NIRMA UNIVERSITY

Institute:	Institute of Technology
Name of Programme:	BTech (CSE)
Course Code:	3CS211ME24
Course Title:	System and Website Audit
Course Type:	Disciplinary Minor-Elective
Year of Introduction:	2024-25

L	T	Practical Component				C
		LPW	PW	W	S	
3	0	2	-	-	-	4

Course Learning Outcomes (CLO):

At the end of the course, the students will be able to –

1. explain the role of IT governance and Information Security Policy (BL2)
2. identify components of information systems and the concept of critical data (BL3)
3. evaluate the design, implementation, and monitoring of various security controls to ensure that information assets are adequately safeguarded (BL5)
4. develop various reports after the audit process for information systems, web applications, and information assets (BL6)

Unit	Contents	Teaching Hours (Total 45)
Unit-I	**Governance and Management of IT:** IT Governance, Information Security Policy Documents, IS Management Practices, Organizational Quality Management.	05
Unit-II	**Information Systems Auditing**: Understanding the organization's business, The IS audit life-cycle, The IS audit role, The IS auditor responsibility, authority and accountability, Code of professional ethics, laws, and regulations	05
Unit-III	**Security and Risk Management:** Introduction to Security and Risk Management, Understand and Apply Security Concepts, Evaluate and Apply Security Governance Principles, Data Protection Principles, and Risk Analysis, Risk Analysis and Assessment, Risk Handling and Security Control Assessment, Risk Monitoring, Threat Modelling, Third-Party Risk Management Life Cycle	15
Unit-IV	**System Testing and Audit:** Introduction, Design and Validate Assessment, Test and Audit Strategies, SOC Reports and Security Assessments, Network Vulnerability Scan and Web Vulnerability Scan, Penetration Testing Process and Testing Types, Testing Methods.	15
Unit-V	**Protection of Information Assets:** IS Network Infrastructure, Protecting Data, Key Elements, Roles, and Responsibilities	05

Self-Study:

The self-study contents will be declared at the commencement of the semester. Around 10% of the questions will be asked from self-study contents

Suggested Readings/ References:

1. Richard E. Cascarino, Auditor's Guide to Information Systems Auditing, Wiley
2. Mike Kegerreis, Mike Schiller, Chris Davis, IT Auditing Using Controls to Protect Information Assets, Mc Graw Hill
3. Jack J. Champlain, Auditing Information Systems, Wiley
4. Veena Hingarh, Arif Ahmed, Understanding and Conducting Information Systems Auditing + Website, John Wiley & Sons Inc

Suggested List of Experiments:

Sr. No.	Title	Hours
1	Build a picture of the environment you are testing for auditing using Kali Linux scanning commands	04
2	Demonstrate risk prioritization using the trial version of the Nipper Network Audit Tool	02
3	Generation of Event and simulation using Splunk	02
4	System scanning with Nikto, Nessus.	02
5	Website Scanning using BurpSuite and generating vulnerability	02
6	Implement a port scanner for penetration testing using the programming language of your choice	04
7	Develop and execute exploit code against a remote target. Test vulnerability of computer systems	04
8	Perform web server fingerprinting and log analysis.	04
9	Perform system analysis using OpenVAS	04
10	Study an organization and develop a Security Policy for the organization.	02