	Introduction to Cyber Forensics		Semester	7
	Course Code	**BCY714A**	CIE Marks	50
	Teaching Hours/Week (L: T:P: S)	3:0:0:0	SEE Marks	50
	Total Hours of Pedagogy	40	Total Marks	100
	Credits	03	Exam Hours	03
	Examination type (SEE)	Theory		

Course objectives:

- Understand the principles and processes of cyber forensics and the role of digital evidence in investigations.
- Gain expertise in operating system forensics, including Windows, Linux, and Mac OS.
- Explore specialized forensic domains like mobile devices, cloud environments, and malware.
- Investigate forensic techniques for web attacks, emails, and solid-state devices.
- Learn legal and technical aspects of cyber forensics, including Bitcoin forensics and report preparation.

Teaching-Learning Process (General Instructions)

These are sample strategies; which teachers can use to accelerate the attainment of the various course outcomes.

1. Lecturer method (L) does not mean only the traditional lecture method, but different types of teaching methods may be adopted to achieve the outcomes.
2. Utilize video/animation films to illustrate the functioning of various concepts.
3. Promote collaborative learning (Group Learning) in the class.
4. Pose at least three HOT (Higher Order Thinking) questions in the class to stimulate critical thinking.
5. Incorporate Problem-Based Learning (PBL) to foster students' analytical skills and develop their ability to evaluate, generalize, and analyze information rather than merely recalling it.
6. Introduce topics through multiple representations.
7. Demonstrate various ways to solve the same problem and encourage students to devise their own creative solutions.
8. Discuss the real-world applications of every concept to enhance students' comprehension.
9. Use any of these methods: Chalk and board, Active Learning, Case Studies.

Module-1 8 Hours

Foundations of Cyber Forensics

Introduction to Cyber Forensics: Overview of cyber forensics principles and processes; Understanding the role of digital evidence in investigations.
Windows Forensics: Analysis of Windows operating systems; Examining system logs, registry files, and memory dumps.
Linux Forensics: Investigating Linux systems; Log analysis, file system structures, and identifying forensic artifacts.

Module-2 8 Hours

Advanced Operating System Forensics

Mac OS Forensics: Mac OS file systems and log analysis; Extracting artifacts and understanding unique challenges in Mac environments.
Anti-forensics: Techniques used by attackers to cover their tracks; Methods to detect and counter anti-forensic measures.
Network Forensics: Monitoring and analyzing network traffic for forensic evidence; Understanding packet captures, network logs, and intrusion detection systems.

Module-3 8 Hours

Specialized Forensics Domains

Mobile Forensics: Techniques for extracting data from mobile devices; Investigating Android, iOS, and other mobile platforms.
Cloud Forensics: Challenges in collecting evidence from cloud environments; Legal and technical considerations in cloud investigations.
Malware Forensics: Analyzing malware samples to understand their behavior; Identifying and mitigating malware in forensic investigations.

Module-4 8 Hours

Focused Attack and Device Forensics

Web Attack Forensics: Investigating web-based attacks, including SQL injection and cross site scripting; Identifying server logs and tracing attack vectors.
Emails and Email Crime: Tracing email headers and identifying email-based attacks; Investigating phishing and fraud cases.
Solid State Device (SSD) Forensics: Understanding unique challenges in SSD forensics; Techniques for recovering and analyzing data from SSDs.

Module-5 8 Hours

Legal and Emerging Domains

Bitcoin Forensics: Tracking cryptocurrency transactions and wallets; Investigating blockchain based crimes.
Cyber Law and Cyberwarfare: Legal frameworks for handling digital evidence; Understanding international laws and cyberwarfare tactics.
Investigative Reports and Legal Acceptance: Preparing forensic reports for legal proceedings; Ensuring the admissibility of evidence in court.

Course outcome (Course Skill Set)

At the end of the course, the student will be able to:
1 Explain foundational concepts and processes in cyber forensics and digital evidence handling.
2 Analyze forensic artifacts across various operating systems and network environments.
3 Apply forensic methods to specialized domains like mobile devices, cloud environments, and malware analysis.

4 Investigate and trace evidence related to web attacks, email crimes, and SSDs.
5 Explain Bitcoin Forencisc

Assessment Details (both CIE and SEE)

The weightage of Continuous Internal Evaluation (CIE) is 50% and for Semester End Exam (SEE) is 50%. The minimum passing mark for the CIE is 40% of the maximum marks (20 marks out of 50) and for the SEE minimum passing mark is 35% of the maximum marks (18 out of 50 marks). A student shall be deemed to have satisfied the academic requirements and earned the credits allotted to each subject/ course if the student secures a minimum of 40% (40 marks out of 100) in the sum total of the CIE (Continuous Internal Evaluation) and SEE (Semester End Examination) taken together.

Continuous Internal Evaluation:

- For the Assignment component of the CIE, there are 25 marks and for the Internal Assessment Test component, there are 25 marks.
- The first test will be administered after 40-50% of the syllabus has been covered, and the second test will be administered after 85-90% of the syllabus has been covered
- Any two assignment methods mentioned in the 22OB2.4, if an assignment is project-based then only one assignment for the course shall be planned. The teacher should not conduct two assignments at the end of the semester if two assignments are planned.
- For the course, CIE marks will be based on a scaled-down sum of two tests and other methods of assessment.

Internal Assessment Test question paper is designed to attain the different levels of Bloom's taxonomy as per the outcome defined for the course.

Semester-End Examination:

Theory SEE will be conducted by University as per the scheduled timetable, with common question papers for the course (**duration 03 hours).**

1. The question paper will have ten questions. Each question is set for 20 marks.
2. There will be 2 questions from each module. Each of the two questions under a module (with a maximum of 3 sub-questions), **should have a mix of topics** under that module.
3. The students have to answer 5 full questions, selecting one full question from each module.
4. Marks scored shall be proportionally reduced to 50 marks

Suggested Learning Resources:

Text book

1. J. Doherty, Wireless and Mobile Device Security. Jones & Bartlett Learning, 2nd edition Dec. 2021.

Reference Books:

Reference book

1. M. S. Obaidat, A. Anpalagan, I. Woungang, and S. Misra, *Security and Privacy in Wireless and Mobile Networks*. MDPI, 2021.
2. M. Zinkus, T. M. Jois, and M. Green, "Data Security on Mobile Devices: Current State of the Art, Open Problems, and Proposed Solutions," *arXiv*, 2021. [Online]. Available: https://arxiv.org/abs/2105.12613
3. J. Stevenson, Mobile Offensive Security Pocket Guide: A Quick Reference Guide for Android and iOS. Independently Published, 2022.

