application-based questions: buffer overflow analysis, shellcode implementation, debugging using GDB, vulnerability tracing, exploit workflow analysis, memory corruption interpretation, and exploit development case studies
TOTAL	**25**	**TS1–TS4**	**CO1–CO4**	Units 1–3 only. CO5 and CO6 assessed in ETE only.

11. End Term Examination (ETE) — 60 Marks (All Units, All COs)

ETE is comprehensive — all 5 units and all 6 COs. Full progression from TS1 (recall) through TS6 (evaluation). Minimum 20/50 required to pass.

Section	Marks	Theory Skill Dimensions	COs Assessed	Question Type & Guidance
Section A	15	TS1 — Exploit Writing Fundamentals & Security Concepts TS2 — Scripting Techniques & Exploit Automation	CO1, CO2	Short questions (all units): definitions of exploit writing concepts, exploit lifecycle, shellcoding terminology, scripting fundamentals, assembly basics, debugging concepts, memory structures, and exploit automation techniques
Section B	25	TS3 — Buffer Overflow & Exploit Implementation TS4 — Debugging & Vulnerability Analysis TS5 — Protection Mechanisms & Security Evaluation	CO3, CO4, CO5	Medium questions: buffer overflow analysis, shellcode creation, debugging using GDB, exploit tracing, vulnerability identification, ASLR/DEP analysis, fuzzing techniques, antivirus bypass methods, and exploit mitigation comparisons
Section C	10	TS5 — Protection Mechanisms & Security Evaluation TS6 — Advanced Exploit Design & System Exploitation	CO5, CO6	Long/evaluation questions: Windows/Linux exploit development, kernel exploitation analysis, RCE techniques, advanced exploitation methods (SEH, Egg Hunting), exploit defense evaluation, and real-world exploit case study analysis
TOTAL	**50**	**TS1–TS6 (all)**	**CO1–CO6**	Scaled from 100-mark paper if needed. Minimum 20/50 to pass.

11.1 CO-wise Assessment Instrument Summary

CO	CO Statement (Short)	CA (25)	MTE (25)	ETE (50)	TS	PO Primary
CO1	Understand exploit development lifecycle, exploit writing concepts, and cybersecurity fundamentals	✓	✓	✓	TS1	PO1, PO2, PO3, PO4
CO2	Explain scripting techniques using PowerShell and Python for exploit automation	✓	✓	✓	TS2	PO1, PO2, PO3, PO5
CO3	Apply buffer overflow concepts and memory-level exploitation techniques	✓	✓	✓	TS3	PO1, PO2, PO3, PO5
CO4	Analyze program execution using debugging tools and identify vulnerabilities	✓	✓	✓	TS4	PO2, PO3, PO4, PO10
CO5	Evaluate protection mechanisms such as DEP, ASLR, fuzzing, and exploit mitigation techniques	✓	—	✓	TS5	PO1, PO2, PO8, PO10, PO11
CO6	Design and implement exploits targeting Windows, Linux, and real-world vulnerable systems	✓	—	✓	TS6	PO3, PO4, PO5, PO10, PO11, PO12

CO5 and CO6 are NOT assessed in MTE (only Units 1–3 are covered at mid-semester). They are assessed in CA (self-learning activities) and ETE.

PART III

COMBINED MAPPINGS & REFERENCE

CO–PO Matrix, CO–PO Alignment, Self-Learning Activities, Bloom's Reference, Attendance & Pass/Fail

12. CO–PO and CO–PSO Mapping Matrix (Original Framework)

Strength Scale: 3 = Substantial (High) | 2 = Moderate | 1 = Slight (Low) | – = Not Applicable. Averages computed over non-zero entries only. PO framework as per the original course design.

CO	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PSO1	PSO2	PSO3
CO1	3	3	2	1	-	-	-	-	-	-	2	2	3	2
CO2	3	3	2	2	2	-	-	-	-	-	3	3	3	3
CO3	3	3	2	3	3	2	-	2	2	2	2	3	2	3
CO4	2	2	1	1	2	2	2	2	-	1	2	2	2	2
CO5	2	3	2	2	3	3	2	-	2	2	1	2	2	2
CO6	3	3	3	2	3	3	3	2	2	3	3	3	3	3
Avg	2.67	2.83	2.00	1.83	2.60	2.50	2.33	2.00	2.00	2.00	2.17	2.50	2.50	2.50

13. CO × PO Alignment Map (H/M Indicators — All 6 COs)

CO	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PSO1	PSO2	PSO3
CO1	H	H	M		-	-	-	-	-	-	M	M	H	M
CO2	H	H	M	M	M	-	-	-	-	-	H	H	H	H
CO3	H	H	M	H	H	M	-	M	M	M	M	H	M	H
CO4	M	M			M	M	M	M	-		M	M	M	M
CO5	M	H	M	M	H	H	M	-	M	M		M	M	M
CO6	H	H	H	M	H	H	H	M	M	H	H	H	H	H

14. Self-Learning Activities (SL: 45 Hours)

S.No	Activity	Hours	COs / TS	Evaluation Criteria
1	Assignment Writing (5 assignments based on exploit development, shellcoding, buffer overflow analysis, debugging, and exploit mitigation techniques)	5 assignments × 3 hrs each Total = 15 hrs	CO1–CO4 TS1–TS4	Evaluated based on assignment submission, exploit analysis accuracy, vulnerability identification, scripting/debugging tool usage, shellcode implementation, and analytical reasoning
2	Technical Video-Based Learning related to Exploit Writing and Vulnerability Research (e.g., buffer overflows, GDB debugging, shellcoding, ASLR/DEP bypass, fuzzing techniques)	Total = 15 hrs	CO2, CO3, CO5 TS2, TS3, TS5	Report + Presentation based on learning outcomes; must include exploit development concepts, debugging workflows, protection mechanisms, exploit-defense techniques, and personal technical reflections
3	Real-World Exploit & Vulnerability Case Studies (e.g., WannaCry exploitation, EternalBlue, kernel exploits, RCE vulnerabilities, antivirus bypass techniques)	Total = 15 hrs	CO4, CO5, CO6 TS4, TS5, TS6	Evaluated based on technical depth, exploit analysis, debugging observations, vulnerability assessment, mitigation strategies, secure exploitation practices, and analytical conclusions
	TOTAL Self-Learning Hours	**45 hours**	**CO1–CO6**	All activities are compulsory. Submission deadlines communicated at the start of the semester.

15. Bloom's Taxonomy — Domain Level Reference

Cognitive Domain (6 Levels)	Affective Domain (5 Levels)	Psychomotor Domain — Simpson (7 Levels)
L1 — Remember: Recall facts, definitions, basic concepts L2 — Understand: Explain ideas, concepts, and principles L3 — Apply: Use knowledge to solve problems in new situations L4 — Analyze: Break down information, examine relationships	A1 — Receiving: Awareness and willingness to attend A2 — Responding: Active participation and reaction A3 — Valuing: Commitment and assigning value to content A4 — Organizing: Integrating values into a personal system	P1 — Perception: Sensory cues guide motor activity P2 — Set: Mental, physical readiness to act P3 — Guided Response: Practice through imitation/trial P4 — Mechanism: Habitual correct performance

L5 — Evaluate: Judge, justify, assess, and make decisions L6 — Create: Design, develop, and produce new artefacts	A5 — Characterizing: Internalized value system	P5 — Complex Overt Response: Skilled performance P6 — Adaptation: Modify skills for special situations P7 — Origination: Create new solution patterns

OBE Compliance Statement: This is a theory-only course. All 6 COs are mapped primarily to the Cognitive domain (L1–L5). Psychomotor domain (P3) appears only for CO3 (algorithm implementation as mental tracing). Affective domain (A3) appears for CO4 and CO5, reflecting valuing of algorithmic efficiency.

16. Attendance Policy & Pass / Fail Criteria

16.1 Attendance Policy

Component	Minimum	Applicable To	Consequence
Theory Classes	**75%**	All lecture sessions	Debarred from ETE if below threshold
Self-Learning / Assignment Submission	**All activities**	SL activities (30 hrs)	Incomplete SL affects CA score directly

Theory attendance must meet 75% minimum. Missing SL activities (assignments, video report, case study) directly impacts CA marks and is not compensable by exam performance.

16.2 Pass / Fail Criteria

Condition	Threshold	Status	Remarks
ETE Score	**≥ 24 / 60**	**MANDATORY**	40% of ETE paper required; failing ETE means failing the course regardless of CA + MTE
Overall Total (CA + MTE + ETE)	**≥ 40 / 100**	**Must pass overall**	CA 25 + MTE 25 + ETE 50 = 100; 40% overall minimum required

CSCF4202— EXPLOIT WRITING

Theory-Only Course | 6 COs (CO1–CO6) | 3 Assessment Instruments | 6 Theory Skill Dimensions (TS1–TS6)

CO1–CO2: Conceptual / Understand → TS1, TS2 → CA + MTE Sec A + ETE Sec A

CO3–CO4: Apply / Analyze → TS3, TS4 → CA + MTE Sec B + ETE Sec B

CO5–CO6: Analyze / Evaluate → TS5, TS6 → CA + ETE Sec B/C

CA 25 marks + MTE 25 marks + ETE 50 marks = Total 100 marks

COURSE PLAN

Risk Management (CSCF4203)

Sharda School of Computing Science & Engineering (SSCSE-) | B.Tech CSCF | Semester VII | Batch 2026–2030

Theory-Only Course Plan — All 6 COs (CO1–CO6) | Theory Skill Dimensions TS1–TS6 | CA + MTE + ETE Assessment

PART I

COURSE SYLLABUS

Course Identification, Details, Outcomes, BTL Mapping & Lecture Plan

1. Course Identification

School:	SSCSE- Sharda School of Computing Science & Engineering	**Batch:**	2026–2030
Program:	B.Tech	**Current Academic Year:**	2026-27
Branch:	CSE	**Semester:**	VII
Course Code:	CSCF4203	**Course Type:**	Core — Theory Only

2. Course Details

 THEORY-ONLY COURSE — All 6 COs (CO1–CO6) are assessed exclusively via Continuous Assessment (CA), MTE, and ETE. No laboratory component.

