CTMSCS SI P2: Cyber Security Audit and Compliance

Teaching Scheme					Evaluation Scheme								
					Theory						Practical		Total
					Internal Exams				University Exams		University Exams (LPW)		
					TA-1/TA-2		MSE						
Th	Tu	Pr	C	TCH	Marks	Hrs	Marks	Hrs	Marks	Hrs	Marks	Hrs	
03	01	00	04	04	25	00:45	50	01:30	100	03.00	-	-	200

Objectives

1. To learn Security Audit and Compliance
2. To understand the process of security audit
3. To understand the industry standard practices for auditing
4. To learn various security standards
5. To learn the policy making and organizational structure
6. To understand the Risk and Continuity planning

UNIT – I

The need for information system security compliance

What is IT security assessment? What is an IT security audit? What is compliance? How does an audit differ from an assessment? Why are governance and compliance important? What if an organization does not comply with compliance laws? What is the scope of an IT compliance audit? What does your organization do to be in compliance? What are you auditing within the IT infrastructure? Maintaining IT compliance.

UNIT - II

Planning and implementation of an IT Infrastructure Audit for compliance

Defining the scope for audit, Identifying critical requirements for the audit, assessing IT security, Obtaining Information, Documentation and Resources, Mapping the IT security policy framework definition to the seven domains of typical IT infrastructure, Identifying and Testing Monitoring Requirements **What Are Controls and Why Are They Important?:** Goal- Based Security Controls, Implementation-Based Security Controls, The Security Control Formulation and Development Process, Setting the Stage for Control Implementation through

Security Architecture Design, Implementing a Multitiered Governance and Control Framework in a Business **The IT Audit Process:** Audit Plan, Audit Process, Types of IT Audits, Computer-Assisted Audit Techniques (CAATs), CAATs for Sampling, CAATs for Application Reviews, CAATs for Auditing Application Controls.

UNIT – III

Conducting an IT Infrastructure Audit for Compliance

Identifying the Minimum Acceptable Level of Risk and Appropriate Security Baseline Definitions, Seven Domains of a Typical IT Infrastructure, Writing the IT Infrastructure Audit Report **Compliance within User Domain:** Compliance law requirements and business drivers, Items Commonly Found in the User Domain, **Compliance within the workstation domain:** Compliance law requirements and business drivers, devices and components commonly found in the workstation domain, Maximizing C-I-A, **Compliance within the LAN Domain:** Compliance law requirements and business drivers, devices and components commonly found in the LAN domain, Maximizing C-I-A, **Compliance within LAN and WAN Domain:** Devices and Components Commonly Found in the Domain , Penetration Testing and Validating Configurations, **Compliance within Remote Access and Application Domain:** Devices and Components Commonly Found in the Domain, Application Server Vulnerability Management, Application Patch Management.

UNIT – IV

Risk Assessment and BCP, DR Planning

Introduction to Risk Analysis, Risk Identification, Risk Assessment, Risk Response and Mitigation, Risk Reporting, Introduction to Business Continuity Planning (BCP), Overview of BCP Life Cycle, Need for BCP, Identifying and Selecting Business Continuity Strategies, Introduction to Disaster Recovery (DR) planning, Identification of potential disaster status, DR Strategies, Plans for Business Resumption.

UNIT–V

Cyber Law and Auditing Standards/Frameworks

Indian IT ACT with Amendments, Adjudication under Indian IT ACT, Auditing Standards and Frameworks: ISO/IEC 27001/2, COBIT, SOC Compliance, HIPAA,

0931

GDPR and PCIDSS.

Reference Books

1. Auditing IT Infrastructures for Compliance by Martin M. Weiss, Michael G. Solomon, Jones & Bartlet Learning, 2015
2. The IT Regulatory and Standards Compliance Handbook by Craig S. Wright, Syngress, 2015
3. Information Technology Control and Audit 5th Edition by Angel R. Otero, 2019
4. (Internal Audit and IT Audit Series) The Complete Guide to Cyber Security Risks and Controls by Anne Kohnke, Dan Shoemaker, Ken Sigler, 2016
5. PCI DSS An Integrated Data Security Standard Guide- Press by Jim Seaman, 2020
6. AICPA - Guide_ SOC 2 Reporting on an Examination of Controls at a Service Organization Relevant to Security, Availability, Processing Integrity, Confidentiality, or Privacy-Wiley, 2018
7. The EU General Data Protection Regulation (GDPR) A Practical Guide by Paul Voigt and Axel von dem Bussche, 2017
8. PCI DSS, SAQ Instructions and Guidelines (Available online)
9. Bob Hayes, Kathleen Kotwica, "Business Continuity 2nd Edition", Elsevier Pub.2013.
10. Governance, risk, and compliance by Microsoft, 2019.

NATIONAL FORENSIC SCIENCES UNIVERSITY GANDHINAGAR

0932