Activity Based Learning (Suggested Activities in Class)/ Practical Based learning

1. Preparing legally admissible forensic reports and address challenges in cryptocurrency and cyber law (15 marks)
2. Assignment (10 marks)

	Software-Defined Networks		Semester	7
	Course Code	**BCM714B**	CIE Marks	50
	Teaching Hours/Week (L: T:P: S)	3:0:0:0	SEE Marks	50
	Total Hours of Pedagogy	40	Total Marks	100
	Credits	03	Exam Hours	03
	Examination type (SEE)	Theory		

Course objectives:

- To develop students' ability to understand the concepts of traditional networks with its limitations and the need to move to Software Defined Networks.
- To develop the students' ability to understand the fundamentals of SDN, its planar architecture and to understand the flexibility of multilevel pipeline processing.
- To provide the students with knowledge of the working of SDN between the controller and data plane and emphasis on the table matching.
- To create switches and designing networks by manually adding/deleting flow entries inside the table and learning to dissect the packets.
- To study industrial deployment use-cases of SDN

Teaching-Learning Process (General Instructions)

These are sample Strategies, which teachers can use to accelerate the attainment of the various course outcomes.

1. Use of power point presentation
2. Think -pair and share techniques
3. Workshop on Mininet Network Emulator
4. Usage of OpenFlow
5. Brief about the real-world applications of SDN from the published papers
6. Think-Pair Share, Group Discussions, Peer Tutoring

Module-1

Foundations of Software Defined Networking: Basic Packet-Switching Terminology, The Modern Data Center, Traditional Switch Architecture, Autonomous and Dynamic Forwarding Tables, Evolution of Switches and Control Planes, The Evolution of Networking Technology, Software Defined Networking is Born.

Textbook: Ch.1.1, 1.3, 1.4, 1.5, 2.1,3.1,3.3

Module-2

SDN Architecture and Protocols: Fundamental Characteristics of SDN, SDN Operation, SDN Devices, SDN Controller, SDN Applications, Alternate SDN Methods, OpenFlow

Textbook: Ch. 4.1-4.6, 5.2

Module-3

SDN Controllers and Programming: Potential Drawbacks of Open SDN, Data Center Demands, Tunneling Technologies for the Data Center, Path Technologies in the Data Center, Ethernet Fabrics in the Data Center, SDN in Wide Area Networks, SDN in Campus Networks, SDN in Hospitality Networks.

Textbook: Ch. 6.1, 7.2-7.5, 8.1, 8.3, 8.4

Module-4

SDN Applications and Real-World Use Cases: Reactive versus Proactive Applications, Analyzing Simple SDN Applications, A Simple Reactive Java Application, Using the Floodlight Controller, Creating Network Virtualization Tunnels, Traffic Engineering for Service Providers

Textbook: Ch. 10.2-10.4,10.6,10.11,10.14

	Module-5
	Challenges, Trends, and Advanced Topics: Open Source Licensing Issues, Profiles of SDN Open Source Users, OpenFlow Source Code, SDN Applications, Simulation, Testing, and Tools, OpenStack, Major SDN Acquisitions, SDN Startups. Textbook: Ch.11.2-11.4, 11.7, 11.9, 11.10, 12.8, 12.9

Course outcome (Course Skill Set)

At the end of the course, the student will be able to:

1. Explain the challenges and opportunities associated with adopting SDN compared to traditional approaches to networking.
2. Identify the functions of the data plane and control plane
3. Analyze the performance of routing, optimizing traffic engineering using SDN.
4. Demonstrate the operations of SDN network consisting of switches and a centralized controller through simulation.
5. Demonstrate the industrial deployment use-cases of SDN.

Assessment Details (both CIE and SEE)

The weightage of Continuous Internal Evaluation (CIE) is 50% and for Semester End Exam (SEE) is 50%. The minimum passing mark for the CIE is 40% of the maximum marks (20 marks out of 50) and for the SEE minimum passing mark is 35% of the maximum marks (18 out of 50 marks). A student shall be deemed to have satisfied the academic requirements and earned the credits allotted to each subject/ course if the student secures a minimum of 40% (40 marks out of 100) in the sum total of the CIE (Continuous Internal Evaluation) and SEE (Semester End Examination) taken together.

Continuous Internal Evaluation:

- For the Assignment component of the CIE, there are 25 marks and for the Internal Assessment Test component, there are 25 marks.
- The first test will be administered after 40-50% of the syllabus has been covered, and the second test will be administered after 85-90% of the syllabus has been covered
- Any two assignment methods mentioned in the 22OB2.4, if an assignment is project-based then only one assignment for the course shall be planned. The teacher should not conduct two assignments at the end of the semester if two assignments are planned.
- For the course, CIE marks will be based on a scaled-down sum of two tests and other methods of assessment.

Internal Assessment Test question paper is designed to attain the different levels of Bloom's taxonomy as per the outcome defined for the course.

Semester-End Examination:

Theory SEE will be conducted by University as per the scheduled timetable, with common question papers for the course (**duration 03 hours).**

1. The question paper will have ten questions. Each question is set for 20 marks.
2. There will be 2 questions from each module. Each of the two questions under a module (with a maximum of 3 sub-questions), **should have a mix of topics** under that module.
3. The students have to answer 5 full questions, selecting one full question from each module.
4. Marks scored shall be proportionally reduced to 50 marks

Suggested Learning Resources:

Text Book

Paul Goransson, Chuck Black, Timothy Culver, "Software Defined Networks: A Comprehensive Approach", 2nd Edition 2017.

Reference Books

1. Nadeau, Thomas D., and Ken Gray. SDN: Software Defined Networks: an authoritative review of network programmability technologies. " O'Reilly Media, Inc.", 2013.
2. Coker, Oswald, and Siamak Azodolmolky. Software-defined Networking with OpenFlow: Deliver Innovative Business Solutions. Packt Publishing Ltd, 2017.

Web links and Video Lectures (e-Resources):

- https://nptel.ac.in/courses/106106243
- https://www.opennetworking.org/ (Open Network Foundation)
- https://www.opennetworking.org/wp-content/uploads/2014/10/openflow-spec-v1.3.0.pdf (OpenFlow version 1.3)
- http://mininet.org/ (Mininet Network Emulator).

Activity Based Learning (Suggested Activities in Class)/Practical-Based learning

- Course projects by the students (group of two) using Mininet Network Emulator and OpenFlow.

	Cyber Policies and CERT-IN		Semester	7
	Course Code	**BCY714C**	CIE Marks	50
	Teaching Hours/Week (L: T:P: S)	3:0:0:0	SEE Marks	50
	Total Hours of Pedagogy	40	Total Marks	100
	Credits	03	Exam Hours	03
	Examination type (SEE)	Theory		

Course objectives:

1. To understand the National Cyber Security Policy, cyber security guidelines, and legal frameworks for secure cyber environments.
2. To explore the roles and responsibilities of CISOs and best practices for safe application and infrastructure management.
3. To comprehend the implications of cyber laws, data governance, and international data protection standards.
4. To analyze the Karnataka Cyber Security Policy and key international frameworks like GDPR, PCI-DSS, NIST, SOX, and HIPAA.
5. To study CERT-In guidelines, technical recommendations, and case studies for effective incident response and cyber threat management.