S.No	Attribute	Details
1	**Course Code**	**CSCF4203**
2	**Course Title**	Risk Management
3	**Credits**	3

4	**Contact Hours (L-T-P-SL)**	3-0-0-3 (Theory: 45 hrs Classroom + 45 hrs Self Learning = 90 hrs total)
5	**Course Status**	**Core — Theory Only (No Laboratory Component)**
6	**Course Objectives**	1. Understand the principles, importance, and various types of risks in organizations and projects. 2. Analyze and evaluate risks using qualitative and quantitative risk assessment methods. 3. Develop and implement risk mitigation, control, and management strategies effectively. 4. Apply risk management frameworks while ensuring proper communication, compliance, ethical, and regulatory practices
7	**Course Outcomes (COs)**	**After successful completion of this course, students will be able to:** CO1 (Understand – L1/L2): Define the basic concept of risk, types, uncertainty, managing, evaluation and prediction of risk. CO2 (Explore – L2/L3): Illustrate the key stages, component, framework, standards, architecture, strategy policies, and protocols process of the risk management. CO3 (Apply – L3): Identify various risk, score them, control and opportunity risk. CO4 (Analyze – L4/L5): Apply approach/technique of risk assessment for strategy, projects and operations, and make use of risk matrix. CO5 (Analyze – L4/L5): Analyze uncertainty and risk in projects and apply measurement. CO6 (Analyze – L2/L4): Explain, compare and apply risk management concept and techniques in projects to the success of the organization.
8	**Course Description**	This course is to provide students with the concepts and fundamentals of risk management, a study of risk assessment and management techniques, methods, and models used in industry to minimize, control and communicate risks.
9	**Teaching & Learning Scheme**	Classroom Instructions (CI): 45 hrs | Self Learning (SL): 45 hrs | Total: 90 hrs
10	**Mode of Examination**	**Theory Only. CA: 25% | MTE: 15% | ETE: 60% | Total: 100 marks**
11	**Textbook**	Paul Hopkin, "Fundamental of Risk Management- Understanding evaluating and implementing effective risk management", Kogan Page London Philadelphia New Delhi.
12	**References**	1. Crouhy, Michel, Dan Galai, and Robert Mark. *The Essentials of Risk Management*. McGraw-Hill Education, New York. 2. Hull, John C. *Risk Management and Financial Institutions*. Wiley, Hoboken, New Jersey. 3. Lam, James. *Enterprise Risk Management: From Incentives to Controls*. Wiley, Hoboken, New Jersey.

		4. McNeil, Alexander J., Rüdiger Frey, and Paul Embrechts. *Quantitative Risk Management: Concepts, Techniques and Tools*. Princeton University Press, Princeton, New Jersey.

3. Outline Syllabus with CO Mapping

All CO mappings in this section refer to Theory COs (CO1–CO6). This is a theory-only course; all assessment is via CA, MTE, and ETE.

	Topic	CO Mapping
	Unit 1: Introduction to Risk Management	
A	The Concept of Risk, Risk and Uncertainty: Distinction, Classification of Risks	**CO1**
B	Managing Risk, Sources and Measurement of Risk	**CO1**
C	Risk Evaluation and Prediction, Types of Risk	**CO1**
	Unit 2: Principles and aims of risk management	
A	Principles of risk management, Importance of risk management, Risk management activities, Perspectives of risk management	**CO1, CO2**
B	Scope of risk management standards, Risk management process, Risk management framework	**CO1, CO2**
C	Risk architecture, strategy Policies and protocols	**CO1, CO2**
	Unit 3: Risk classification Systems	
A	Short-, medium- and long-term Risk	**CO1, CO2, CO3**
B	FIRM risk scorecard, PESTLE risk classification system	**CO1, CO2, CO3, CO4**
C	Hazard, control and opportunity risk	**CO1, CO2, CO3, CO4**
	Unit 4: Risk Assessment	
A	Importance of risk assessment, Approaches to risk assessment, risk assessment techniques	**CO1, CO2, CO3, CO5**

B	Risk Matrix, Risk Perception, Risk appetite	**CO1, CO2, CO3, CO5**
C	Application of risk matrix, inherent and current level of risk, 4T's of risk response	**CO1, CO2, CO3, CO5**
	Unit 5: Risk Management	
A	Importance of risk appetite – Risk tolerance, treatment, termination	**CO1, CO2, CO3, CO6**
B	Introduction to Project Risk Management, uncertainty in projects , project lifecycle, Project risk analysis and management	**CO1, CO2, CO3, CO4, CO6**
C	Operational risk management- definition, measurement, difficulties of measurement	**CO1, CO2, CO3, CO6**

4. Topic-wise Bloom's Taxonomy Level Mapping

S.No	Topic	L1 Remember	L2 Understand	L3 Apply	L4 Analyze	L5 Evaluate	L6 Create
1	1.A	□	□				
2	1.B	□	□				
3	1.C		□				
4	2.A		□	□			
5	2.B		□	□			
6	2.C			□	□		
7	3.A	□					
8	3.B			□	□		
9	3.C			□	□	□	
10	4.A		□				

11	4.B			□	□		
12	4.C			□	□	□	
13	5.A		□	□			
14	5.B			□	□		
15	5.C		□	□	□		

5. CO vs Bloom's Taxonomy — All Three Domains

□ *Only strong/dominant alignments are mapped. This is a theory-only course; Psychomotor mapping is limited to Guided Response (P3) for algorithm implementation in CO3. Affective domain appears at A3 (Valuing) for efficiency analysis in CO4 and CO5.*

CO	Cognitive Domain (L1–L6)						Affective (A1–A5)					Psychomotor (P1–P7)						
CO	L1	L2	L3	L4	L5	L6	A1	A2	A3	A4	A5	P1	P2	P3	P4	P5	P6	P7
CO1	□	□																
CO2		□	□															
CO3			□	□											□			
CO4				□	□				□									
CO5				□	□			□										
CO6		□	□	□														

Legend: □ = Strong / Dominant mapping. Theory-only course: Cognitive domain is primary. Psychomotor (P3) limited to CO3 (algorithm implementation). Affective (A3) for CO4 and CO5 (valuing efficiency).

6. Lecture Plan Outline (Theory — 45 Lectures /45 Hours)

Total classroom contact: 45 hours across 5 units. Self-Learning activities (45 hrs) are structured separately in Section 11.

Date	Topics to be Covered/Title	UNIT	Total Lectures
DD/MM/YY	The Concept of Risk	UNIT-1	8
DD/MM/YY	Risk and Uncertainty: Distinction		
DD/MM/YY	Classification of Risks		
DD/MM/YY	Managing Risk		
DD/MM/YY	Sources and Measurement of Risk		
DD/MM/YY	Risk Evaluation		
DD/MM/YY	Risk Prediction,		
DD/MM/YY	Types of Risk		
DD/MM/YY	Principles of risk management	UNIT-2	10
DD/MM/YY	Importance of risk management		
DD/MM/YY	Risk management activities		
DD/MM/YY	Perspectives of risk management		
DD/MM/YY	Scope of risk management standards		
DD/MM/YY	Risk management process		
DD/MM/YY	Risk management framework		
DD/MM/YY	Risk architecture,		
DD/MM/YY	Strategy Policies		
DD/MM/YY	Risk protocols		

DD/MM/YY	Short-, medium- and long-term Risk	UNIT-3	8
DD/MM/YY	FIRM risk scorecard		
DD/MM/YY	FIRM risk scorecard		
DD/MM/YY	PESTLE risk classification system		
DD/MM/YY	PESTLE risk classification system		
DD/MM/YY	Hazard, control and opportunity risk		
DD/MM/YY	Hazard, control and opportunity risk		
DD/MM/YY	Hazard, control and opportunity risk		
DD/MM/YY	Importance of risk assessment	UNIT-4	9
DD/MM/YY	Approaches to risk assessment		
DD/MM/YY	risk assessment techniques		
DD/MM/YY	Risk Matrix		
DD/MM/YY	Risk Perception		
DD/MM/YY	Risk appetite		
DD/MM/YY	Application of risk matrix		
DD/MM/YY	inherent and current level of risk		
DD/MM/YY	4T's of risk response		
DD/MM/YY	Importance of risk appetite – Risk tolerance, treatment, termination	UNIT-5	10
DD/MM/YY	Importance of risk appetite – Risk tolerance, treatment, termination		
DD/MM/YY	Importance of risk appetite – Risk tolerance, treatment, termination		
DD/MM/YY	Introduction to Project Risk Management		
DD/MM/YY	uncertainty in projects		
DD/MM/YY	project lifecycle		

DD/MM/YY	Project risk analysis and management		
DD/MM/YY	Operational risk management- definition, measurement, difficulties of measurement		
DD/MM/YY	Operational risk management- definition, measurement, difficulties of measurement		
DD/MM/YY	Operational risk management- definition, measurement, difficulties of measurement		

PART II

THEORY ASSESSMENT FRAMEWORK

Theory Skill Dimensions, CO × TS Mapping, CA / MTE / ETE Structure

7. Theory Skill Dimensions (TS1–TS6)

THEORY-ONLY COURSE — All 6 COs (CO1–CO6) are assessed exclusively via Continuous Assessment (CA), MTE, and ETE. No laboratory component.

Six Theory Skill Dimensions — one per Bloom's progression (L1–L4) — correspond directly to the six COs. They define precisely what competency is being measured in each section of the CA, MTE, and ETE, providing a clear NBA-auditable assessment rationale.

ID	Dimension	What is Measured	CO / BTL	Assessment
TS1	**Introduction to Risk Management**	Define the basic concept of risk, types, uncertainty, managing, evaluation and prediction of risk	CO1 | L1–L2	CA | MTE Sec A | ETE Sec A
TS2	**Principles and aims of risk management**	Illustrate the key stages, component, framework, standards, architecture, strategy policies, and protocols process of the risk management.	CO2 | L2–L3	CA | MTE Sec A | ETE Sec A
TS3	**Risk classification Systems**	Identify various risk, score them, control and opportunity risk.	CO3 | L3	CA | MTE Sec B | ETE Sec B

TS4	**Risk Assessment**	Apply approach/technique of risk assessment for strategy, projects and operations, and make use of risk matrix.	CO4 | L4–L5	MTE Sec B | ETE Sec B
TS5	**Risk Management**	Analyze uncertainty and risk in projects and apply measurement.	CO5 | L4–L5	ETE Sec B/C
TS6	**Risk Management**	Explain, compare and apply risk management concept and techniques in projects to the success of the organization	CO6 | L2–L4	ETE Sec C

8. CO × Theory Skill Dimension Mapping (6 COs × 6 Dimensions)

Each CO maps primarily to one TS dimension (H) with adjacent dimensions receiving secondary mapping (M), reflecting the progressive Bloom's structure of this course.

