CTMTAIDS SI P3: Incident Response and Audit Compliances

Teaching Scheme					Evaluation Scheme									
					Theory							Practical		Total
					Internal Exams					University Exams		University Exams (LPW)		
					TA-1		MSE		TA-2 *					
L	T	P	C	TCH	Marks	Hrs	Marks	Hrs	Marks	Marks	Hrs	Marks	Hrs	
03	00	00	03	03	25	00:45	50	01:30	25	100	03:00	-	-	200

* Note: TA-2 will be in form of assignments or workshops.

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

Cyber Incident Statistics, Computer Security Incident, Information Warfare, Key Concepts of Information Security, Types of Computer Security Incidents, Examples of Computer Security Incidents, How to Identify an Incident, Need for Incident Response, Goals and Purpose of Incident Response, Signs of an Incident, Incident Categories

UNIT–II

Incident Prioritization, Use of Disaster Recovery Technologies, Impact of Virtualization on Incident Response and Handling, Estimating Cost of an Incident, Incident Reporting, Incident Reporting Organizations, Vulnerability Resources, Incident Management, Incident Response Team Roles, Incident Response Team Responsibilities, Dependencies.

UNIT – III

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

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

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

Reference Books: -

1. Auditing IT Infrastructures for Compliance by Martin M. Weiss, Michael G. Solomon, Jones and 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.
11. Computer Incident Response and Forensics Team Management: Conducting a Successful Incident Response by Leighton Johnson
12. Incident Handling and Response: A Holistic approach for an efficient security incident management by Jithin Aby Alex
13. Blue Team Handbook: Incident Response Edition by Don Murdoch
14. The Computer Incident Response Planning Handbook: Executable Plans for Protecting Information at Risk by N. K. McCarthy
15. Critical Incident Management: A Complete Response Guide, Second Edition by John McNall, Thomas T. Gillespie, Vincent F. Faggiano