Teaching-Learning Process (General Instructions)

These are sample strategies; which teachers can use to accelerate the attainment of the various course outcomes.

- Lecturer method (L) does not mean only the traditional lecture method, but different types of teaching methods may be adopted to achieve the outcomes.
- Utilize video/animation films to illustrate the functioning of various concepts.
- Promote collaborative learning (Group Learning) in the class.
- Pose at least three HOT (Higher Order Thinking) questions in the class to stimulate critical thinking.
- Incorporate Problem-Based Learning (PBL) to foster students' analytical skills and develop their ability to evaluate, generalize, and analyze information rather than merely recalling it.
- Introduce topics through multiple representations.
- Demonstrate various ways to solve the same problem and encourage students to devise their own creative solutions.
- Discuss the real-world applications of every concept to enhance students' comprehension.
- Use any of these methods: Chalk and board, Active Learning, Case Studies.

Module-1 8 Hours

National Cyber Security Policy (Refer PDF);

Major research projects in cyber security(Refer DOC);

general guidelines for secure application and infrastructure;
(https://www.cert-in.org.in/PDF/Application_Security_Guidelines.pdf)

	Public procurement for cyber security products (Refer PDF) https://pn.ispirt.in/cybersecurityproductsprocurement/ roles and responsibilities of CISO ((https://cea.nic.in/wp-content/uploads/2020/04/ciso_roles.pdf); Top Best practices for CISOs (Refer PDF) Checklist for secure code programming in Application; (https://owasp.org/www-project-secure-coding-practices-quick-reference-guide/stable-en/02-checklist/05-checklist) Notification of Forensic labs as 'Examiner of Electronic Evidence' under Section 79A of the Information Technology Act 2000; (https://www.itlaw.in/section-79a-central-government-to-notify-examiner-of-electronic-evidence/) Top Best Practices for a Safe & Secure Cyber Environment (https://levelblue.com/blogs/security-essentials/25-essential-cybersecurity-tips-and-best-practices-for-your-business)
	Module-2 8 Hours
	Introduction to Cyber Laws (https://www.lexisnexis.in/blogs/cyber-law-in-india/); Data Governance (https://info.talend.com/rs/talend/images/WP_EN_DG_Talend_DefinitiveGuide_DataGovernance.pdf); Section 69A of IT Act (https://www.indiacode.nic.in/bitstream/123456789/13116/1/it_act_2000_updated.pdf); Data Protection Framework (https://www.dsci.in/content/data-protection-framework-india) ; Advisories (https://www.dsci.in/advisory/threat-intel);
	Module-3 8 Hours
	Karnataka Cyber Security Policy: Public and Government (https://eitbt.karnataka.gov.in/uploads/media_to_upload1728735887.pdf) Operational and Procedure Guidelines. (https://eitbt.karnataka.gov.in/uploads/media_to_upload1728735901.pdf) Introduction to GDPR, PCI-DSS, NIST, SOX and HIPAA (https://www.sattrix.com/blog/wp-content/uploads/2025/04/si-whitepaperNavigating-Compliance-GDPR-HIPAA-and-More_compressed.pdf)

	https://sprinto.com/blog/compliance-standards/
	Module-4 8 Hours
	Introduction; Structure of the CERT-In guidelines; https://www.cert-in.org.in/s2cMainServlet?pageid=CHARTMISSION https://www.cert-in.org.in/s2cMainServlet?pageid=WHATWELIST Key highlights of CERT-In guidelines; https://www.cert-in.org.in/s2cMainServlet?pageid=PUBROLFUN01 Recommendations to help organisations comply with the guidelines(Refer PDF); Technical Guidelines on SBOM (Refer PDF)
	Module-5 8 Hours
	Guidelines on Information Security Practices for Government Entities; (https://cert-in.org.in/PDF/guidelinesgovtentities.pdf) CERT-In white paper on API Security (Refer PDF); Case studies (Refer PDFs) ; India Ransomware Report(Refer PDF); Directions by CERT-In under 70B of Information Technology Act 2000 (https://www.cert-in.org.in/Directions70B.jsp)

Course outcome (Course Skill Set)

At the end of the course, the student will be able to:

1. Apply principles from the National Cyber Security Policy and secure coding practices to enhance cyber security measures in organizations.
2. Assess the legal aspects of cyber operations, including data protection and compliance with Section 69A of the IT Act.
3. Evaluate and implement data governance frameworks and international security standards in diverse environments.
4, Interpret CERT-In guidelines and recommend organizational strategies for cyber security compliance.
5. Analyze real-world cyber incidents, including ransomware, and propose actionable solutions based on case studies and reports.

Assessment Details (both CIE and SEE)

The weightage of Continuous Internal Evaluation (CIE) is 50% and for Semester End Exam (SEE) is 50%. The minimum passing mark for the CIE is 40% of the maximum marks (20 marks out of 50) and for the SEE minimum passing mark is 35% of the maximum marks (18 out of 50 marks). A student shall be deemed to have satisfied the academic requirements and earned the credits allotted to each subject/ course if the student secures a minimum of 40% (40 marks out of 100) in the sum total of the CIE (Continuous Internal Evaluation) and SEE (Semester End Examination) taken together.

Continuous Internal Evaluation:

- For the Assignment component of the CIE, there are 25 marks and for the Internal Assessment Test component, there are 25 marks.
- The first test will be administered after 40-50% of the syllabus has been covered, and the second test will be administered after 85-90% of the syllabus has been covered
- Any two assignment methods mentioned in the 22OB2.4, if an assignment is project-based then only one assignment for the course shall be planned. The teacher should not conduct two assignments at the end of the semester if two assignments are planned.
- For the course, CIE marks will be based on a scaled-down sum of two tests and other methods of assessment.

Internal Assessment Test question paper is designed to attain the different levels of Bloom's taxonomy as per the outcome defined for the course.