CO	TS1 Conceptual Recall	TS2 Process Interpretation	TS3 Algorithmic Application	TS4 Performance Evaluation	TS5 Memory System Analysis	TS6 File & Disk Evaluation
CO1	**H**	**M**				
CO2	**M**	**H**	**M**			
CO3		**M**	**H**	**M**		
CO4			**M**	**H**	**M**	
CO5				**M**	**H**	**M**
CO6		**M**		**M**	**M**	**H**

H = High / Primary alignment **M** = Medium / Secondary alignment *Blank = No direct alignment*

9. Continuous Assessment (CA) — 25 Marks

CA is formative and covers COs progressively as the syllabus is taught. It includes numerical-based assignments, a technical video learning report, and a real-world case study — mirroring TS1 through TS6.

9.1 CA Component Breakdown (Sample)

Component	Quantum	Marks	COs Assessed	Skill Dimensions
Assignments 1–5	5 assignments	**15**	CO1, CO2, CO3, CO4	TS1, TS2, TS3, TS4
Technical Video Learning Report	1 Report + Presentation	**5**	CO2, CO3	TS2, TS3
Real-World Case Study (Report)	1 Report	**5**	CO4, CO5, CO6	TS4, TS5, TS6
TOTAL	—	**25**	CO1–CO6	TS1–TS6

9.2 Assignment-wise CO & TS Mapping

Item	Topic / Focus	COs	TS Dims	SL Hours	Evaluation Criteria
Assignment 1	The Concept of Risk, Risk and Uncertainty: Distinction, Classification of Risks	CO1	TS1	5h SL	Report submission + evaluation
Assignment 2	Principles of risk management, Importance of risk management, Risk management activities, Perspectives of risk management	CO2	TS2	5h SL	Numerical problems on process management
Assignment 3	FIRM risk scorecard, PESTLE risk classification system	CO2, CO3	TS2, TS3	5h SL	Numerical computation + comparison
Assignment 4	Application of risk matrix, inherent and current level of risk, 4T's of risk response	CO3, CO4	TS3, TS4	5h SL	Step-by-step numerical trace required
Assignment 5	Importance of risk appetite – Risk tolerance, treatment, termination	CO3, CO4, CO5	TS3, TS4, TS5	5h SL	Algorithm application + performance analysis
Video Learning Report	Technical video on Risk Management	CO2, CO3	TS2, TS3	9h SL	Report: learning outcomes, key concepts, self-reflection. Presentation: 10 min
Case Study Report	Real-world Risk Management case study	CO4, CO5, CO6	TS4, TS5, TS6	6h SL	Technical depth, data collection, fact finding, comparative analysis

10. Mid Term Examination (MTE) — 15 Marks (Units 1–3)

MTE covers Units 1–3 (CO1, CO2, CO3, CO4). CO5 and CO6 are assessed in ETE only. MTE maps to TS1–TS4.

Section	Marks	Theory Skill Dimensions	COs Assessed	Question Type & Guidance
Section A	**10**	Principles of risk management, Importance of risk management, Risk management activities, Perspectives of risk management	**CO1, CO2**	Short-answer: define OS types, explain process states, IPC mechanisms, describe semaphore working, identify scheduling criteria
Section B	**15**	TS3 — Application of risk matrix, inherent and current level of risk, 4T's of risk response TS4 — Algorithmic Analysis & Performance Evaluation	**CO2, CO3, CO4**	Numerical problems: compute Gantt charts, CPU utilization, waiting/turnaround time; apply Banker's Algorithm; compare scheduling algorithms on performance criteria
TOTAL	**25**	TS1–TS4	**CO1–CO4**	Units 1–3 only. CO5 and CO6 assessed in ETE only.

11. End Term Examination (ETE) — 60 Marks (All Units, All COs)

ETE is comprehensive — all 5 units and all 6 COs. Full progression from TS1 (recall) through TS6 (evaluation). Minimum 20/50 required to pass.

Section	Marks	Theory Skill Dimensions	COs Assessed	Question Type & Guidance
Section A	**15**	TS1 — Conceptual Recall TS2 — Principles of risk management, Importance of risk management, Risk management activities, Perspectives of risk management	**CO1, CO2**	Short questions (all units): definitions, OS type identification, process state diagrams, IPC mechanisms, synchronization concepts
Section B	**25**	TS3 — Risk classification Systems	**CO3, CO4, CO5**	Medium questions: scheduling algorithm numericals, deadlock handling, paging/segmentation

		TS4 — Risk Assessment TS5 — Risk Management		calculations, page replacement algorithm traces, performance comparisons
Section C	**10**	TS5 — Risk Management TS6 — Risk Management	**CO5, CO6**	Long/evaluation questions: virtual memory analysis, thrashing, disk scheduling comparisons (FCFS/SSTF/SCAN/C-SCAN), file system design, Windows OS case study analysis
TOTAL	**50**	TS1–TS6 (all)	**CO1–CO6**	Scaled from 100-mark paper if needed. Minimum 20/50 to pass.

11.1 CO-wise Assessment Instrument Summary

CO	CO Statement (Short)	CA (25)	MTE (25)	ETE (50)	TS	PO Primary
CO1	Define the basic concept of risk, types, uncertainty, managing, evaluation and prediction of risk.	□	□	□	TS1	PO1, PO2, PO3, PO4
CO2	Illustrate the key stages, component, framework, standards, architecture, strategy policies, and protocols process of the risk management.	□	□	□	TS2	PO1, PO3, PO4
CO3	Identify various risk, score them, control and opportunity risk	□	□	□	TS3	PO1, PO2, PO3, PO4
CO4	Apply approach/technique of risk assessment for strategy, projects and operations, and make use of risk matrix.	□	□	□	TS4	PO9, PO10, PO11
CO5	Analyze uncertainty and risk in projects and apply measurement.	□	—	□	TS5	PO1, PO2, PO8, PO9, PO10
CO6	Explain, compare and apply risk management concept and techniques in projects to the success of the organization.	□	—	□	TS6	PO1, PO2, PO10, PO11

□ *CO5 and CO6 are NOT assessed in MTE (only Units 1–3 are covered at mid-semester). They are assessed in CA (self-learning activities) and ETE.*

PART III

COMBINED MAPPINGS & REFERENCE

CO–PO Matrix, CO–PO Alignment, Self-Learning Activities, Bloom's Reference, Attendance & Pass/Fail

12. CO–PO and CO–PSO Mapping Matrix (Original Framework)

Strength Scale: 3 = Substantial (High) | 2 = Moderate | 1 = Slight (Low) | – = Not Applicable. Averages computed over non-zero entries only. PO framework as per the original course design.

CO	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PO12	PSO1	PSO2	PSO3
CO1	3	3	3	3	–	–	–	2	2	1	2	1	3	2	2
CO2	3	2	3	3	–	–	–	2	2	2	1	1	2	3	2
CO3	3	3	3	3	–	–	–	1	1	1	3	2	3	2	1
CO4	2	2	2	2	1	–	–	2	3	3	3	1	2	2	2
CO5	2	2	3	–	–	–	–	3	3	1	2	–	3	–	–
CO6	3	2	–	–	–	–	–	–	–	2	3	–	2	2	–
Avg	**2.67**	**2.33**	**2.80**	**2.75**	**1.00**	**–**	**–**	**2.00**	**2.20**	**1.67**	**2.33**	**1.25**	**2.50**	**2.20**	**1.75**

13. CO × PO Alignment Map (H/M Indicators — All 6 COs)

CO	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PO12	PSO1	PSO2	PSO3
CO1	H	H	H	H				M	M	M	M	M	H	M	M
CO2	H	M	H	H				M	M	M	M	M	M	H	M
CO3	H	H	H	H				M	M	M	H	M	H	M	M
CO4	M	M	M	M	M			M	H	H	H	M	M	M	M
CO5	M	M	H					H	H	M	M		H		
CO6	H	M								M	H		M	M	

H = High / Primary alignment M = Medium / Secondary alignment *Blank = No direct alignment*

14. Self-Learning Activities (SL: 45 Hours)

S.No	Activity	Hours	COs / TS	Evaluation Criteria
1	**Numerical Assignment Writing (5 assignments, problem-based, one per unit focus area)**	5 assignments × 3 hrs each Total = 15 hrs	CO1–CO4 TS1–TS4	Evaluated based on the assignment submitted; correctness, steps shown, comparison of algorithm performance
2	**Real world case studies-based learning**	Duration of data collection/study = 5h Report preparation = 10h Total = 15h	CO2, CO3 TS2, TS3	Based on in-depth study, technical depth, data collected, fact finding, etc.
3	**Reverse Engineering of a Product/System**	Product study=7 h; Functional analysis=4 h; Report= 4 h, Total =15h	CO4, CO5, CO6 TS4, TS5, TS6	Technical understanding, diagrams, explanation of working
	TOTAL Self-Learning Hours	**30 hours**	CO1–CO6	All activities are compulsory. Submission deadlines communicated at the start of the semester.

15. Bloom's Taxonomy — Domain Level Reference

Cognitive Domain (6 Levels)	Affective Domain (5 Levels)	Psychomotor Domain — Simpson (7 Levels)
L1 — Remember: Recall facts, definitions, basic concepts L2 — Understand: Explain ideas, concepts, and principles L3 — Apply: Use knowledge to solve problems in new situations L4 — Analyze: Break down information, examine relationships L5 — Evaluate: Judge, justify, assess, and make decisions L6 — Create: Design, develop, and produce new artefacts	A1 — Receiving: Awareness and willingness to attend A2 — Responding: Active participation and reaction A3 — Valuing: Commitment and assigning value to content A4 — Organizing: Integrating values into a personal system A5 — Characterizing: Internalized value system	P1 — Perception: Sensory cues guide motor activity P2 — Set: Mental, physical readiness to act P3 — Guided Response: Practice through imitation/trial P4 — Mechanism: Habitual correct performance P5 — Complex Overt Response: Skilled performance P6 — Adaptation: Modify skills for special situations P7 — Origination: Create new solution patterns

OBE Compliance Statement: This is a theory-only course. All 6 COs are mapped primarily to the Cognitive domain (L1–L5). Psychomotor domain (P3) appears only for CO3 (algorithm implementation as mental tracing). Affective domain (A3) appears for CO4 and CO5, reflecting valuing of algorithmic efficiency.

16. Attendance Policy & Pass / Fail Criteria

16.1 Attendance Policy

Component	Minimum	Applicable To	Consequence
Theory Classes	**75%**	All lecture sessions	Debarred from ETE if below threshold
Self-Learning / Assignment Submission	**All activities**	SL activities (30 hrs)	Incomplete SL affects CA score directly

Theory attendance must meet 75% minimum. Missing SL activities (assignments, video report, case study) directly impacts CA marks and is not compensable by exam performance.

