Marwadi University
Marwadi Chandarana Group

NAAC A+

Syllabus for Master of Technology

Computer Engineering

Subject Code: 01CY0119
Subject Name: ISO/IEC 27001
M. Tech. Year – 1

Objective:

To provide foundational knowledge of ISO/IEC 27001:2022 and enable students to understand the principles, structure, and implementation aspects of Information Security Management Systems (ISMS) in alignment with global standards and practices.

Credits Earned: 3 Credits

Course Outcomes: After completion of this course, student will be able to

- Understand the scope and applicability of ISO/IEC 27001 in an organizational context.
- Explain the structure and purpose of the ISMS standard and its clauses.
- Identify organizational information assets and evaluate threats and vulnerabilities.
- Apply basic risk management principles and design control strategies.
- Draft policies and ISMS-related documentation based on real-world scenarios.

Pre-requisite of course: Basic understanding of Cybersecurity Concepts, Network Security, and Organizational Processes.

Teaching and Examination Scheme

Teaching Scheme (Hours)			Credits	Theory Marks			Tutorial/ Practical Marks		Total Marks
Theory	Tutorial	Practical		ESE (E)	Mid Sem (M)	Internal (I)	Viva (V)	Termwork (TW)	
3	0	0	3	50	30	20	00	00	100

Contents:

Unit	Topics	Contact Hours
1	**Introduction to ISMS & ISO/IEC 27001** Importance of Information Security,History and need for ISMS,Overview of ISO/IEC 27001 and family (27000, 27002, etc.), Key Terminologies (CIA, SoA, Risk, Controls, etc.).	7
2	**Structure of ISO/IEC 27001:2022** High-Level Structure (HLS) of ISO Standards,Clauses 4 to 10 Overview:	8

	Context, Leadership, Planning, Support, Operation, Evaluation, and Improvement.	
3	**Asset Management & Risk Fundamentals** Asset Identification & Classification, Threat & Vulnerability concepts ,Introduction to Risk Assessment and ISO 27005.	7
4	**Control Objectives & Annex A** Introduction to Control Domains in Annex A, Themes: Organizational, People, Physical, Technological,Basic examples of applying controls in small setups.	7
5	**ISMS Documentation and Introduction to Audit** Overview of Policy, Procedures, SoA, Risk Treatment Plan, Internal audit basics and ISO certification process, Case studies on small business ISMS deployment.	7
	Total Hours	36

References:

1. **ISO/IEC 27001:2022** Standard
2. **ISO/IEC 27002:2022** – Guidelines for controls
3. **Edward Humphreys** – "Implementing the ISO/IEC 27001 ISMS Standard"
4. **Alan Calder** – "IT Governance: An International Guide"
   NIST SP 800-30 and SP 800-53 documents (for comparison)

Suggested Theory distribution:

Distribution of Theory for course delivery and evaluation					
Remember	Understand	Apply	Analyse	Evaluate	Create
15 %	30%	25%	15%	10%	5%

Instructional Method:

a) The course delivery method will depend upon the requirement of content and need of students. The teacher in addition to conventional teaching method by black board, may also use any of tools such as demonstration, role play, Quiz, brainstorming, MOOCs etc.
b) The internal evaluation will be done on the basis of continuous evaluation of students in the laboratory and class-room.
c) Students will use supplementary resources such as online videos, NPTEL videos, e-courses, Virtual Laboratory.

Supplementary Resources:

a. ISO.org training guides and templates
b. NIST Cyber security Framework
c. CIS Controls

d. MOOC/NPTEL on Information Security Governance
e. Online tools: Risk Assessment Templates, SoA builders