Semester-End Examination:

Theory SEE will be conducted by University as per the scheduled timetable, with common question papers for the course (**duration 03 hours).**

- The question paper will have ten questions. Each question is set for 20 marks.
- There will be 2 questions from each module. Each of the two questions under a module (with a maximum of 3 sub-questions), **should have a mix of topics** under that module.
- The students have to answer 5 full questions, selecting one full question from each module.
- Marks scored shall be proportionally reduced to 50 marks

Suggested Learning Resources:

https://www.meity.gov.in/cyber-security-division

https://www.meity.gov.in/cyber-security

https://eitbt.karnataka.gov.in/uploads/media_to_upload1728735887.pdf

https://eitbt.karnataka.gov.in/uploads/media_to_upload1728735901.pdf

https://www2.deloitte.com/in/en/pages/risk/articles/CERT-IN-direction-for-reporting-cyber-incidents.html

https://cert-in.org.in/PDF/guidelinesgovtentities.pdf

Activity Based Learning (Suggested Activities in Class)/ Practical Based learning

Assignment -1: Comparison/Analysis of cyber policies of different countries (Min 5) - A report by a group of TWo students : 15 Marks

Assignment -2: Summary report on the analysis of cyber operations, data protection, data governance and compliance strategies (policies) of organization/state/country. A report by a group of TWo students : 10 Marks

	Cyber Security and Management, Compliance and Governance		**Semester**	VI
	Course Code	BCY714D	**CIE Marks**	50
	Teaching Hours/Week (L: T:P: S)	3:0:0:0	**SEE Marks**	50
	Total Hours of Pedagogy	40	**Total Marks**	100
	Credits	03	**Exam Hours**	03
	Examination type (SEE)	Theory		

Course objectives:

1. To understand the fundamentals of Governance, Risk, and Compliance (GRC) and their role in strategic cyber security planning.
2. To explore risk management life cycles, NIST frameworks, and best practices for cyber security program management.
3. To develop proficiency in utilizing cyber security metrics, frameworks, and risk assessment methodologies.
4. To analyse and apply cyber security controls, architectures, and risk mitigation strategies to secure organizational assets.
5. To examine emerging trends in cyber security, including cloud security, AI-powered solutions, and the impact of quantum computing.

Teaching-Learning Process (General Instructions)

These are sample strategies; which teachers can use to accelerate the attainment of the various course outcomes.

1. Lecturer method (L) does not mean only the traditional lecture method, but different types of teaching methods may be adopted to achieve the outcomes.
2. Utilize video/animation films to illustrate the functioning of various concepts.
3. Promote collaborative learning (Group Learning) in the class.
4. Pose at least three HOT (Higher Order Thinking) questions in the class to stimulate critical thinking.
5. Incorporate Problem-Based Learning (PBL) to foster students' analytical skills and develop their ability to evaluate, generalize, and analyze information rather than merely recalling it.
6. Introduce topics through multiple representations.
7. Demonstrate various ways to solve the same problem and encourage students to devise their own creative solutions.
8. Discuss the real-world applications of every concept to enhance students' comprehension.
9. Use any of these methods: Chalk and board, Active Learning, Case Studies.

Module-1 8 Hours

Governance, Risk, and Compliance Fundamentals

Governance, Risk Management, and Compliance: Understanding GRC and its intersection. GRC frameworks, standards, tools, and culture. Role of GRC in strategic planning. Cybersecurity Program and Project Management: Fundamentals of program and project management. Agile project management in cybersecurity. Communication and collaboration

	in cybersecurity projects.
	Module-2 8 Hours
	Risk Management and NIST Frameworks Risk Management: Understanding risk management life cycle. Third party risk management and compliance expectations. Monitoring, reporting, and risk approvals. NIST Risk Management Framework (RMF): Steps in the NIST RMF authorization process. Integrating NIST RMF into organizational risk management. Challenges and best practices in implementing RMF.
	Module-3 8 Hours
	Metrics, Assessments, and Cybersecurity Frameworks Cybersecurity Metrics: KPIs and KRIs in cybersecurity. Role of metrics in decision making, compliance, and strategy. Risk Assessments: Conducting cybersecurity risk assessments. NIST, FFIEC approaches, and best practices. Cybersecurity Frameworks: ISO/IEC 27001, COBIT, CMMC, and PCI DSS. Comparing and integrating multiple frameworks. Future trends in cybersecurity frameworks.
	Module-4 8 Hours
	Cybersecurity Controls and Architecture NIST SP 80053: Overview and structure of NIST SP 80053 controls. Control families and their applications. Cybersecurity Architecture: Components and layers of cybersecurity architecture. Security reference models and adapting to emerging threats. Risk Mitigation: Basics of risk mitigation and security controls. Policies, user security controls, and physical security measures.
	Module-5 8 Hours
	Emerging Trends in Cybersecurity Cloud Security: Cloud computing services, challenges, and best practices. Security tools, techniques, and future trends in cloud security. Artificial Intelligence in Cybersecurity: AI powered cybersecurity solutions. CISO's AI preparation checklist and its role in cyber defense. Quantum Computing: Quantum cryptography and its impact on cybersecurity. Strategic and security implications of quantum computing.

Course outcome (Course Skill Set)

At the end of the course, the student will be able to:

1. Implement GRC principles and frameworks to enhance organizational cybersecurity and compliance.
2. Apply risk management strategies and integrate NIST RMF processes into organizational workflows.
3. Utilize metrics, assessments, and international frameworks like ISO/IEC 27001 and COBIT for effective cyber security decision-making.
4. Design and evaluate cyber security architectures and controls to mitigate risks and address evolving threats.
5. Assess emerging cyber security technologies and trends, leveraging AI and quantum computing to address future challenges.

Assessment Details (both CIE and SEE)

The weightage of Continuous Internal Evaluation (CIE) is 50% and for Semester End Exam (SEE) is 50%. The minimum passing mark for the CIE is 40% of the maximum marks (20 marks out of 50) and for the SEE minimum passing mark is 35% of the maximum marks (18 out of 50 marks). A student shall be deemed to have satisfied the academic requirements and earned the credits allotted to each subject/ course if the student secures a minimum of 40% (40 marks out of 100) in the sum total of the CIE (Continuous Internal Evaluation) and SEE (Semester End Examination) taken together.

Continuous Internal Evaluation:

- For the Assignment component of the CIE, there are 25 marks and for the Internal Assessment Test component, there are 25 marks.
- The first test will be administered after 40-50% of the syllabus has been covered, and the second test will be administered after 85-90% of the syllabus has been covered
- Any two assignment methods mentioned in the 22OB2.4, if an assignment is project-based then only one assignment for the course shall be planned. The teacher should not conduct two assignments at the end of the semester if two assignments are planned.
- For the course, CIE marks will be based on a scaled-down sum of two tests and other methods of assessment.

Internal Assessment Test question paper is designed to attain the different levels of Bloom's taxonomy as per the outcome defined for the course.

Semester-End Examination:

Theory SEE will be conducted by University as per the scheduled timetable, with common question papers for the course (duration 03 hours).