16.2 Pass / Fail Criteria

Condition	Threshold	Status	Remarks
ETE Score	**≥ 24 / 60**	**MANDATORY**	40% of ETE paper required; failing ETE means failing the course regardless of CA + MTE
Overall Total (CA + MTE + ETE)	**≥ 40 / 100**	**Must pass overall**	CA 25 + MTE 15 + ETE 60 = 100; 40% overall minimum required

CSCF 4203 — MEASUREMENT ARCHITECTURE SUMMARY

Theory-Only Course | 6 COs (CO1–CO6) | 3 Assessment Instruments | 6 Theory Skill Dimensions (TS1–TS6)

CO1–CO2: Conceptual / Understand → TS1, TS2 → CA + MTE Sec A + ETE Sec A

CO3–CO4: Apply / Analyze → TS3, TS4 → CA + MTE Sec B + ETE Sec B

CO5–CO6: Analyze / Evaluate → TS5, TS6 → CA + ETE Sec B/C

CA 25 marks + MTE 25 marks + ETE 50 marks = Total 100 marks

COURSE PLAN

Digital Watermarking & Steganography (CSCF4204)

School of Computing Engineering and Technology (SSCSE) | B.Tech CSE | Semester VII | Batch 2026–2030

Theory-Only Course Plan — All 6 COs (CO1–CO6) | Theory Skill Dimensions TS1–TS6 | CA + MTE + ETE Assessment

PART I

COURSE SYLLABUS

Course Identification, Details, Outcomes, BTL Mapping & Lecture Plan

1. Course Identification

School:	SSCSE	School of Computing Science and Engineering	**Batch:**	2026–2030	2018–2022
Program:	B.Tech	B.Tech	**Current Academic Year:**	2026–27	2018–19
Branch:	CSE	CSE	**Semester:**	VII	IV
Course Code:	CSCF4204		**Course Type:**	Elective	Core — Theory Only

2. Course Details

THEORY-ONLY COURSE — All 6 COs (CO1–CO6) are assessed exclusively via Continuous Assessment (CA), MTE, and ETE. No laboratory component.

S.No	Attribute	Details
1	**Course Code**	**CSCF4204**

2	**Course Title**	**Digital Watermarking & Steganography**
3	**Credits**	3
4	**Contact Hours (L-T-P-SL)**	3-0-0-3 (Theory: 45 hrs Classroom + 45 hrs Self Learning = 90 hrs total)
5	**Course Status**	**Elective — Theory Only (No Laboratory Component)**
6	**Course Objectives**	7. Understand information hiding techniques including digital watermarking and steganography, 8. Explore transform domain methods and secure embedding techniques, analyze security, robustness, and perceptual models, 9. Evaluate watermarking systems and attacks, and develop secure data hiding mechanisms.
7	**Course Outcomes (COs)**	**After successful completion of this course, students will be able to:** CO1 (Remember– L1) Define watermarking models, message coding, and information hiding concepts CO2 (Understand – L2) Explain watermark security, authentication, and communication models CO3 (Apply– L3) Apply steganography techniques and perceptual models CO4 (Analyze – L4) Analyze watermarking techniques for different media objects CO5 (Evaluate – L5) Evaluate watermarking protocols and performance metrics CO6 (Create – L6) Design secure watermarking and steganographic systems against attacks
8	**Course Description**	This course introduces digital watermarking and steganography techniques for secure information hiding. It covers watermarking models, perceptual models, security mechanisms, and real-world applications across multimedia systems. Emphasis is placed on robustness, security, and evaluation of watermarking systems along with protection against attacks.
9	**Teaching & Learning Scheme**	Classroom Instructions (CI): 45 hrs | Self Learning (SL): 45 hrs | Total: 90 hrs
10	**Mode of Examination**	**Theory Only. CA: 25% | MTE: 15% | ETE: 60% | Total: 100 marks**

11	**Textbook**	Textbook: 1. Digital Watermarking and Steganography – Ingemar J. Cox 2. Digital Watermarking – Cox et al.
12	**References**	Other References: 1. Techniques and Applications of Digital Watermarking – Arnold 2. Disappearing Cryptography – Peter Wayner

3. Outline Syllabus with CO Mapping

All CO mappings in this section refer to Theory COs (CO1–CO6). This is a theory-only course; all assessment is via CA, MTE, and ETE.

	Topic	CO Mapping
	Unit 1: Introduction to Information Hiding	
A	A Information Hiding, Steganography, Watermarking Concepts	CO1, CO2
B	Watermarking Models and Communication-based Models	CO1, CO2
C	Message Coding, Error Correction, Multi-symbol Detection	CO2, CO3
	Unit 2: Watermarking Techniques	
A	A Watermarking with Side Information	CO3, CO4
B	Coding Techniques and Structured Codes	CO3, CO4
C	Error Analysis (False Positives/Negatives, ROC Curves)	CO4, CO5
	Unit 3: Perceptual Models & Robust Techniques	
A	Perceptual Models and Evaluation	CO3, CO4
B	Robust Watermarking Approaches	CO4, CO5
C	Spread Spectrum and Coefficient Embedding	CO3, CO4, CO5
	Unit 4: Security & Authentication	
A	Watermark Security Requirements	CO2, CO5

B	Cryptography and Attacks on Watermarking	CO4, CO5, CO6
C	Authentication Techniques (Selective, Localization)	CO2, CO4, CO5
	Unit 5: Steganography & Applications	
A	A Steganography Communication & Terminology	CO1, CO2, CO3
B	Information-Theoretic Foundations & Practical Methods	CO3, CO4, CO5
C	Steganalysis and Minimizing Embedding Impact	CO4, CO5, CO6

4. Topic-wise Bloom's Taxonomy Level Mapping

S.No	Topic	L1 Remember	L2 Understand	L3 Apply	L4 Analyze	L5 Evaluate	L6 Create
1	1.A	✓	✓				
2	1.B	✓	✓				
3	1.C		✓	✓			
4	2.A			✓	✓		
5	2.B			✓	✓		
6	2.C				✓	✓	
7	3.A			✓	✓		
8	3.B				✓	✓	
9	3.C			✓	✓	✓	
10	4.A		✓			✓	
11	4.B				✓	✓	✓
12	4.C		✓		✓	✓	✓
13	5.A	✓	✓	✓			

14	5.B			✓	✓	✓	
15	5.C				✓	✓	✓

5. CO vs Bloom's Taxonomy — All Three Domains

Only strong/dominant alignments are mapped. This is a theory-only course; Psychomotor mapping is limited to Guided Response (P3) for algorithm implementation in CO3. Affective domain appears at A3 (Valuing) for efficiency analysis in CO4 and CO5.

CO	Cognitive Domain (L1–L6)						Affective (A1–A5)					Psychomotor (P1–P7)						
CO	L1	L2	L3	L4	L5	L6	A1	A2	A3	A4	A5	P1	P2	P3	P4	P5	P6	P7
CO1	✓						✓					✓						
CO2		✓					✓	✓					✓	✓				
CO3			✓					✓	✓					✓	✓			
CO4				✓					✓	✓					✓	✓		
CO5					✓				✓	✓						✓	✓	
CO6						✓				✓	✓					✓	✓	✓

Legend: ✓ = Strong / Dominant mapping. Theory-only course: Cognitive domain is primary. Psychomotor (P3) limited to CO3 (algorithm implementation). Affective (A3) for CO4 and CO5 (valuing efficiency).

6. Lecture Plan Outline (Theory — 45 Lectures / 45 Hours)

Total classroom contact: 45 hours across 5 units. Self-Learning activities (45 hrs) are structured separately in Section 11.

1	DD/MM/YY	Introduction to Information Hiding & Watermarking	UNIT-1	9
2	DD/MM/YY	History and Evolution of Watermarking		
3	DD/MM/YY	Importance and Applications of Watermarking		
4	DD/MM/YY	Watermarking Communication Models		

5	DD/MM/YY	Watermarking System Components		
6	DD/MM/YY	Watermarking Models and Architectures		
7	DD/MM/YY	Message Coding Techniques		
8	DD/MM/YY	Error Correction Techniques		
9	DD/MM/YY	Numerical Problems and Unit Review		
10	DD/MM/YY	Fundamentals of Watermarking Techniques	UNIT-2	9
11	DD/MM/YY	Spatial Domain Watermarking		
12	DD/MM/YY	Frequency Domain Watermarking		
13	DD/MM/YY	Watermarking with Side Information		
14	DD/MM/YY	Informed Coding Techniques		
15	DD/MM/YY	Structured Codes in Watermarking		
16	DD/MM/YY	Error Types: False Positive and False Negative		
17	DD/MM/YY	ROC Curves and Performance Analysis		
18	DD/MM/YY	Effect of Whitening on Error Rates		
19	DD/MM/YY	Introduction to Perceptual Models	UNIT-3	9
20	DD/MM/YY	General Perceptual Model Framework		
21	DD/MM/YY	Human Visual System and Perceptual Analysis		
22	DD/MM/YY	Examples of Perceptual Models		
23	DD/MM/YY	Robust Watermarking Approaches		
24	DD/MM/YY	Redundant Embedding Techniques		
25	DD/MM/YY	Spread Spectrum Coding		
26	DD/MM/YY	Embedding in Perceptual Coefficients		
27	DD/MM/YY	Case Study and Review of Perceptual Models		
28	DD/MM/YY	Introduction to Watermark Security	UNIT-4	9
29	DD/MM/YY	Security Requirements in Watermarking		
30	DD/MM/YY	Threat Models and Security Challenges		
31	DD/MM/YY	Cryptographic Techniques in Watermarking		
32	DD/MM/YY	Encryption and Key Management		
33	DD/MM/YY	Attacks on Watermarking Systems		
34	DD/MM/YY	Authentication Techniques		
35	DD/MM/YY	Localization and Restoration Methods		
36	DD/MM/YY	Unit Review and Practice Problems		
37	DD/MM/YY	Introduction to Steganography	UNIT-5	9
38	DD/MM/YY	Steganography Communication Models		
39	DD/MM/YY	Information-Theoretic Foundations		
40	DD/MM/YY	Image and Audio Steganography Techniques		
41	DD/MM/YY	Practical Steganographic Techniques		
42	DD/MM/YY	Minimizing Embedding Impact		
43	DD/MM/YY	Steganalysis Techniques		
44	DD/MM/YY	Comparative Study of Watermarking and Steganography		
45	DD/MM/YY	Final Review, Case Studies and Discussion		

PART II

THEORY ASSESSMENT FRAMEWORK

Theory Skill Dimensions, CO × TS Mapping, CA / MTE / ETE Structure

7. Theory Skill Dimensions (TS1–TS6)

THEORY-ONLY COURSE — All 6 COs (CO1–CO6) are assessed exclusively via Continuous Assessment (CA), MTE, and ETE. No laboratory component.

