**Subject Code:** 01CY0306

**Subject Name: Information Security Management System**

**MTech. Year – 2 (Semester – 3)**

**Objective:**

|  |
| --- |
| To overcome security threats which are exposed through organizations and their information systems and networks. To reduce risk effects which undermines or creates difficulties for its business operations. Therefore, need of information security management methodology to protect information systematically. This creates importance of ISMS. |

**Credits Earned:** 4 Credits

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

* Understand key elements of ISO 19011 and ISO/IEC 17021 Standards
* Understand key information security issues
* Plan an audit against a set of audit criteria
* Successfully execute an Information Security Management system audit
* Create clear, concise and relevant audit reports
* Communicate the audit findings to a client

**Pre-requisite of course:** Understand the Plan Do Check Act (PDCA) Cycle

**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) | Term work (TW) |
| 3 | 0 | 2 | 4 | 50 | 30 | 20 | 25 | 25 | 150 |

**Contents:**

|  |  |  |
| --- | --- | --- |
| **Unit** | **Topics** | **Contact Hours** |
| 1 | **Information Security Management System**   |  |  | | --- | --- | | |  | | --- | | Introduction, Importance of Information in ISMS, CIA and DAD triads, ISMS purpose and objectives, Legal and Regulatory Framework, Conformance Vs. Compliance. | | | 6 |
| 2 | **Audit Planning and Preparation**  Reasons for auditing, Audit principles, Process of audit program management, Audit competence and evaluation methods, Audit Responsibilities, Audit time and process flow, ISMS audit check list. | 7 |
| 3 | **Audit Techniques and collecting evidence.**  Auditor quality and selection, Audit Script, Audit stages, Audit techniques, collecting evidence through questions, Observation, reporting to audit finding, Audit team meeting, Nonconformities and observation, Corrective and preventive actions. | 8 |
| 4 | |  | | --- | | **ISO 27001**  Process approach and processes involved in establishing, Implementing and Operation, Monitoring and reviewing, Maintaining and Improving the ISMS, ISMS scope and exclusions. | | 10 |
| 5 | |  | | --- | | **Asset Management**  Responsibility for asset, Managing business assets, agreements on how to deal with business assets, Media handling, BYOD, Information Classifications. | | 9 |
|  | **Total Hours** | **40** |

**References:**

|  |  |
| --- | --- |
| 1. Foundations Of Information Security Based On ISO27001, Van Haren Publishing 2. Information Security based on ISO 27001/ISO 27002: A Management Guide (Best Practice), Alan Calder 3. IT Auditing Using Controls to Protect Information Assets, 2nd Edition 2nd Edition, Chris Davis  |  | | --- | |  | |

**Suggested Theory distribution:**

The suggested theory distribution as per Bloom’s taxonomy is as per follows. This distribution serves as guidelines for teachers and students to achieve effective teaching-learning process

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|  | Distribution of Theory for course delivery and evaluation | | | |  |
| Remember | Understand | Apply | Analyze | Evaluate | Create |
| 5% | 10% | 15% | 30% | 20% | 30% |

**Suggested List of Experiments:**

1. Identify the Risk in given Audit area by using RM Studio.
2. Identify the Risk in given Audit area by using RiskWatch.
3. Practical on Risk Management by using Ear / Pilar risk analysis.
4. Audit and Analyse risk in your organization by using ISMS tools.
5. By using GNU PGP learn encryption.

**Instructional Method:**

1. 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.
2. The internal evaluation will be done on the basis of continuous evaluation of students in the laboratory and class-room.
3. Practical examination will be conducted at the end of semester for evaluation of performance of students in laboratory.
4. Students will use supplementary resources such as online videos, NPTEL videos, e-courses, Virtual Laboratory