1. The question paper will have ten questions. Each question is set for 20 marks.
2. There will be 2 questions from each module. Each of the two questions under a module (with a maximum of 3 sub-questions), should have a mix of topics under that module.
3. The students have to answer 5 full questions, selecting one full question from each module.
4. Marks scored shall be proportionally reduced to 50 marks

Suggested Learning Resources:

Textbook

J. Edwards and G. Weaver, *The Cybersecurity Guide to Governance, Risk, and Compliance*. Wiley, May 2024

Reference Book

P. Trim and Y.-I. Lee, *Cyber Security Management: A Governance, Risk and Compliance Framework*, 1st ed. Routledge, 2014.

Activity Based Learning (Suggested Activities in Class)/ Practical Based learning

1. Case Study (15 marks)
2. Assignment (10 marks)

Introduction to DBMS		Semester	7
Course Code	**BCS755A**	CIE Marks	50
Teaching Hours/Week (L:T:P: S)	3:0:0:0	SEE Marks	50
Total Hours of Pedagogy	40	Total Marks	100
Credits	03	Exam Hours	3
Examination nature (SEE)	Theory		

Course objectives:

- To Provide a strong foundation in database concepts, technology, and practice.
- To Practice SQL programming through a variety of database problems.
- To Understand the relational database design principles.
- To Demonstrate the use of concurrency in database.
- To Design and build database applications for real world problems.

Teaching-Learning Process (General Instructions)

These are sample Strategies; that teachers can use to accelerate the attainment of the various course outcomes.

- Lecturer method (L) needs not to be only a traditional lecture method, but alternative effective teaching methods could be adopted to attain the outcomes.
- Use of Video/Animation to explain functioning of various concepts.
- Encourage collaborative (Group Learning) Learning in the class.
- Ask at least three HOT (Higher order Thinking) questions in the class, which promotes critical thinking.
- Discuss how every concept can be applied to the real world - and when that's possible, it helps improve the students' understanding.
- Use any of these methods: Chalk and board, Active Learning, Case Studies.

MODULE-1

Introduction to Databases: Introduction, Characteristics of database approach, Advantages of using the DBMS approach, History of database applications.

Overview of Database Languages and Architectures: Data Models, Schemas, and Instances. Three schema architecture and data independence, database languages, and interfaces, The Database System environment.

Textbook 1:Ch 1.1 to 1.8, 2.1 to 2.6

MODULE-2

Conceptual Data Modeling using Entities and Relationships: Entity types, Entity sets and structural constraints, Weak entity types, ER diagrams, Specialization and Generalization.

Mapping Conceptual Design into a Logical Design: Relational Database Design using ER-to-Relational mapping

Textbook 1: Ch 3.1 to 3.10, 9.1 & 9.2

MODULE-3

Relational Model: Relational Model Concepts, Relational Model Constraints and relational database schemas, Update operations, transactions, and dealing with constraint violations.

Relational Algebra: Unary and Binary relational operations, additional relational operations (aggregate, grouping, etc.) Examples of Queries in relational algebra.

Textbook 1: Ch 5.1 to 5.3, Ch 8.1 to 8.5

MODULE-4

SQL: SQL data definition and data types, Schema change statements in SQL, specifying constraints in SQL, retrieval queries in SQL, INSERT, DELETE, and UPDATE statements in SQL, Additional features of SQL

Normalization: Database Design Theory – Introduction to Normalization using Functional and Multivalued Dependencies: Informal design guidelines for relation schema, Functional Dependencies, Normal Forms based on Primary Keys, Second and Third Normal Forms, Boyce-Codd Normal Form, Multivalued Dependency and Fourth Normal Form, Join Dependencies and Fifth Normal Form.

Textbook 1: Ch 6.1 to 6.5,14.1 to 14.7

MODULE-5

SQL: Advanced Queries: More complex SQL retrieval queries, Specifying constraints as assertions and action triggers, Views in SQL.

Concurrency Control in Databases: Two-phase locking techniques for Concurrency control, Concurrency control based on Timestamp ordering, Multiversion Concurrency control techniques, Validation Concurrency control techniques, Granularity of Data items and Multiple Granularity Locking.

Textbook 1: Ch 7.1 to 7.3, 21.1 to 21.5

Course outcomes (Course Skill Set):
At the end of the course, the student will be able to:

- Demonstrate the basic elements of a database management system.
- Design entity relationship and convert entity relationship diagrams into RDBMS.
- Use Structured Query Language (SQL) for database manipulation.
- Apply normalization to increase the efficiency of database design.
- Illustrate the concepts of concurrency control techniques.

Assessment Details (both CIE and SEE)

The weightage of Continuous Internal Evaluation (CIE) is 50% and for Semester End Exam (SEE) is 50%. The minimum passing mark for the CIE is 40% of the maximum marks (20 marks out of 50) and for the SEE minimum passing mark is 35% of the maximum marks (18 out of 50 marks). A student shall be deemed to have satisfied the academic requirements and earned the credits allotted to each subject/ course if the student secures a minimum of 40% (40 marks out of 100) in the sum total of the CIE (Continuous Internal Evaluation) and SEE (Semester End Examination) taken together.

Continuous Internal Evaluation:

For the Assignment component of the CIE, there are 25 marks and for the Internal Assessment Test component, there are 25 marks.

The first test will be administered after 40-50% of the syllabus has been covered, and the second test will be administered after 85-90% of the syllabus has been covered

Any two assignment methods mentioned in the 22OB2.4, if an assignment is project-based then only one assignment for the course shall be planned. The teacher should not conduct two assignments at the end of the semester if two assignments are planned.

For the course, CIE marks will be based on a scaled-down sum of two tests and other methods of assessment.

Internal Assessment Test question paper is designed to attain the different levels of Bloom's taxonomy as per the outcome defined for the course.

Semester-End Examination:

- Theory SEE will be conducted by University as per the scheduled timetable, with common question papers for the course (duration 03 hours).
- The question paper will have ten questions. Each question is set for 20 marks.
- There will be 2 questions from each module. Each of the two questions under a module (with a maximum of 3 sub-questions), should have a mix of topics under that module.
- The students have to answer 5 full questions, selecting one full question from each module.
- Marks scored shall be proportionally reduced to 50 marks.

Suggested Learning Resources:

Text Books:

1. Fundamentals of Database Systems, Ramez Elmasri and Shamkant B. Navathe, 7th Edition, 2017, Pearson.

Reference Books:

1. Database management systems, Ramakrishnan, and Gehrke, 3rd Edition, 2014, McGraw Hill

Activity Based Learning (Suggested Activities in Class)/ Practical Based learning

Course Project (25 marks)

- For any problem selected
    - Develop the application having at least five tables & domain areas shall include health care, agriculture & so on.