Six Theory Skill Dimensions — one per Bloom's progression (L1–L4) — correspond directly to the six COs. They define precisely what competency is being measured in each section of the CA, MTE, and ETE, providing a clear NBA-auditable assessment rationale.

ID	Dimension	What is Measured	CO / BTL	Assessment
TS1	Conceptual Recall & Information Hiding Fundamentals	Recall watermarking terminology, steganography concepts, communication models, message coding, and multimedia security fundamentals; identify watermarking and information hiding techniques	CO1 | L1–L2	CA | MTE Sec A | ETE Sec A
TS2	Conceptual Explanation & Watermarking Interpretation	Explain watermarking models, authentication methods, communication-based models, coding schemes, and perceptual models; interpret multimedia information hiding workflows	CO2 | L2–L3	CA | MTE Sec A | ETE Sec A
TS3	Steganography & Watermarking Application	Apply steganography methods, perceptual models, spread spectrum techniques, and coefficient embedding approaches for multimedia security applications	CO3 | L3	CA | MTE Sec B | ETE Sec B
TS4	Watermarking Analysis & Media Evaluation	Analyze watermarking techniques for text, image, audio, and video media; evaluate robustness, embedding efficiency, distortion, and attack resistance	CO4 | L4–L5	MTE Sec B | ETE Sec B
TS5	Security Protocol & Performance Evaluation	Compare watermarking protocols, authentication schemes, ROC analysis, cryptographic protection, and steganalysis methods; evaluate security and performance metrics	CO5 | L4–L5	ETE Sec B/C
TS6	Secure Watermarking & Steganographic System Design	Design secure watermarking and steganographic systems resistant to attacks, embedding distortions, and unauthorized extraction for real-world multimedia applications	CO6 | L5–L6	ETE Sec C

8. CO × Theory Skill Dimension Mapping (6 COs × 6 Dimensions)

Each CO maps primarily to one TS dimension (H) with adjacent dimensions receiving secondary mapping (M), reflecting the progressive Bloom's structure of this course.

CO	TS1 Information Hiding Fundamentals & Watermarking Concepts	TS2 Watermarking Models & Communication Interpretation	TS3 Steganography & Embedding Application	TS4 Watermarking Analysis & Media Evaluation	TS5 Security Protocols & Performance Evaluation	TS6 Secure Watermarking & Steganographic System Design
CO 1	H	M	-	M	H	-
CO 2	H	H	-	M	H	M
CO 3	H	H	M	-	H	M
CO 4	H	-	-	H	H	M
CO 5	-	M	-	-	H	M
CO 6	-	M	-	M	H	M

H = High / Primary alignment M = Medium / Secondary alignment Blank = No direct alignment

9. Continuous Assessment (CA) — 25 Marks

CA is formative and covers COs progressively as the syllabus is taught. It includes numerical-based assignments, a technical video learning report, and a real-world case study — mirroring TS1 through TS6.

9.1 CA Component Breakdown (Sample)

Component	Quantum	Marks	COs Assessed	Skill Dimensions
Assignments 1–5 (Watermarking, Steganography, Embedding Techniques & Security Analysis Problems)	5 Assignments	15	CO1, CO2, CO3, CO4	TS1, TS2, TS3, TS4
Technical Tool Demonstration / Video Learning Report	1 Report + Presentation	5	CO2, CO3, CO5	TS2, TS3, TS5
Real-World Watermarking & Steganography Security Case Study (Report)	1 Report	5	CO4, CO5, CO6	TS4, TS5, TS6
TOTAL	—	**25**	**CO1–CO6**	**TS1–TS6**

9.2 Assignment-wise CO & TS Mapping

Item	Topic / Focus	COs	TS Dims	SL Hours	Evaluation Criteria
Assignment 1	Unit 1 concepts: Information hiding overview, watermarking models, steganography basics, communication-based models	CO1, CO2	TS1, TS2	5h SL	Conceptual understanding, terminology accuracy, report submission
Assignment 2	Message coding, error correction, structured codes, and watermark embedding techniques	CO2, CO3	TS2, TS3	5h SL	Coding implementation, workflow explanation, embedding accuracy
Assignment 3	Perceptual models, spread spectrum techniques, coefficient embedding, and robust watermarking approaches	CO3, CO4	TS3, TS4	5h SL	Watermark analysis, practical implementation, robustness evaluation

Assignment 4	Watermark security, cryptographic protection, authentication techniques, and attack analysis	CO4, CO5	TS4, TS5	5h SL	Comparative analysis, security evaluation, protocol assessment
Assignment 5	Advanced steganography, steganalysis, secure watermarking system design, and attack-resistant embedding methods	CO5, CO6	TS5, TS6	5h SL	Secure system design proposal, embedding methodology, technical justification
Video Learning Report	Technical video on watermarking, steganography, multimedia security, authentication techniques, or steganalysis methods (min 3 hrs); structured report + presentation	CO2, CO3, CO5	TS2, TS3, TS5	9h SL	Learning outcomes, technical understanding, self-reflection, 10-minute presentation
Case Study Report	Real-world watermarking and steganography case study (e.g., copyright protection, multimedia authentication, covert communication, digital media attacks)	CO4, CO5, CO6	TS4, TS5, TS6	6h SL	Technical depth, attack analysis, comparative evaluation, security and defense recommendations

10. Mid Term Examination (MTE) — 15 Marks (Units 1–3)

MTE covers Units 1–3 (CO1, CO2, CO3, CO4). CO5 and CO6 are assessed in ETE only. MTE maps to TS1–TS4.

Section	Marks	Theory Skill Dimensions	COs Assessed	Question Type & Guidance
Section A	10	TS1 — Information Hiding Fundamentals & Watermarking Concepts TS2 — Watermarking Models & Communication Interpretation	CO1, CO2	Short-answer questions: define information hiding concepts, explain watermarking and steganography terminology, describe communication-based models, explain message coding, authentication methods, perceptual models, and multimedia security workflows
Section B	15	TS3 — Steganography & Embedding Application TS4 —	CO2, CO3, CO4	Analytical and application-based questions: watermark embedding analysis, spread spectrum

		Watermarking Analysis & Media Evaluation		techniques, coefficient embedding, perceptual model interpretation, robustness evaluation, steganographic implementation, attack analysis, and multimedia watermarking case studies
TOTAL	**25**	**TS1–TS4**	**CO1–CO4**	Units 1–3 only. CO5 and CO6 assessed in ETE only.

11. End Term Examination (ETE) — 60 Marks (All Units, All COs)

ETE is comprehensive — all 5 units and all 6 COs. Full progression from TS1 (recall) through TS6 (evaluation). Minimum 20/50 required to pass.

Section	Marks	Theory Skill Dimensions	COs Assessed	Question Type & Guidance
Section A	15	TS1 — Information Hiding Fundamentals & Watermarking Concepts TS2 — Watermarking Models & Communication Interpretation	CO1, CO2	Short questions (all units): definitions of watermarking and steganography concepts, communication-based models, message coding, authentication terminology, multimedia security concepts, perceptual models, and information hiding techniques
Section B	25	TS3 — Steganography & Embedding Application TS4 — Watermarking Analysis & Media Evaluation TS5 — Security Protocols & Performance Evaluation	CO3, CO4, CO5	Medium questions: watermark embedding analysis, spread spectrum methods, coefficient embedding, perceptual evaluation, ROC curve analysis, robustness testing, cryptographic protection, authentication mechanisms, and steganalysis comparisons
Section C	10	TS5 — Security Protocols & Performance Evaluation TS6 — Secure Watermarking & Steganographic System Design	CO5, CO6	Long/evaluation questions: secure watermarking system design, attack-resistant steganographic methods, authentication framework analysis, multimedia copyright protection, steganalysis resistance, and real-world digital media security case studies
TOTAL	**50**	**TS1–TS6 (all)**	**CO1–CO6**	Scaled from 100-mark paper if needed. Minimum 20/50 to pass.

11.1 CO-wise Assessment Instrument Summary

CO	CO Statement (Short)	CA (25)	MTE (25)	ETE (50)	TS	PO Primary
CO1	Understand watermarking models, message coding, and information hiding fundamentals	✓	✓	✓	TS1	PO1, PO2, PO3, PO4
CO2	Explain watermark security, authentication, and communication-based models	✓	✓	✓	TS2	PO1, PO2, PO3, PO5
CO3	Apply steganography techniques, perceptual models, and embedding methods	✓	✓	✓	TS3	PO1, PO2, PO3, PO5
CO4	Analyze watermarking techniques for image, audio, video, and multimedia objects	✓	✓	✓	TS4	PO2, PO3, PO4, PO10
CO5	Evaluate watermarking protocols, authentication methods, and performance metrics	✓	—	✓	TS5	PO1, PO2, PO8, PO10, PO11
CO6	Design secure watermarking and steganographic systems resistant to attacks and distortions	✓	—	✓	TS6	PO3, PO4, PO5, PO10, PO11, PO12

CO5 and CO6 are NOT assessed in MTE (only Units 1–3 are covered at mid-semester). They are assessed in CA (self-learning activities) and ETE.

PART III

COMBINED MAPPINGS & REFERENCE

CO–PO Matrix, CO–PO Alignment, Self-Learning Activities, Bloom's Reference, Attendance & Pass/Fail

12. CO–PO and CO–PSO Mapping Matrix (Original Framework)

Strength Scale: 3 = Substantial (High) | 2 = Moderate | 1 = Slight (Low) | – = Not Applicable. Averages computed over non-zero entries only. PO framework as per the original course design.

