NIRMA UNIVERSITY

Institute:	Institute of Technology
Name of Programme:	M.Tech
Course Code:	6CS463
Course Title:	System and Website Audit
Course Type:	(□ Core/ □ Value Added Course / √ **Department Elective** / □ Institute Elective/ □ University Elective/ □ Open Elective / □ Any other)
Year of Introduction:	2022-23

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

Course Learning Outcomes (CLOs):

At the end of the course, the student 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 system and websites to carry out the audit processes (BL5)
4. develop various reports after audit process for information systems, web applications and information assets (BL6)

Syllabus: **Total Teaching hours: 45**

Unit	**Syllabus**	**Teaching hours**
Unit-I	**Governance and Management of IT:** IT Governance, Information Security Policy Document, IS Management Practices, Organizational Quality Management	10
Unit-II	**Security and Risk Management:** Introduction to Security and Risk Management, Understand and Apply Security Concepts, Evaluate and Apply Security Governance Principles, Data Protection Principles, Risk Analysis, Risk Analysis and Assessment, Risk Handling and Security Control Assessment, Risk Monitoring, Threat Modeling, Third-Party Risk Management Life Cycle	15
Unit-III	**Information Security audit process:** Understanding the Auditing Process and Roles of Auditors, Audit Classifications, Inherent Risks During Audits, A Risk-Based Audit Approach, Control Self-Assessment (CSA), Role of Auditor, Practices & Procedures, Information Security Governance	10
Unit-IV	**Security Assessment and Testing:** 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	05
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 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. Jack J. Champlain, Auditing Information Systems, Wiley
3. https://www.udemy.com/course/information-systems-audit-fundamentals/
4. https://www.udemy.com/course/information-systems-auditor/

Suggested List of Experiments:

Sr. No.	Title	Hours
1	Demonstrate your understanding of network traffic auditing using wireshark. Figure out what is wrong in the .pcap (captured file) given to you with the help of wireshark.	04
2	Build the picture of the environment you are testing for auditing using kali linux scanning commands from the following list: 1. nmap -sn -PE <target> 2. netdiscover -r <target> 3. crackmapexec <target> 4. nmap <target> –top-ports 10 –open 5. nmap <target> -p- -sV –reason –dns-server ns 6. us -mT -Iv <target>:a -r 3000 -R 3 && us -mU -Iv <target>:a -r 3000 -R 3 7. nmap -sS -sV -T4 <target> 8. hping3 –scan known <target> 9. nc -nvz <target> 1-1024 10. nc -nv <target> 22 11. nmap -sV <target> 12. db_import <file.xml> (For Metasploit Framework) 13. nmap -f –mtu=512 <target> 14. masscan <network> -p80 –banners –source-ip <target>	04
3	Demonstrate risk prioritization using the trial version of Nipper Network Audit Tool	04
4	Implement a port scanner for penetration testing using programming language of your choice	06
5	Develop and execute exploit code against a remote target. Test vulnerability of computer systems	04
6	Study of an organization and develop a Security Policy for the organization.	04
7	Perform web server fingerprinting and log analysis.	04

Suggested Case List: -NA-