	Introduction to Algorithms		Semester	7
	Course Code	BCS755B	CIE Marks	50
	Teaching Hours/Week (L: T:P: S)	3:0:0:0	SEE Marks	50
	Total Hours of Pedagogy	40	Total Marks	100
	Credits	03	Exam Hours	03
	Examination type (SEE)	Theory		

Course objectives:

- To learn the methods for analyzing algorithms and evaluating their performance.
- To demonstrate the efficiency of algorithms using asymptotic notations.
- To solve problems using various algorithm design methods, including brute force, greedy, divide and conquer, decrease and conquer, transform and conquer, dynamic programming, backtracking, and branch and bound.
- To learn the concepts of P and NP complexity classes.

Teaching-Learning Process (General Instructions)

These are sample Strategies, which teachers can use to accelerate the attainment of the various course outcomes.

1. Lecturer method (L) does not mean only the traditional lecture method, but different types of teaching methods may be adopted to achieve the outcomes.
2. Utilize video/animation films to illustrate the functioning of various concepts.
3. Promote collaborative learning (Group Learning) in the class.
4. Pose at least three HOT (Higher Order Thinking) questions in the class to stimulate critical thinking.
5. Incorporate Problem-Based Learning (PBL) to foster students' analytical skills and develop their ability to evaluate, generalize, and analyze information rather than merely recalling it.
6. Introduce topics through multiple representations.
7. Demonstrate various ways to solve the same problem and encourage students to devise their own creative solutions.
8. Discuss the real-world applications of every concept to enhance students' comprehension.

Module-1

INTRODUCTION: What is an Algorithm?, Fundamentals of Algorithmic Problem Solving, Important problem Types, Fundamental Data Structures, Analysis Framework, Asymptotic Notations and Basic Efficiency Classes, ,Analysis Framework, Asymptotic Notations and Basic Efficiency Classes,

Chapter 1 (Sections 1.1 to 1.4), Chapter 2 (2.1, 2.2)

Module-2

FUNDAMENTALS OF THE ANALYSIS OF ALGORITHM EFFICIENCY: Mathematical Analysis of Non-recursive Algorithms, Mathematical Analysis of Recursive Algorithms.

BRUTE FORCE APPROACHES: Selection Sort and Bubble Sort, Sequential Search and Brute Force String Matching.

Chapter 2(Sections 2.3,2.4), Chapter 3(Section 3.1,3.2)

	Module-3
	Exhaustive Search (Travelling Salesman problem and Knapsack Problem). **Depth First search and Breadth First search.** **DECREASE-AND-CONQUER:** Insertion Sort, Topological Sorting. **DIVIDE AND CONQUER:** Merge Sort, Binary Tree Traversals. **Chapter 3(3.4,3.5), Chapter 4 (Sections 4.1,4.2), Chapter 5 (Section 5.1,5.3)**
	Module-4
	TRANSFORM-AND-CONQUER: Balanced Search Trees (AVL Trees), Heaps and Heapsort. **SPACE-TIME TRADEOFFS:** Sorting by Counting: Comparison counting sort, Input Enhancement in String Matching: Horspool's Algorithm, Hashing. **Chapter 6 (Sections 6.3,6.4), Chapter 7 (Sections 7.1,7.2, 7.3)**
	Module-5
	DYNAMIC PROGRAMMING: Three basic examples, The Knapsack Problem and Memory Functions. **THE GREEDY METHOD:** Kruskal's Algorithm, Dijkstra's Algorithm, Huffman Trees and Codes. **Chapter 8 (Sections 8.1,8.2), Chapter 9 (Sections 9.2,9.3,9.4)**

Course outcome (Course Skill Set)

At the end of the course, the student will be able to:

1. Explain the algorithm design steps and computational problem types.
2. Apply the asymptotic notational method to analyze the performance of the algorithms in terms of time complexity.
3. Demonstrate divide & conquer approaches and decrease & conquer approaches to solve computational problems.
4. Make use of the transform & conquer design approach to solve the given real-world or complex computational problems.
5. Apply greedy and dynamic programming methods to solve graph & string-based computational problems.

Assessment Details (both CIE and SEE)

The weightage of Continuous Internal Evaluation (CIE) is 50% and for Semester End Exam (SEE) is 50%. The minimum passing mark for the CIE is 40% of the maximum marks (20 marks out of 50) and for the SEE minimum passing mark is 35% of the maximum marks (18 out of 50 marks). A student shall be deemed to have satisfied the academic requirements and earned the credits allotted to each subject/ course if the student secures a minimum of 40% (40 marks out of 100) in the sum total of the CIE (Continuous Internal Evaluation) and SEE (Semester End Examination) taken together.

Continuous Internal Evaluation:

- For the Assignment component of the CIE, there are 25 marks and for the Internal Assessment Test component, there are 25 marks.
- The first test will be administered after 40-50% of the syllabus has been covered, and the second test will be administered after 85-90% of the syllabus has been covered
- Any two assignment methods mentioned in the 22OB2.4, if an assignment is project-based then only one assignment for the course shall be planned. The teacher should not conduct two assignments at the end of the semester if two assignments are planned.
- For the course, CIE marks will be based on a scaled-down sum of two tests and other methods of assessment.

Internal Assessment Test question paper is designed to attain the different levels of Bloom's taxonomy as per the outcome defined for the course.

Semester-End Examination:

Theory SEE will be conducted by University as per the scheduled timetable, with common question papers for the course (**duration 03 hours).**

1. The question paper will have ten questions. Each question is set for 20 marks.
2. There will be 2 questions from each module. Each of the two questions under a module (with a maximum of 3 sub-questions), **should have a mix of topics** under that module.
3. The students have to answer 5 full questions, selecting one full question from each module.
4. Marks scored shall be proportionally reduced to 50 marks

Suggested Learning Resources:

Textbooks

1. Introduction to the Design and Analysis of Algorithms, By Anany Levitin, 3rd Edition (Indian), 2017, Pearson.

Reference books

1. Computer Algorithms/C++, Ellis Horowitz, SatrajSahni and Rajasekaran, 2nd Edition, 2014, Universities Press.
2. Introduction to Algorithms, Thomas H. Cormen, Charles E. Leiserson, Ronal L. Rivest, Clifford Stein, 3rd Edition, PHI.
3. Design and Analysis of Algorithms, S. Sridhar, Oxford (Higher Education)

Web links and Video Lectures (e-Resources):

- Design and Analysis of Algorithms: https://nptel.ac.in/courses/106/101/106101060/

Activity Based Learning (Suggested Activities in Class)/ Practical Based learning

1. Problem Solving - Competitive programming (Hacker Rank/ Hacker Earth / Leetcode) – 10 Marks
2. Problem solving (Numerical examples) related to different algorithms – 15 Marks

	SOFTWARE ENGINEERING		Semester	7
	Course Code	**BCS755C**	CIE Marks	50
	Teaching Hours/Week (L:T:P: S)	3:0:0:0	SEE Marks	50
	Total Hours of Pedagogy	50	Total Marks	100
	Credits	04	Exam Hours	3
	Examination type (SEE)	Theory		

Course objectives:

To understand foundational principles and the evolving nature of software engineering.
- To learn various software process models and their practical applications.
- To acquire skills in gathering, modeling, and validating software requirements.
- To apply Agile methodologies and understand core software engineering practices.
- To build a foundation for software design, testing, and quality assurance.

