Devi Ahilya University, Indore, India Institute of Engineering & Technology				IV B.E. Information Technology (Full Time)			
Subject Code & Name	**Instructions Hours per Week**			**Credits**			
ITR7E4	**L**	**T**	**P**	**L**	**T**	**P**	**Total**
Security Assessment, Risk Management and Digital Forensics	**3**	**1**	**1**	**3**	**1**	**1**	**5**
Duration of Theory Paper: 3 Hours							

Learning Objectives:

- To Understand the fundamentals of managing information security systems and personnel
- To Learn how security and management are interrelated - Understand the laws and regulations surrounding information security –
- To Learn how to plan for disaster recovery - Learn how to conduct security audit

Unit I

Network Security Assessment: - The Business Benefits, IP: The Foundation of the Internet, Classifying Internet-Based Attackers, Assessment Service Definitions, Network Security Assessment Methodology, and the Cyclic Assessment Approach

Network Security Assessment Platform :- Virtualization Software, Operating Systems, Reconnaissance Tools , Network Scanning Tools , Exploitation Frameworks , Web Application Testing Tools.

Unit-II

Internet Host and Network Enumeration: - Querying Web and Newsgroup Search Engines, Querying Domain WHOIS Registrars, Querying IP WHOIS Registrars, BGP Querying. DNS Querying, Web Server Crawling, Automating Enumeration, SMTP Probing; Enumeration Technique Recap, Enumeration Countermeasures

IP Network Scanning: - ICMP Probing, TCP Port Scanning, UDP Port Scanning, IDS Evasion and Filter Circumvention, Low-Level IP Assessment, Network Scanning Recap

Network Scanning Countermeasures.

Unit III

Risk Management: - Introduction, Overview of Risk Management, Components of Risk Management, Risk Identification, Risk Assessment, Risk Control,

Asset identification and valuation: - People, procedure and data asset identification; Hardware, software and network asset identification; Information asset classification and valuation; Data classification and management, Threat identification. Risk Likelihood, Valuation of information asset, Risk determination, Identification of possible controls.

Unit IV

Documenting the results of Risk assessment, Risk Control, Risk avoidance, transference, mitigation, and acceptance, selecting a Risk control strategy, architecture layer, characteristics of secure information, feasibility studies and cost benefit analysis.

Information Security Maintenance:- Information Security maintenance models, ISO network

management models, Configuration and change management, Maintenance model.

Unit V

Digital Forensics, The forensic process, collecting digital evidence, live vs. dead analysis, imaging electronic media, collecting volatile data, database forensics.
Forensics science, history of forensics science, sub division, and litigation science.

Learning Outcomes:

- In this course students will learn the practical skills necessary to perform regular risk assessments for their organizations.
- The ability to perform risk management is crucial for organizations hoping to defend their systems

REFERENCE BOOKS:

- Whitman &Mattord, Principles of Incident Response and Disaster Recovery, Course Technology,