The Institute of Cost Accountants of India

INFORMATION SYSTEM SECURITY AUDIT

BATCH: 3 | Chapter: 1 | Day 1 TO 5

DISSA
INFORMATION SYSTEM SECURITY AUDIT

Elocutionist: Dr. Saurabh Maheshwari

PURPOSE OF THE COURSE

As we are already into Industry 4.0 and marching towards Industry 5.0, working on a real-time basis and disseminating information globally, computing devices are taking the driving seat in all organizations irrespective of their size and working nature.

More computing devices mean more digital assets, data, and technical resources… leading to more openness, more risk, and higher compliance.

An Information System Security Audit aims to establish whether information systems safeguard corporate assets, maintain the integrity of stored and communicated data, support corporate objectives effectively, and operate efficiently.

This course will equip and upskill members of ICMAI to have basic and hands-on knowledge in the file of Information System Security Audit.

WHAT IS ‘INFORMATION SYSTEM SECURITY AUDIT’?

An information Security Systems Audit is taking stock of various controls within the IT systems infrastructure. It is the process involving the collection and evaluation of evidence of the design and function of controls designed and implemented in information systems, practices, and operations.

In many countries, it is not mandatory by law to perform an information systems audit; it is mostly done as a best practice. It can be performed by any competent auditor with a recognized qualification in this field. An information systems audit can be performed independently by a competent individual capable of using tools for testing controls, aware of technical know-how & prevailing market, and keeping himself updated about the global cyber world.

Chapter - 1

OVERVIEW OF INFORMATION SYSTEM SECURITY & AUDIT

GOVERNANCE

- What is a Governance Framework?
- A good governance model will address the following concerns in an organization
  - Inappropriate Strategy for Information System
  - Laboriousness in Quantifying the Value of Informative System
  - Reviewing Existing Informative System Security Controls
  - Systems and Applications
  - Business Application Audits
  - Information Processing Facilities
  - System Development & Maintenance
  - IT and Enterprise Management Architecture
  - Uncertainly as the Major Cost of Information System
  - Performance Management System
  - Regulation and Compliance Frameworks

RISKS & SECURITY POLICY

- Risk?
- Why Risk Assessment is required:
  - Security, Privacy, and Continuity
  - Client's, Partner's, and Customer's Assurance
  - Migration
  - Network Vulnerabilities
  - Data Centre as a key IRM entity [Information Resource Management]
  - Web Application Security
- Security Policies
  - Team
  - IS Security Plan as per prevailing global frameworks and standards [CERT, ISO, DIT, etc.]
  - Periodic Review
  - Conducting VAPT [Vulnerability Assessment and Penetration Testing]
  - Audit of the actual system from all possible different angles

CONTROLS

- What are controls?
  - Internal Controls = General Controls + IS Controls [Application Controls + IT General Controls]
- Categories of Controls
  - **Deterrent Controls**: Deterrent Controls are designed to deter unauthorized people, internal as well as external, from accessing the information and information systems.
  - **Preventive Controls**: Preventive Controls prevent the cause of exposure from occurring or at least minimize the probability of the occurrence of unlawful events.
  - **Detective Controls**: When a cause of exposure has occurred, detective controls report its existence to arrest further damage or minimize the extent of the damage. Detective controls limit the losses if an unlawful event at all occurs.
  - **Corrective Controls**: Corrective Controls are designed to help the organization recover from a loss situation. Business Continuity Planning is a corrective control. Without corrective controls in place, the organization will suffer from the risk of loss of business and other losses, due to its inability to recover essential IT-based services, information, and other resources after the disaster has taken place

DATA SECURITY

- Data Input Controls
- Data Processing Controls
- Data Movement Controls
- Data Storage Controls

Let us talk about some terms related to ‘data’ and have a deeper understanding.

HOW AND IN WHAT MANNER TECHNOLOGY IS IMPLEMENTED IN ORGANIZATIONS?

- Different departments with their respective requirements and respective Information Systems
- Development, implementation, and upgradation of the team [also discuss Change Management]
- Components of any Information System
- Centralized & De-centralized System
- ITIL Framework

AUDIT IN COMPUTERIZED ENVIRONMENT

- Risk based audit

- Change in evidence collection technique
- Change in evidence evaluation technique
- Change in reporting formats

PHASES OF AUDIT

- Setting up Audit Objective
- Request for Proposal [RFP] → Response to RFP → Finalizing Auditor
- Drafting Audit Charter
- Audit Engagement Letter → Understanding Business
- Communication with Auditee
- Quality Assurance Process
- Scope of Audit
- Audit Planning
- Evidence Collection & Preservation
- Evidence Evaluation
- Audit Documentation
- Audit Report

STANDARDS OF AUDITING

- SA 200 – Describes the basic principles of the audit. these principles are applicable to IS Audit also & have to be complied with
- SA 210 – States the terms of Audit Engagements require the auditor and the client to agree on the terms of engagement and document them in the audit engagement letter. It requires that the engagement letters be renewed if necessary, before the commencement of the audit in succeeding years.
- SA 220 – States that Quality Control Systems, policies, and procedures are the responsibility of the audit firm.
- SA 250 – “Considerations of laws and regulations in conducting an Audit” mentions that the auditor has to obtain just a general understanding of the laws and regulations applicable to the organization and he should alert the management of the material non-compliances and the applicable penalties hereof, found during the engagement.
- SA 300 – Focuses on rigorous, well documented and thoughtful planning to be done before starting audit of an organization.
- SA 315 – This standard is for risk identification and assessment requires IS Auditors to assess risk that is part of the business environment and the internal control system.
- SA 320 – Is the Auditing standard for Audit Materiality. It requires the Auditor to report those items that create an impact on the financial statements and which change the decision that would be made by the stakeholder.
- SA 330 – Requires IS Auditors to review whether management has designed and implemented appropriate risk remediation measures and provide recommendations on the residual risks that have been identified as critical and are not appropriately mitigated.
- SA 530 – It deals with the auditor’s use of statistical and non-statistical sampling when designing and selecting the audit sample, performing tests of controls and tests of details, and evaluating the results from the sample. … and a few more

Two-thirds of the Earth is covered with Water and the rest one-third is covered with Auditors from different verticals evaluating the business operations from different angles.

- Dr. Saurabh Maheshwari

THANKS!

Any questions?