SECURITY AND AUDIT PRACTITIONER

ENCTNS 625

Credits: 4 **Year: II** **Part: I**

Course Objectives

This course provides students with advanced knowledge and practical skills necessary for planning, executing, and managing security audits in complex information system environments. It integrates frameworks like ISO 27001, NIST, COBIT, and CIS controls and applies industry practices aligned with CISA standards, emphasizing IT governance, risk management, audit process, business resilience, and information asset protection.

Learning Outcomes	Chapter Contents	Credit Hours	Teaching Methods
- Understand IS auditing principles - Apply global standards - Develop risk-based plans	**1. Introduction to Security and Audit Practices** 1.1 Overview of IS Auditing 1.2 IS Audit Standards (ISACA, ISO 27001, NIST) 1.3 Types of Audits 1.4 Risk-based Planning	10	• Interactive case study lectures • Risk assessment workshop • Audit type classification exercise
- Evaluate governance frameworks - Conduct risk assessments - Ensure compliance	**2. IT Governance and Risk Management** 2.1 IT Governance Frameworks 2.2 Enterprise Architecture 2.3 Risk Management Process 2.4 Maturity Models 2.5 Regulatory Compliance	10	• COBIT implementation lab • Risk assessment simulation • Compliance scenario analysis
- Audit SDLC phases - Assess project feasibility - Test development controls	**3. Auditing IS Acquisition & Development** 3.1 Project Management Audits 3.2 Feasibility Analysis 3.3 SDLC/Agile Controls 3.4 Security Testing Methods	10	• SDLC control testing lab • Agile vs Waterfall comparison • Secure code review practice
- Analyze operations resilience - Perform BIA - Validate DRP/BCP	**4. IS Operations & Business Continuity** 4.1 IT Operations Management 4.2 Business Impact Analysis 4.3 Business Continuity Planning 4.4 Disaster Recovery Strategies	12	• BIA development workshop • DRP tabletop exercise • System resilience case studies

- Apply security frameworks - Evaluate IAM controls - Conduct security audits	**5. Information Asset Protection** 5.1 Security Frameworks 5.2 Identity & Access Management 5.3 Encryption/PKI Systems 5.4 Network/Cloud Security	10	• Nessus scanning practical • IAM policy review • Cloud security configuration audit
- Investigate security incidents - Follow forensic protocols - Manage breach response	**6. Incident Response & Forensics** 6.1 Security Event Monitoring 6.2 Incident Response Process 6.3 Digital Evidence Handling 6.4 Forensic Investigation Techniques	8	• Splunk SIEM lab session • Incident response simulation • Forensic toolkit demonstration

Practical Activities

1. Information Security Gap Assessment through ISO 27001
2. Cyber Security Maturity Assessment thorough NIST Cyber Security Framework.
3. IT Governance Audit through Control Objective for Related Technologies.
4. Develop IS Audit Terms of Reference

Evaluation Schemes

a. Internal Evaluation

Type	**Weightage**
Minor tests	70%
Assignments	30%

b. Final Exam

The questions will cover all chapters of the syllabus. The evaluation scheme will be as indicated in the table:

Chapter	**Hours**	**Mark distribution***
1	10	10
2	10	10
3	10	10
4	12	12
5	10	10

6	8	8
Total	**60**	**60**

*There may be minor deviation in marks distribution.

References

1. Hall, J. A. (2020). *Information Technology Auditing and Assurance* (5th ed.). Cengage Learning
2. Moeller, R. (2022). *IT Audit, Control, and Security* (3rd ed.). Wiley.
3. ISACA. (2023). *CISA Review Manual, 28th Edition*. Information Systems Audit and Control Association. https://books.google.com.np/books?id=3irIzwEACAAJ
4. Hingarh, V., & Ahmed, A. (2013). *Understanding and conducting information systems auditing*. John Wiley & Sons.
5. Champlain, J. J. (2003). *Auditing information systems*. John Wiley & Sons.
6. Cascarino, R. E. (2007). *Auditor's guide to information systems auditing*. John Wiley & Sons.