SECURITY STANDARDS AND AUDITS

Subject Code: CS34326CS	Subject Type: Elective
Evaluation Scheme: MSE(30), TA(20), ESE(50)	L-T-P: 3-0-0

Pre-Requisites: Cyber Security, Information Security Fundamentals, Computer Networks, Audit Reporting.

Course Objective: To provide knowledge of security standards, risk management, and audit practices for assessing compliance and strengthening organizational security.

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

CO-1	Understand major security standards, frameworks, and governance practices.
CO-2	Analyze risk management and regulatory compliance requirements.
CO-3	Apply security audit methods, control assessment, and evidence collection techniques.
CO-4	Evaluate security compliance of systems, networks, cloud, and applications.
CO-5	Prepare audit reports and recommend corrective actions for continuous improvement.

Course Articulation Matrix:

CO/PO	PO-1	PO-2	PO-3	PO-4	PO-5	PO-6
CO-1	2	2	1	2	1	1
CO-2	2	3	2	2	2	1
CO-3	1	3	3	2	2	1
CO-4	2	3	3	3	2	1
CO-5	1	2	2	2	3	1

1 - Slightly; 2 - Moderately; 3 – Substantially

Syllabus:

Unit-1: Security Governance, Risk, and Compliance

Introduction to security governance: security policies, procedures, and baselines; security standards and frameworks: ISO/IEC 27001, ISO/IEC 27002, NIST Cybersecurity Framework, COBIT, and CIS Controls; governance, risk, and compliance (GRC) concepts; asset classification; security roles and responsibilities; and security awareness and training.

Unit 2: Risk Management and Regulatory Compliance

Risk management and compliance: risk identification, qualitative and quantitative risk assessment, business impact analysis, risk treatment, and risk acceptance; major regulatory frameworks: GDPR, PCI-DSS, DPDP Act (India), RBI, and SEBI guidelines; third-party and vendor risk management; security metrics; documentation and control mapping.

Unit 3: Security Auditing and Assessment Techniques

Security audit process: internal, external, compliance, and technical audits; audit planning and scope definition; audit lifecycle; control testing; evidence collection and sampling methods;

interview techniques; vulnerability assessment basics; audit of operating systems, databases, networks, and cloud systems; log review and audit trails.

Unit 4: Audit Reporting, Continuous Assurance, and Emerging Trends

Audit reporting and continuous assurance: classification of audit findings, root cause analysis, corrective and preventive actions; remediation planning and follow-up; business continuity and disaster recovery audits; secure SDLC audits; cloud security audits, and case studies of compliance failures and security breaches. emerging trends: AI in auditing and automated compliance monitoring.

Learning Resources:

Text Books:

1. Davis, Chris, Mike Schiller, and Kevin Wheeler. IT auditing: Using controls to protect information assets. McGraw-Hill Osborne Media, 2006.
2. Moeller, Robert R. IT audit, control, and security. John Wiley & Sons, 2010.
3. Humphreys, Edward. Implementing the ISO/IEC 27001 information security management system standard. Artech House, 2025..
4. Pascoe, Cherilyn, Stephen Quinn, and Karen Scarfone. "The NIST cybersecurity framework (CSF) 2.0." (2024).

Reference Books:

1. Isaca. The risk IT framework. ISACA, 2009.
2. Chapple, Mike, James Michael Stewart, and Darril Gibson. ISC2 CISSP Certified Information Systems Security Professional Official Study Guide. John Wiley & Sons, 2018.
3. Williams, Branden, and James Adamson. PCI Compliance: Understand and implement effective PCI data security standard compliance. CRC Press, 2022.

PROJECT WORK/DISSERTATION-I