CO	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PSO1	PSO2	PSO3
CO1	3	2	-	2	3	-	-	-	-	-	2	3	2	-
CO2	3	3	-	2	3	2	-	-	-	-	2	3	3	-
CO3	3	3	2	-	3	2	-	-	-	-	2	3	3	2
CO4	3	-	-	3	3	2	-	-	-	-	2	3	3	2
CO5	-	2	-	-	3	2	-	-	2	2	2	-	3	2
CO6	-	2	-	2	3	2	-	-	-	2	2	-	3	2
Avg	3	2.4	2	2.25	3	2	-	-	2	2	2	3	2.83	2

13. CO × PO Alignment Map (H/M Indicators — All 6 COs)

CO	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PSO1	PSO2	PSO3
CO1	H	M	-	M	H	-	-	-	-	-	M	H	M	-
CO2	H	H	-	M	H	M	-	-	-	-	M	H	H	-
CO3	H	H	M	-	H	M	-	-	-	-	M	H	H	M
CO4	H	-	-	H	H	M	-	-	-	-	M	H	H	M
CO5	-	M	-	-	H	M	-	-	M	M	M	-	H	M
CO6	-	M	-	M	H	M	-	-	-	M	M	-	H	M

14. Self-Learning Activities (SL: 45 Hours)

S.No	Activity	Hours	COs / TS	Evaluation Criteria
1	Assignment Writing (5 assignments based on watermarking models, steganography techniques, embedding methods, perceptual models, and multimedia security analysis)	5 assignments × 3 hrs each Total = 15 hrs	CO1–CO4 TS1–TS4	Evaluated based on assignment submission, watermark/steganography analysis accuracy, embedding methodology, protocol understanding, robustness evaluation, and analytical reasoning
2	Technical Video-Based Learning related to Digital Watermarking and Steganography (e.g., spread spectrum embedding, authentication techniques, steganalysis, multimedia copyright protection, watermark attacks)	Video viewing: 5hrs Report preparation: 5 hrs Presentation: 5 hrs Total = 15 hr	CO2, CO3, CO5 TS2, TS3, TS5	Report + Presentation based on learning outcomes; must include watermarking concepts, embedding techniques, security mechanisms, attack-defense strategies, and personal technical reflections
3	Real-World Watermarking & Steganography Case Studies (e.g., digital copyright protection, multimedia authentication, covert communication systems, watermark attack analysis, steganalysis techniques)	Data collection/study: 10 hrs Report preparation: 5 hrs Total = 15 hrs	CO4, CO5, CO6 TS4, TS5, TS6	Evaluated based on technical depth, multimedia security analysis, attack evaluation, robustness assessment, mitigation strategies, secure system design practices, and analytical conclusions
	TOTAL Self-Learning Hours	**45 hours**	**CO1–CO6**	All activities are compulsory. Submission deadlines communicated at the start of the semester.

15. Bloom's Taxonomy — Domain Level Reference

Cognitive Domain (6 Levels)	Affective Domain (5 Levels)	Psychomotor Domain — Simpson (7 Levels)
L1 — Remember: Recall facts, definitions, basic concepts	A1 — Receiving: Awareness and willingness to attend	P1 — Perception: Sensory cues guide motor activity

L2 — Understand: Explain ideas, concepts, and principles L3 — Apply: Use knowledge to solve problems in new situations L4 — Analyze: Break down information, examine relationships L5 — Evaluate: Judge, justify, assess, and make decisions L6 — Create: Design, develop, and produce new artefacts	A2 — Responding: Active participation and reaction A3 — Valuing: Commitment and assigning value to content A4 — Organizing: Integrating values into a personal system A5 — Characterizing: Internalized value system	P2 — Set: Mental, physical readiness to act P3 — Guided Response: Practice through imitation/trial P4 — Mechanism: Habitual correct performance P5 — Complex Overt Response: Skilled performance P6 — Adaptation: Modify skills for special situations P7 — Origination: Create new solution patterns

OBE Compliance Statement: This is a theory-only course. All 6 COs are mapped primarily to the Cognitive domain (L1–L5). Psychomotor domain (P3) appears only for CO3 (algorithm implementation as mental tracing). Affective domain (A3) appears for CO4 and CO5, reflecting valuing of algorithmic efficiency.

16. Attendance Policy & Pass / Fail Criteria

16.1 Attendance Policy

Component	Minimum	Applicable To	Consequence
Theory Classes	**75%**	All lecture sessions	Debarred from ETE if below threshold
Self-Learning / Assignment Submission	**All activities**	SL activities (30 hrs)	Incomplete SL affects CA score directly

Theory attendance must meet 75% minimum. Missing SL activities (assignments, video report, case study) directly impacts CA marks and is not compensable by exam performance.

16.2 Pass / Fail Criteria

Condition	Threshold	Status	Remarks
ETE Score	**≥ 24 / 60**	**MANDATORY**	40% of ETE paper required; failing ETE means failing the course regardless of CA + MTE
Overall Total (CA + MTE + ETE)	**≥ 40 / 100**	**Must pass overall**	CA 25 + MTE 25 + ETE 50 = 100; 40% overall minimum required

CSCF4204— MEASUREMENT ARCHITECTURE SUMMARY

Theory-Only Course | 6 COs (CO1–CO6) | 3 Assessment Instruments | 6 Theory Skill Dimensions (TS1–TS6)

CO1–CO2: Conceptual / Understand → TS1, TS2 → CA + MTE Sec A + ETE Sec A

CO3–CO4: Apply / Analyze → TS3, TS4 → CA + MTE Sec B + ETE Sec B

CO5–CO6: Analyze / Evaluate → TS5, TS6 → CA + ETE Sec B/C

CA 25 marks + MTE 25 marks + ETE 50 marks = Total 100 marks

COURSE PLAN

Information Security & Audit Monitoring (CSCF 4205)

Sharda School of Computing Science & Engineering | B.Tech CSE | Semester VIII | Batch 2026–2030

Theory-Only Course Plan — All 6 COs (CO1–CO6) | Theory Skill Dimensions TS1–TS6 | CA + MTE + ETE Assessment

PART I

COURSE SYLLABUS

Course Identification, Details, Outcomes, BTL Mapping & Lecture Plan

1. Course Identification

School:	SSCSE- Sharda School of Computing Science & Engineering	**Batch:**	2026 – 2030
Program:	B. Tech	**Current Academic Year:**	2029-30
Branch:	Cyber Security & Forensics	**Semester:**	VIII
Course Code:	**CSC4205**	**Course Type:**	Core — Theory Only/ Elective

2. Course Details

▧ **THEORY-ONLY COURSE — All 6 COs (CO1–CO6) are assessed exclusively via Continuous Assessment (CA), MTE, and ETE. No laboratory component.**

S.No	Attribute	Details
1	**Course Code**	**CSC052**
2	**Course Title**	**Information Security & Audit Monitoring**
3	**Credits**	3

4	**Contact Hours (L-T-P-SL)**	3-0-0-3 (Theory: 45 hrs. Classroom + 45 hrs. Self-Learning = 90 hrs. total)
5	**Course Status**	**Core — Theory Only (No Laboratory Component)**
6	**Course Objectives**	1. To provide knowledge of information security principles, auditing concepts, and monitoring frameworks. 2. To develop the ability to investigate and analyze information security risks, vulnerabilities, and compliance issues. 3. To familiarize students with security auditing tools, monitoring techniques, and forensic audit practices. 4. To enable students to apply audit and monitoring concepts for effective security management and cyber resilience.
7	**Course Outcomes (COs)**	**After successful completion of this course, students will be able to:** **CO1 (Apply/Analyze – L3/L4):** Identify security weaknesses in information systems and apply appropriate security mechanisms to mitigate them. **CO2 (Analyze – L4):** Analyze emerging computer security threats, attack trends, and corresponding defence mechanisms. **CO3 (Understand – L2):** Explain physical, logical, and operational security controls used in information systems protection. **CO4 (Analyze – L4):** Examine and assess the security posture of information systems through auditing and monitoring practices. **CO5 (Understand/Analyze – L2/L4):** Compare different types of computer viruses and their objectives in compromising information security. **CO6 (Evaluate – L5):** Evaluate various intrusion detection techniques and firewall design principles for securing organizational networks.
8	**Course Description**	This course aims to introduce students to the fundamental concepts and techniques in computer and network security, and giving students an overview of information security and auditing, and to expose students to the latest trend of computer attack and defense. Other advanced topics on information security such as mobile computing security, security and privacy of cloud computing, as well as secure information system development will also be discussed.
9	**Teaching & Learning Scheme**	Classroom Instructions (CI): 45 hrs. | Self Learning (SL): 45 hrs. | Total: 90 hrs.
10	**Mode of Examination**	**Theory Only. CA: 25% | MTE: 15% | ETE: 60% | Total: 100 marks**
11	**Textbook**	1. William Stallings and Lawrie Brown, *Computer Security: Principles and Practice*, Pearson, Latest Edition 2. Mike Chapple, David Seidl, James Michael Stewart, CISSP Official Study Guide, Wiley. *(Excellent for security controls, auditing, risk management, IDS/firewalls, governance)* 3. David Kim and Michael G. Solomon, *Fundamentals of Information Systems Security*, Jones & Bartlett
12	**References**	1. Chris Davis, Mike Schiller, Kevin Wheeler, *IT Auditing Using Controls to Protect Information Assets*, McGraw Hill. 2. ISO/IEC 27001:2013 Information Security Management Systems. *(Strong Compliance reference)*

		3. Nina Godbole & Sunit Belapure, *Cyber Security: Understanding Cyber Crimes, Computer Forensics and Legal Perspectives*, Wiley India

3. Outline Syllabus with CO Mapping

ℹ *All CO mappings in this section refer to Theory COs (CO1–CO6). This is a theory-only course; all assessment is via CA, MTE, and ETE.*

	Topic	CO Mapping
Unit 1	**Introduction to Information Security and IS Auditing**	
A	Objectives of Information Security, objectives of IS audit and control, security governance, risk management fundamentals	**CO1, CO3**
B	Structure of an IS audit, audit lifecycle, audit planning, evidence collection, audit documentation, audit reporting	**CO3, CO4**
C	IS auditing standards, compliance frameworks, ISO/IEC 27001 overview, computer-assisted audit tools (CAATs), security monitoring concepts	**CO3, CO4**
Unit 2	**Organizational Security and Security Controls**	
A	Physical security controls, contingency planning, disaster recovery, business continuity, environmental controls	**CO1, CO2, CO3**
B	Logical security controls: operating system security, access control mechanisms, authentication, segregation of duties, monitoring and logging controls	**CO1, CO3, CO4**
C	Personnel security practices, user awareness training, incident reporting, third-party/vendor security, software development controls, input-processing-output controls	**CO2, CO3, CO4**
Unit 3	**Cryptographic Foundations for Information Security**	
A	Symmetric and asymmetric encryption fundamentals, cryptographic applications in information security	**CO2, CO3**
B	Message authentication, cryptographic hash functions, integrity mechanisms, secure communication concepts	**CO2, CO3**
C	Digital signatures, digital certificates, Public Key Infrastructure (PKI), trust models, secure transaction mechanisms	**CO3, CO4**