Teaching-Learning Process

These are sample Strategies, which teachers can use to accelerate the attainment of the various course outcomes.

1. Lecturer method (L) needs not to be only a traditional lecture method, but alternative effective teaching methods could be adopted to attain the outcomes.
2. Use of Video/Animation to explain functioning of various concepts.
3. Encourage collaborative (Group Learning) Learning in the class.
4. Ask at least three HOT (Higher order Thinking) questions in the class, which promotes critical thinking.
5. Adopt Problem Based Learning (PBL), which fosters students' Analytical skills, develop design thinking skills such as the ability to design, evaluate, generalize, and analyze information rather than simply recall it.
6. Introduce Topics in manifold representations.
7. Show the different ways to solve the same problem with different circuits/logic and encourage the students to come up with their own creative ways to solve them.
8. Discuss how every concept can be applied to the real world - and when that's possible, it helps improve the students' understanding
9. Use any of these methods: Chalk and board, Active Learning, Case Studies

Module-1

Software and Software Engineering: The nature of Software, The unique nature of WebApps, Software Engineering, The software Process, Software Engineering Practice, Software Myths.

Process Models: A generic process model, Process assessment and improvement, Prescriptive process models: Waterfall model, Incremental process models, Evolutionary process models, Concurrent models, Specialized process models. Unified Process , Personal and Team process models

Textbook 1: Chapter 1: 1.1 to 1.6, Chapter 2: 2.1 to 2.5

Module-2

	Understanding Requirements: Requirements Engineering, Establishing the ground work, Eliciting Requirements, Developing use cases, Building the requirements model, Negotiating Requirements, Validating Requirements. **Requirements Modeling Scenarios, Information and Analysis classes**: Requirement Analysis, Scenario based modeling, UML models that supplement the Use Case, Data modeling Concepts, Class-Based Modeling. Requirement Modeling Strategies : Flow oriented Modeling , Behavioral Modeling. **Textbook 1: Chapter 5: 5.1 to 5.7, Chapter 6: 6.1 to 6.5, Chapter 7: 7.1 to 7.3**
	Module-3
	Agile Development: What is Agility?, Agility and the cost of change. What is an agile Process?, Extreme Programming (XP), Other Agile Process Models, A tool set for Agile process . **Principles that guide practice**: Software Engineering Knowledge, Core principles, Principles that guide each framework activity. **Textbook 1: Chapter 3: 3.1 to 3.6, Chapter 4: 4.1 to 4.3**
	Module-4
	Software Design: Design within the context of software engineering, Design process and quality, Design concepts: abstraction, modularity, architecture, patterns. **Architectural Design**: Architectural styles and patterns, reference architectures, component-level design, designing class-based components, conducting component-level design, design for reuse. **Textbook 1:Chapter 8: 8.1–8.6, Chapter 9: 9.1–9.5**
	Module-5
	Software Testing: Introduction to software testing, Strategic approach, Test strategies for conventional and object-oriented software, Validation testing, System testing, White-box and Black-box testing, Basis Path Testing, Control structure testing. **Software Quality:** Concepts of quality, Software quality assurance, Reviews, Software reliability and metrics. **Textbook 1: Chapter 14: Sections 14.1 to 14.5,Chapter 15: Sections 15.1 to 15.5, Chapter 19: Sections 19.1 to 19.5**

Course outcome

At the end of the course, the student will be able to :

1. Explain the software nature, engineering practices, myths, and software process models.
2. Apply requirements engineering, elicitation, modeling, and validation in software development.
3. Demonstrate agile principles, practices, and tools for software development agility.
4. Apply design concepts, process, and architecture for quality software development.
5. Explain software testing strategies and quality assurance for reliable software.

Assessment Details (both CIE and SEE)

The weightage of Continuous Internal Evaluation (CIE) is 50% and for Semester End Exam (SEE) is 50%. The minimum passing mark for the CIE is 40% of the maximum marks (20 marks out of 50) and for the SEE minimum passing mark is 35% of the maximum marks (18 out of 50 marks). A student shall be deemed to have satisfied the academic requirements and earned the credits allotted to each subject/ course if the student secures a minimum of 40% (40 marks out of 100) in the sum total of the CIE (Continuous Internal Evaluation) and SEE (Semester End Examination) taken together.

Continuous Internal Evaluation:

- For the Assignment component of the CIE, there are 25 marks and for the Internal Assessment Test component, there are 25 marks.
- The first test will be administered after 40-50% of the syllabus has been covered, and the second test will be administered after 85-90% of the syllabus has been covered
- Any two assignment methods mentioned in the 22OB2.4, if an assignment is project-based then only one assignment for the course shall be planned. The teacher should not conduct two assignments at the end of the semester if two assignments are planned.
- For the course, CIE marks will be based on a scaled-down sum of two tests and other methods of assessment.

Internal Assessment Test question paper is designed to attain the different levels of Bloom's taxonomy as per the outcome defined for the course.

Semester-End Examination:

Theory SEE will be conducted by University as per the scheduled timetable, with common question papers for the course (**duration 03 hours).**

1. The question paper will have ten questions. Each question is set for 20 marks.
2. There will be 2 questions from each module. Each of the two questions under a module (with a maximum of 3 sub-questions), **should have a mix of topics** under that module.
3. The students have to answer 5 full questions, selecting one full question from each module.
4. Marks scored shall be proportionally reduced to 50 marks

Suggested Learning Resources:

Textbook

Roger S. Pressman: Software Engineering – A Practitioner's Approach, 7th Edition, Tata McGraw Hill, 2010.

Web links and Video Lectures (e-Resources):

https://www.geeksforgeeks.org/software-engineering/software-engineering/

Activity-Based Learning (Suggested Activities in Class)/Practical-Based learning

- Course project (Group of two students): Simulation that covers all the phases of SDLC - 25 marks

CYBERSECURITY AND ETHICAL HACKING		Semester	7
Course Code	**BCY755D**	CIE Marks	50
Teaching Hours/Week (L: T:P: S)	3:0:0:0	SEE Marks	50
Total Hours of Pedagogy	40	Total Marks	100
Credits	03	Exam Hours	03
Examination type (SEE)	Theory		

Course objectives:

- Understand the fundamentals of cybersecurity and recognize common attack vectors including phishing, malware, and password thefts.
- Analyze various internet and network-based threats, including network tapping, wireless intrusions, and cloud-based attacks.
- Explore the methods used by attackers, such as encryption cracking and account access tricks, to compromise systems and data.
- Develop strategies and best practices to defend against cyber-attacks, including techniques to outsmart black hats and secure digital assets effectively.

