Semester 2
Paper 205: Information Security Compliance Management

Marks: 100 **Lectures 60**

Objective: In view of providingtechnical superiority essentially be complimented with the appropriate compliance advancement to maintain hygiene from the point of view of cyber security.Complianceshaveincreasinglycoming up not in just financial or aviation space but also in conventional industries like manufacturing, real estate among others and hence its of tremendous importance for a cyber-security professional to have comprehensive knowledge of the most important compliances and the modus operandi from people, process and technology to get through a compliance check.

Unit I: Introduction to Information Security Management System (ISMS) - ISO/IEC 27001
Critical Appraisal of ISO 9000, Normative, regulatory and legal framework related to information security Fundamental principles of information security,ISO/IEC 27001 certification process,Information Security Management System (ISMS), detailed presentation of the clauses 4 to 8 of ISO/IEC 27001

Unit II: Planning and Initiating an ISO/IEC 27001 audit
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

Unit III: Conducting an ISO/IEC 27001 audit
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

Unit IV: Concluding and ensuring the follow-up of an ISO/IEC 27001 audit
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

Unit V: PCI DSS, HIPPA
Security Management Process, Risk Analysis Risk Management, Information System Activity Review, Assigned Security Responsibility, Authorization and/or Supervision, Termination Procedures, Access Authorization, Access Establishment and Modification, Protection from

Malicious Software, Log-in Monitoring, Password Management, Response and Reporting, Contingency Plan Evaluation, Facility Access Control and Validation Procedures, Unique User Identification, Emergency Access Procedure, Automatic Logoff Encryption and Decryption, Audit Controls, Data Integrity, Person or Entity Authentication, Integrity Controls Encryption

Unit VI Intellectual Property Rights

Intellectual Property Rights: Types and Issues related to IPR, Policy framework in India and Abroad, Bitcoin and law enforcement.

Suggested Readings:

1. Godbole, N. *Information Systems Security: Security Management, Metrics, Frameworks and Best Practices*. Wiley
2. Calder, A. (2009*). Implementing Information Security Based on ISO 27001/ISO 27002: A Management Guide* (2nd Ed.). Van Haren Publishing
3. Humphreys, E. (2007). *Implementing the ISO / IEC 27001 Information Security Management System Standard*. Artech House Publishers.
4. Watkins, S. G. (2013). *An Introduction to Information Security and ISO 27001: A Pocket Guide*. IT Governance Publishing.

Latest research papers from refereed journals discussed by the faculty may also be referred.