Unit 4	**Network Security, Threats, and Defense Mechanisms**	
A	Network security fundamentals, authentication mechanisms, identity and access management, secure communication controls	**CO1, CO4**
B	Security threats and attack trends: malware, host-based attacks, network attacks, web application attacks, emerging cyber threats	**CO2, CO5**
C	Network defense mechanisms: intrusion detection systems, intrusion prevention systems, firewall design principles, IPSec, DNS Security, cloud security basics	**CO4, CO6**
Unit 5	**Security Auditing, Monitoring, and Digital Forensics**	
A	Information system security auditing, security assessment methodologies, audit controls, security standards and compliance frameworks	**CO4, CO5**
B	Security monitoring, incident handling, log analysis, SIEM concepts, computer forensic fundamentals	**CO4, CO5, CO6**
C	Advanced security technologies, threat intelligence, endpoint security, security analytics, forensic investigation support technologies	**CO5, CO6**

4. Topic-wise Bloom's Taxonomy Level Mapping

S.No	Topic	L1 Remember	L2 Understand	L3 Apply	L4 Analyze	L5 Evaluate	L6 Create
1	1.A	✓	✓		✓		
2	1.B		✓	✓	✓		✓
3	1.C	✓	✓		✓	✓	
4	2.A	✓	✓	✓			
5	2.B	✓	✓	✓	✓		
6	2.C		✓	✓	✓	✓	
7	3.A	✓	✓	✓			
8	3.B	✓	✓	✓	✓		

9	3.C		✓	✓	✓	✓	
10	4.A	✓	✓	✓			
11	4.B	✓	✓	✓	✓		
12	4.C	✓	✓	✓	✓	✓	
13	5.A	✓	✓		✓		✓
14	5.B		✓	✓	✓	✓	
15	5.C		✓	✓	✓	✓	✓

5. CO vs Bloom's Taxonomy — All Three Domains

ℹ *Only strong/dominant alignments are mapped. This is a theory-only course; Psychomotor mapping is limited to Guided Response (P3) for algorithm implementation in CO3. Affective domain appears at A3 (Valuing) for efficiency analysis in CO4 and CO5.*

CO	Cognitive Domain (L1–L6)						Affective (A1–A5)					Psychomotor (P1–P7)						
CO	L1	L2	L3	L4	L5	L6	A1	A2	A3	A4	A5	P1	P2	P3	P4	P5	P6	P7
CO1	✓	✓					✓											
CO2		✓	✓	✓				✓					✓	✓				
CO3		✓	✓	✓			✓						✓	✓				
CO4				✓	✓				✓									
CO5			✓	✓	✓	✓			✓					✓	✓			
CO6		✓	✓	✓	✓			✓					✓	✓				

Legend: ✓ = Strong / Dominant mapping. Theory-only course: Cognitive domain is primary. Psychomotor (P3) limited to CO3 (algorithm implementation). Affective (A3) for CO4 and CO5 (valuing efficiency).

6. Lecture Plan Outline (Theory — 45 Lectures / 45 Hours)

ℹ *Total classroom contact: 45 hours across 5 units. Self-Learning activities (45 hrs.) are structured separately in Section 11.*

Date	Topics to be Covered/Title	UNIT	Total Lectures
DD/MM/YYYY	Introduction to Information Security and Course Overview	Unit 1	9
DD/MM/YYYY	Objectives of Information Security and Security Governance		
DD/MM/YYYY	IS Audit Objectives and Risk Management Fundamentals		
DD/MM/YYYY	Audit Lifecycle: Planning and Scope Definition		
DD/MM/YYYY	Audit Evidence Collection and Documentation		
DD/MM/YYYY	Audit Reporting and Audit Communication		
DD/MM/YYYY	IS Auditing Standards and Compliance Frameworks		
DD/MM/YYYY	ISO/IEC 27001 and Governance Controls		
DD/MM/YYYY	Computer Assisted Audit Tools (CAATs) and Monitoring Concepts		
DD/MM/YYYY	Physical Security Controls and Environmental Protection	Unit 2	9
DD/MM/YYYY	Contingency Planning, Disaster Recovery, and BCM		
DD/MM/YYYY	Logical Security Controls and Access Control		
DD/MM/YYYY	Authentication and OS Security		
DD/MM/YYYY	Segregation of Duties and Monitoring Controls		
DD/MM/YYYY	Logging Controls and Audit Trails		
DD/MM/YYYY	Personnel Security and Security Awareness Training		
DD/MM/YYYY	Third-Party Security and Outsourcing Risks		
DD/MM/YYYY	Application Security Controls and Incident Reporting		
DD/MM/YYYY	Introduction to Cryptographic Technologies		

DD/MM/YYYY	Symmetric Encryption	Unit 3	9
DD/MM/YYYY	Asymmetric Encryption		
DD/MM/YYYY	Message Authentication		
DD/MM/YYYY	Cryptographic Hash Functions		
DD/MM/YYYY	Digital Signatures		
DD/MM/YYYY	Digital Certificates and PKI		
DD/MM/YYYY	Web of Trust and Secure Communication		
DD/MM/YYYY	Cryptographic Applications in Information Security		
DD/MM/YYYY	Network Security Fundamentals	Unit 4	9
DD/MM/YYYY	Authentication and Identity Management		
DD/MM/YYYY	Access Control in Networks		
DD/MM/YYYY	Malware and Host-Based Attacks		
DD/MM/YYYY	Network Attacks		
DD/MM/YYYY	Web-Based Attacks		
DD/MM/YYYY	Emerging Cyber Threats		
DD/MM/YYYY	IDS / IPS		
DD/MM/YYYY	Firewall Design, IPSec, DNS Security, Cloud Security		
DD/MM/YYYY	Information System Security Auditing	Unit 5	9
DD/MM/YYYY	Security Assessment Methodologies		
DD/MM/YYYY	Security Standards and Compliance		
DD/MM/YYYY	Security Monitoring and Log Analysis		
DD/MM/YYYY	SIEM and Incident Handling		
DD/MM/YYYY	Computer Forensics Fundamentals		
DD/MM/YYYY	Threat Intelligence and Endpoint Security		
DD/MM/YYYY	Security Analytics and Advanced Technologies		
DD/MM/YYYY	Integrated Case Study / Revision		

PART II

THEORY ASSESSMENT FRAMEWORK

Theory Skill Dimensions, CO × TS Mapping, CA / MTE / ETE Structure

7. Theory Skill Dimensions (TS1–TS6)

THEORY-ONLY COURSE — All 6 COs (CO1–CO6) are assessed exclusively via Continuous Assessment (CA), MTE, and ETE. No laboratory component.

★ *Six Theory Skill Dimensions — one per Bloom's progression (L1–L4) — correspond directly to the six COs. They define precisely what competency is being measured in each section of the CA, MTE, and ETE, providing a clear NBA-auditable assessment rationale.*

ID	Dimension	What is Measured	CO / BTL	Assessment
TS1	**Conceptual Recall & Information Security Fundamentals**	Recall and explain core concepts of information security, IS auditing, governance, risk management, security principles, and audit standards	**CO1 / CO3 | L1–L2**	CA | MTE Sec A | ETE Sec A
TS2	**Threat Analysis & Security Control Interpretation**	Analyze emerging cyber threats, malware, attack patterns, and explain physical, logical, operational, and administrative security controls	**CO2 / CO3 | L2–L4**	CA | MTE Sec A | ETE Sec A
TS3	**Security Mechanism Application & Cryptographic Foundations**	Apply authentication mechanisms, access control models, cryptographic techniques, integrity mechanisms, and security implementation concepts	**CO1 / CO3 | L3**	CA | MTE Sec B | ETE Sec B
TS4	**Audit Monitoring & Security Assessment Analysis**	Examine information system security posture through audit methodologies, monitoring frameworks, logging analysis, compliance checks, and security assessment practices	**CO4 | L4–L5**	MTE Sec B | ETE Sec B
TS5	**Security Evaluation & Defense Mechanism Assessment**	Evaluate malware behavior, intrusion detection mechanisms, firewall architectures, security defense strategies, and network protection effectiveness	**CO5 / CO6 | L4–L5**	ETE Sec B/C
TS6	**Incident Response, Forensics & Advanced Security Monitoring**	Analyze incident handling processes, SIEM concepts, forensic investigation support, threat intelligence, endpoint monitoring, and advanced security analytics	**CO4 / CO6 | L3–L5**	ETE Sec C

8. CO × Theory Skill Dimension Mapping (6 COs × 6 Dimensions)

ℹ *Each CO maps primarily to one TS dimension (H) with adjacent dimensions receiving secondary mapping (M), reflecting the progressive Bloom's structure of this course.*

CO	TS1 Conceptual Recall	TS2 Process Interpretation	TS3 Algorithmic Application	TS4 Performance Evaluation	TS5 Memory System Analysis	TS6 File & Disk Evaluation
CO1	M	H	H	M		
CO2		H	M	M	M	
CO3	H	H	M			
CO4		M		H	M	M
CO5		H			H	
CO6		M	M	M	H	H

H = High / Primary alignment M = Medium / Secondary alignment *Blank = No direct alignment*

9. Continuous Assessment (CA) — 25 Marks

★ *CA is formative and covers COs progressively as the syllabus is taught. It includes numerical-based assignments, a technical video learning report, and a real-world case study — mirroring TS1 through TS6.*

9.1 CA Component Breakdown (Sample)

Component	Quantum	Marks	COs Assessed	Skill Dimensions
Assignments 1–5 (Conceptual / Security Analysis / Audit-based Tasks)	5 Assignments	15	CO1, CO2, CO3, CO4	TS1, TS2, TS3, TS4
Technical Video Learning Report + Presentation	1 Report + Presentation	5	CO2, CO4, CO6	TS2, TS4, TS6
Real-World Security Audit / Incident Case Study Report	1 Report	5	CO4, CO5, CO6	TS4, TS5, TS6
TOTAL	—	25	CO1–CO6	TS1–TS6

9.2 Assignment-wise CO & TS Mapping

Item	Topic / Focus	COs	TS Dims	SL Hours	Evaluation Criteria
Assignment 1	Information security fundamentals, IS audit concepts, governance, audit standards, risk management basics	CO1, CO3	TS1	5 hrs.	Conceptual clarity, audit terminology understanding, governance interpretation, security weakness identification
Assignment 2	Security threats, malware analysis, physical/logical/operational security controls, access control mechanisms	CO2, CO3	TS2	5 hrs.	Threat analysis, control interpretation, comparative analysis of security controls
Assignment 3	Cryptographic technologies, authentication mechanisms, access control implementation, integrity mechanisms	CO1, CO3	TS3	5 hrs.	Application of security mechanisms, cryptographic understanding, authentication implementation logic
Assignment 4	IS audit process, monitoring frameworks, logging analysis, audit assessment methodologies, compliance evaluation	CO4	TS4	5 hrs.	Audit assessment quality, log interpretation, analytical reasoning, compliance analysis
Assignment 5	Malware comparison, IDS/firewall evaluation, network defense analysis, security monitoring case scenarios	CO5, CO6	TS5, TS6	5 hrs.	Threat evaluation, defense mechanism comparison, incident response reasoning, technical recommendations