Teaching-Learning Process (General Instructions)

These are sample strategies; which teachers can use to accelerate the attainment of the various course outcomes.

1. Lecturer method (L) does not mean only the traditional lecture method, but different types of teaching methods may be adopted to achieve the outcomes.
2. Utilize video/animation films to illustrate the functioning of various concepts.
3. Promote collaborative learning (Group Learning) in the class.
4. Pose at least three HOT (Higher Order Thinking) questions in the class to stimulate critical thinking.
5. Incorporate Problem-Based Learning (PBL) to foster students' analytical skills and develop their ability to evaluate, generalize, and analyze information rather than merely recalling it.
6. Introduce topics through multiple representations.
7. Demonstrate various ways to solve the same problem and encourage students to devise their own creative solutions.
8. Discuss the real-world applications of every concept to enhance students' comprehension.
9. Use any of these methods: Chalk and board, Active Learning, Case Studies.

Module-1

An Introduction to Cybersecurity: What Is Cybersecurity? Black Hats vs. White Hats, More about Cybersecurity and Threats.

Attack Targets on the Internet: How the Internet Works, The Black Hat Attack Methodology, How Black Hats Find You, How to Hide from Black Hats, Analyzing the Network.

Text Book: Ch. 1, Ch. 2

Module-2

Phishing Tactics: What Is Phishing? Vishing and Other Non-Email Phishing, How to Protect Yourself Against Phishing, Hoaxes, Why Black Hats Love Phishing, Analyzing a Phishing Email.

Malware Infections: What Is Malware? Types of Malware, How Black Hats Deploy Malware, How to Defend Against Malware, Analyzing Malware and Managing Antivirus Settings.

Text Book: Ch. 3, Ch. 4

Module-3

Password Thefts and Other Account Access Tricks: Authentication, Authorization, Accounting, Setting Up Accounts in Windows 10 and macOS.

Network Tapping: The Basics of Network Design, Attacking the Network, Defense Against Network Attacks, Setting Up the Firewall.

Text Book: Ch. 5, Ch. 6

Module-4

Attacks In the Cloud: How Cloud Computing Works, Attacking the Cloud, Defending the Cloud**,** Performing SQL Injection on the Damn Vulnerable Web Application.

Wireless Network Pirating: How Wireless Networks Work, Wireless Standards, Wireless Security, Wireless Attacks, Setting Up a Wireless Network with Security in Mind, Secure the WAP.

Text Book: Ch. 7, Ch. 8

Module-5

Encryption Cracking: What Is Cryptography? What We Encrypt, Early Cryptography, Modern Cryptography, What Happens When We Visit a Website? How Black Hats Steal the Keys, Protecting the Keys, How Black Hats Break Hashes, Salting the Hashes, Encrypting and Hashing Files.

How To Defeat Black Hats: What's the Worst that Could Happen? Controls, Risk Management Programs, Putting it All Together, Conducting a Risk Analysis.

Text Book: Ch. 9, Ch. 10

Course Outcomes (Course Skill Set)

At the end of the course, the student will be able to:

1. Identify and explain common cyber threats such as phishing, malware and network attacks targeting individuals and organizations.
2. Demonstrate understanding of various attack surfaces, including wireless networks, cloud infrastructure and password vulnerabilities.
3. Apply attacker techniques such as encryption cracking, network tapping and unauthorized account access.
4. Experiment with security measures and defense mechanisms to prevent and mitigate cyber-attacks across different platforms.
5. Explain basic cybersecurity practices to recognize, respond to and recover from potential cyber incidents effectively.

Assessment Details (both CIE and SEE)

The weightage of Continuous Internal Evaluation (CIE) is 50% and for Semester End Exam (SEE) is 50%. The minimum passing mark for the CIE is 40% of the maximum marks (20 marks out of 50) and for the SEE minimum passing mark is 35% of the maximum marks (18 out of 50 marks). A student shall be deemed to have satisfied the academic requirements and earned the credits allotted to each subject/ course if the student secures a minimum of 40% (40 marks out of 100) in the sum total of the CIE (Continuous Internal Evaluation) and SEE (Semester End Examination) taken together.

Continuous Internal Evaluation:

- For the Assignment component of the CIE, there are 25 marks and for the Internal Assessment Test component, there are 25 marks.
- The first test will be administered after 40-50% of the syllabus has been covered, and the second test will be administered after 85-90% of the syllabus has been covered
- Any two assignment methods mentioned in the 22OB2.4, if an assignment is project-based then only one assignment for the course shall be planned. The teacher should not conduct two assignments at the end of the semester if two assignments are planned.
- For the course, CIE marks will be based on a scaled-down sum of two tests and other methods of assessment.

Internal Assessment Test question paper is designed to attain the different levels of Bloom's taxonomy as per the outcome defined for the course.

Semester-End Examination:

Theory SEE will be conducted by University as per the scheduled timetable, with common question papers for the course (**duration 03 hours).**

1. The question paper will have ten questions. Each question is set for 20 marks.
2. There will be 2 questions from each module. Each of the two questions under a module (with a maximum of 3 sub-questions), **should have a mix of topics** under that module.
3. The students have to answer 5 full questions, selecting one full question from each module.
4. Marks scored shall be proportionally reduced to 50 marks

Suggested Learning Resources:

Textbook:

1. Sam Grubb, How Cybersecurity Really Works: A Hands-On Guide for Total Beginners, No Starch Press

Reference Books:

1. EC-Council, "Ethical Hacking and Countermeasures Attack Phases", Cengage Learning.
2. Michael Simpson, Kent Backman, James Corley, "Hands-On Ethical Hacking and Network Defense", Cengage Learning.

Web links and Video Lectures (e-Resources):

- https://www.youtube.com/watch?v=fNzpcB7ODxQ
- https://www.youtube.com/watch?v=uHU2uajL1EE
- https://www.youtube.com/watch?v=K6V7fc5Hj2s
- https://archive.nptel.ac.in/courses/106/105/106105217/

Activity Based Learning (Suggested Activities in Class)/ Practical Based learning

- Students can choose one of the following activities: Capture the Flag (CTF) Competition, SQL Injection Challenge, Phishing Simulation, Social Engineering Role-Play, Security Policy Creation, Incident Response Simulation, Cryptography Challenge, Ethics Debate etc. (25 Marks)