SILVER OAK UNIVERSITY

School of Technology, Design and Computer Application
Silver Oak College of Computer Application
Department of Computer Application
Master of Science Cyber Security & Digital Forensics

Course Name: Information Security Management System
Course Code: 1040147109
Semester: 2nd

Prerequisite: Understanding of Information Technology (IT)**,** Foundational Knowledge of Information Security**,** Knowledge of Regulatory Compliance.

Course Objective: The objective of ISMS is to understand the foundational principles and components of ISMS, including risk assessment, policy development, and security controls implementation, to design and deploy a robust security framework tailored to organizational needs.

Teaching Scheme:

Teaching Scheme				
L	T	P	Contact Hours	Credit
3	1	0	4	4

Content:

Unit No.	Course Contents	Teaching Hours	% Weightage
1	**ISMS – ISO27001 & Audit Planning:** Introduction to ISO27001, Fundamental principles of information security, ISO/IEC 27001 certification process, Information Security Management System (ISMS), Fundamental audit concepts and principles, Audit approach based on evidence and on risk, Preparation of an ISO/IEC 27001 certification audit, ISMS documentation audit, Conducting an opening meeting	12	30
2	**ISMS Audit – Implementation:** Communication during the audit, Audit procedures: observation, Document review, interview, sampling techniques, technical verification, corroboration and evaluation, Audit test plans, Formulation of audit findings, Documenting nonconformities	12	30
3	**ISMS Audit – Assurance:** Audit documentation, Quality review, Conducting a closing meeting and conclusion of an ISO/IEC 27001 audit, Evaluation of corrective action plans ISO/IEC 27001 Surveillance audit, Internal audit management program	10	25

4	**Monitoring and Reviewing ISMS** Continuous Monitoring,Internal Audits, Management Review, Incident Management and Response, Incident Response Plan, Incident Reporting and Handling, Post-Incident Analysis, ISMS Documentation, Documentation Requirements: Creating and maintaining necessary ISMS documentation, including policies, procedures, records, and reports. Document Control: Ensuring documents are controlled, regularly reviewed, and updated as necessary.Compliance and Legal Requirements, Regulatory Compliance: Ensuring compliance with relevant laws, regulations, and industry standards (e.g., GDPR, HIPAA, PCI-DSS).Legal Considerations: Understanding legal obligations related to information security and data protection.	8	15

Course Outcomes:

Sr. No.	CO-Statement	Unit No
CO-1	Understand and apply core information security principles from ISO/IEC 27001 standards to protect organizational assets.	1
CO-2	Develop and execute comprehensive audit strategies for ISO/IEC 27001 certification using various techniques.	2
CO-3	Analyze audit findings, identify nonconformities, and create test plans for ISO/IEC 27001 compliance.	3
CO-4	Analyze and evaluate the processes of Continuous Monitoring, Internal Audits, Incident Management.	4

Major Equipment:

1. Computer System
2. LAN cable

Teaching & Learning Methodology:-

1. Projector and Computer
2. Experiments shall be performed in the laboratory related to course contents

List of Tutorials: **Total Hours: 14**

Sr. No.	Tutorials Name
1.	Discuss the core principles such as confidentiality, integrity, and availability, fundamental for understanding security mechanisms.
2.	A step-by-step guide through the certification process, covering assessment, audit, and certification issuance.
3.	Exploring the components and methodologies essential for establishing and maintaining an effective ISMS.

4.	Unpacking foundational audit principles like independence, objectivity, and evidence gathering, crucial for conducting successful audits.
5.	A comprehensive explanation of the audit methodology centered around risk assessment and evidence-based decision-making.
6.	Practical insights into preparing for a certification audit, including planning, resource allocation, and documentation review.
7.	Comprehensive guide to auditing ISMS documentation, ensuring alignment with ISO/IEC 27001 standards for compliance.
8.	Essential tips and techniques for conducting effective opening meetings to set the stage for successful audits.
9.	Case Study on PCI DSS.

Books Recommended:

1. Van Haren Publishing - Calder, A "Implementing Information Security Based on ISO 27001/ISO 27002: A Management Guide (2nd Ed.)", Van Haren Publishing
2. Implementing the ISO / IEC 27001 Information Security Management System Standard. Artech House, ISO and the International Electrotechnical Commission (IEC).
3. Publishers - Humphreys, E Implementing the ISO / IEC 27001 Information Security Management System Standard. ISO and the International Electrotechnical Commission (IEC).

CO-PO-PSO MATRIX:

Co.No	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PSO1	PSO2
CO-1	3	1	1	1		3		1	2
CO-2	2	2	1	2				2	2
CO-3	2	3	2	2				2	2
CO-4	1	2	1	1				1	2