Video Learning Report	Video on SIEM, cyber threat monitoring, security auditing, IDS/firewall operation, forensic investigation (minimum 3 hrs)	CO2, CO4, CO6	TS2, TS4, TS6	9 hrs.	Report on learning outcomes, threat interpretation, audit/monitoring understanding, self-reflection; Presentation (10 min)
Case Study Report	Case study on cyber breach, malware incident, audit failure, intrusion detection event, forensic analysis	CO4, CO5, CO6	TS4, TS5, TS6	11 hrs.	Technical depth, factual analysis, security assessment, threat evaluation, incident handling recommendations

10. Mid Term Examination (MTE) — 15 Marks (Units 1–3)

ℹ *MTE covers Units 1–3 (CO1, CO2, CO3, CO4). CO5 and CO6 are assessed in ETE only. MTE maps to TS1–TS4.*

Section	Marks	Theory Skill Dimensions	COs Assessed	Question Type & Guidance
Section A	**10**	TS1 — Information Security Fundamentals TS2 — Threat Analysis & Security Control Interpretation	CO1, CO2, CO3	Short-answer questions: information security concepts, IS audit fundamentals, governance, security controls, malware concepts, threat analysis, audit standards, access control principles
Section B	**15**	TS3 — Security Mechanism Application & Cryptography TS4 — Audit Monitoring & Security Assessment Analysis	CO1, CO3, CO4	Analytical/application questions: cryptographic applications, authentication mechanisms, audit lifecycle, audit assessment scenarios, logging analysis, compliance evaluation, monitoring case-based questions
TOTAL	**25**	**TS1–TS4**	**CO1–CO4**	**Units 1–3 only. CO5 and CO6 assessed in ETE only.**

11. End Term Examination (ETE) — 60 Marks (All Units, All COs)

ℹ *ETE is comprehensive — all 5 units and all 6 COs. Full progression from TS1 (recall) through TS6 (evaluation). Minimum 20/50 required to pass.*

Section	Marks	Theory Skill Dimensions	COs Assessed	Question Type & Guidance
Section A	15	TS1 — Information Security Fundamentals TS2 — Threat Analysis & Security Control Interpretation	CO1, CO2, CO3	Short questions (all units): definitions, audit concepts, security controls, malware, access control, cryptography basics, standards, governance concepts
Section B	25	TS3 — Security Mechanism Application & Cryptography TS4 — Audit Monitoring & Security Assessment Analysis TS5 — Security Evaluation & Defense Mechanisms	CO3, CO4, CO5, CO6	Medium analytical questions: cryptographic applications, audit case analysis, security assessment, malware comparison, IDS/firewall evaluation, attack-defense analysis
Section C	10	TS5 — Security Evaluation & Defense Mechanisms TS6 — Incident Response, Forensics & Advanced Monitoring	CO5, CO6	Long/evaluation questions: IDS/firewall design evaluation, SIEM/monitoring case analysis, forensic incident investigation, advanced defense strategies, security incident response
TOTAL	50	TS1–TS6 (all)	CO1–CO6	Scaled from 100-mark paper if needed. Minimum 20/50 to pass.

11.1 CO-wise Assessment Instrument Summary

CO	CO Statement (Short)	CA (25)	MTE (25)	ETE (50)	TS	PO Primary
CO1	Identify security weaknesses in information systems and apply appropriate security mechanisms	✓	✓	✓	TS1 / TS3	PO1, PO2, PO3, PO5
CO2	Analyze emerging computer security threats and defense mechanisms	✓	✓	✓	TS2	PO1, PO2, PO4
CO3	Explain physical, logical, and operational security controls	✓	✓	✓	TS1 / TS2 / TS3	PO1, PO2, PO5
CO4	Examine and assess the security of information systems through auditing and monitoring	✓	✓	✓	TS4 / TS6	PO2, PO4, PO5
CO5	Compare types and objectives of viruses and security threats	✓	—	✓	TS5	PO2, PO4

CO6	Evaluate intrusion detection techniques and firewall design principles	✓	—	✓	TS5 / TS6	PO4, PO5, PSO3

⚠ *CO5 and CO6 are NOT assessed in MTE (only Units 1–3 are covered at mid-semester). They are assessed in CA (self-learning activities) and ETE.*

PART III

COMBINED MAPPINGS & REFERENCE

CO–PO Matrix, CO–PO Alignment, Self-Learning Activities, Bloom's Reference, Attendance & Pass/Fail

12. CO–PO and CO–PSO Mapping Matrix (Original Framework)

ℹ *Strength Scale: 3 = Substantial (High) | 2 = Moderate | 1 = Slight (Low) | — = Not Applicable. Averages computed over non-zero entries only. PO framework as per the original course design.*

CO	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PSO1	PSO2	PSO3
CO1	3	-	-	-	-	2	-	-	-	-	3	3	3	-
CO2	2	-	-	-	3	2	-	2	-	-	3	3	3	-
CO3	3	3	3	-	3	2	-	-	-	-	2	2	3	-
CO4	3	3	3	3	-	2	2	3	-	-	2	-	-	3
CO5	2	3	2	-	2	2	2	-	-	-	1	-	3	-
CO6	3	3	3	3	3	3	3	3	3	2	3	-	-	3
Avg	**2.67**	**3.00**	**2.75**	**3.00**	**2.75**	**2.17**	**2.33**	**2.67**	**3.00**	**2.00**	**2.33**	**2.67**	**3.00**	**3.00**

13. CO × PO Alignment Map (H/M Indicators — All 6 COs)

CO	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PSO1	PSO2	PSO3
CO1	H					M					H	H	H	
CO2	M				H	M		M			H	H	H	
CO3	H	H	H		H	M					M	M	H	
CO4	H	H	H	H		M	M	H			M			H

CO5	M	H	M		M	M	M						H	
CO6	H	H	H	H	H	H	H	H	H	M	H			H

= High / Primary alignment **M** = Medium / Secondary alignment *Blank = No direct alignment*

14. Self-Learning Activities (SL: 45 Hours)

S.No	Activity	Hours	COs / TS	Evaluation Criteria
1	Assignment Writing (5 assignments covering information security fundamentals, audit controls, cryptographic security, network defense, audit monitoring & security assessment)	5 assignments × 5 hrs. each Total = 25 hrs.	CO1–CO6 TS1–TS6	Evaluated based on conceptual understanding, threat analysis, security mechanism application, audit assessment quality, technical correctness, analytical reasoning, and solution recommendations
2	Technical Video-Based Learning related to Information Security Audit & Monitoring (e.g., IS audit practices, SIEM demonstrations, cyber threat monitoring, IDS/firewall analysis, forensic investigations)	Video viewing: 3 hrs. Report preparation: 3 hrs. Presentation: 3 hrs. Total = 9 hrs.	CO2, CO4, CO6 TS2, TS4, TS6	Report + presentation based on learning outcomes, threat understanding, audit monitoring insights, security assessment observations, technical interpretation, and self-reflection
3	Real-World Security Audit / Incident Case Study Analysis (e.g., ransomware attack audit review, SIEM case study, firewall breach, malware outbreak analysis, forensic investigation case)	Data collection / study: 4 hrs. Report preparation: 4 hrs. Presentation / discussion: 3 hrs. Total = 11 hrs.	CO4, CO5, CO6 TS4, TS5, TS6	Evaluated based on technical depth, factual investigation, security audit interpretation, defense mechanism evaluation, forensic reasoning, and mitigation recommendations
	TOTAL Self-Learning Hours	45 Hours	CO1–CO6	All activities are compulsory. Submission deadlines communicated at the start of the semester.

15. Bloom's Taxonomy — Domain Level Reference

Cognitive Domain (6 Levels)	Affective Domain (5 Levels)	Psychomotor Domain — Simpson (7 Levels)
L1 — Remember: Recall facts, definitions, basic concepts L2 — Understand: Explain ideas, concepts, and principles	A1 — Receiving: Awareness and willingness to attend A2 — Responding: Active participation and reaction	P1 — Perception: Sensory cues guide motor activity P2 — Set: Mental, physical readiness to act

L3 — Apply: Use knowledge to solve problems in new situations L4 — Analyze: Break down information, examine relationships L5 — Evaluate: Judge, justify, assess, and make decisions L6 — Create: Design, develop, and produce new artefacts	A3 — Valuing: Commitment and assigning value to content A4 — Organizing: Integrating values into a personal system A5 — Characterizing: Internalized value system	P3 — Guided Response: Practice through imitation/trial P4 — Mechanism: Habitual correct performance P5 — Complex Overt Response: Skilled performance P6 — Adaptation: Modify skills for special situations P7 — Origination: Create new solution patterns

★ *OBE Compliance Statement: This is a theory-only course. All 6 COs are mapped primarily to the Cognitive domain (L1–L5). Psychomotor domain (P3) appears only for CO3 (algorithm implementation as mental tracing). Affective domain (A3) appears for CO4 and CO5, reflecting valuing of algorithmic efficiency.*

16. Attendance Policy & Pass / Fail Criteria

16.1 Attendance Policy

Component	Minimum	Applicable To	Consequence
Theory Classes	**75%**	All lecture sessions	Debarred from ETE if below threshold
Self-Learning / Assignment Submission	**All activities**	SL activities (45 hrs.)	Incomplete SL affects CA score directly

⚠ *Theory attendance must meet 75% minimum. Missing SL activities (assignments, video report, case study) directly impacts CA marks and is not compensable by exam performance.*

16.2 Pass / Fail Criteria

Condition	Threshold	Status	Remarks
ETE Score	**≥ 24 / 60**	**MANDATORY**	40% of ETE paper required; failing ETE means failing the course regardless of CA + MTE

Overall Total (CA + MTE + ETE)	**≥ 40 / 100**	**Must pass overall**	CA 25 + MTE 25 + ETE 50 = 100; 40% overall minimum required

CSCF4205— MEASUREMENT ARCHITECTURE SUMMARY

Theory-Only Course | 6 COs (CO1–CO6) | 3 Assessment Instruments | 6 Theory Skill Dimensions (TS1–TS6)

CO1–CO2: Conceptual / Understand → TS1, TS2 → CA + MTE Sec A + ETE Sec A

CO3–CO4: Apply / Analyze → TS3, TS4 → CA + MTE Sec B + ETE Sec B

CO5–CO6: Analyze / Evaluate → TS5, TS6 → CA + ETE Sec B/C

CA 25 marks + MTE 25 marks + ETE 50 marks = Total 100 marks