**Subject Code: 01CY0103**

**Subject Name: Information Security Risk Assessment and Assurance**

**MTech. Year – 1 (Semester – 1)**

**Objective:** The purpose is to understand the risk assessment while handling and processing information and implementing security in audit.

**Credits Earned:** 4 Credits

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

* To gain the knowledge about Information Risk.
* Analyse the various control structures that requires to use in real time applications
* To discovery knowledge in collecting data about organization.
* To do various analysis on Information Risk Assessment.
* To understand IT audit and its activities.

**Pre-requisite of course:** Computer Network

**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 | **INTRODUCTION** What is Risk? –Information Security Risk Assessment Overview- Drivers, Lawsand Regulations- Risk Assessment Frame work – Practical Approach. | 9 |
| 2 | **DATA COLLECTION** The Sponsors- The Project Team- Data Collection Mechanisms- ExecutiveInterviews- Document Requests- IT Assets Inventories- Profile & Control Survey-Consolidation.  | 9 |
| 3 | **DATA ANALYSIS** Compiling Observations- Preparation of catalogues- System Risk Computation-Impact Analysis Scheme- Final Risk Score. | 9 |
| 4 | RISK ASSESSMENT System Risk Analysis- Risk Prioritization- System Specific Risk Treatment- IssueRegisters- Methodology- Result- Risk Registers- Post Mortem. | 9 |
| 5 | SECURITY AUDIT PROCESS)Pre-planning audit- Audit Risk Assessment- Performing Audit- Internal Controls-Audit Evidence- Audit Testing- Audit Finding- Follow-up activities | 9 |
|  | **Total Hours** | **45** |

**References:**

1. Mark Talabis, “*Information Security Risk Assessment Toolkit: Practical Assessments through Data Collection and Data Analysis*”, Syngress; 1

edition, ISBN: 978-1-59749-735-0, 2012.

2. David L. Cannon, “*CISA Certified Information Systems Auditor Study Guide*”,

John Wiley & Sons, ISBN: 978-0-470-23152-4, 2009.

**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:**

**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

Supplementary Resources:

1. http://www.isaca.org/Certification/CISA-Certified-Information-Systems-Auditor/Pages/default.aspx