# System Security and Audit

IT audit and information system security services are concerned with identifying and analyzing potential risks, as well as mitigating or eliminating them, in order to keep the information system and the organization's overall operations running smoothly.

## System Audit

### The goal of IT system audit, review and assessment?

- Systematize, improve and integrate business procedures and the coverage of business information in the information system
- Identify risks and weaknesses, thus enabling the definition of solutions for introducing controls over processes supported by IT
- Accelerate the business information collection process
- Centralize the control system and eliminate bottlenecks in information flow through the IS
- Regulatory compliance
- Reduce IT-related costs, as they represent a significant proportion of the organization's total costs
- Ensure information confidentiality, integrity and availability
- Assess ERP system before and after implementation
- Align IT assessment and IT strategy
- Attain IT management standards

### Role of System Auditor

The role of the auditor begins early in the creation of a system to ensure that the final product is secure. It describes a documented idea of system utilization that aids in load planning and determining hardware and software specifications. It indicates if the computer system is being used wisely or whether it is being abused.

### Audit Considerations

Audit considerations examine the results of the analysis by using both the narratives and models to identify the problems caused due to misplaced functions, split processes or functions, broken data flows, missing data, redundant or incomplete processing, and non-addressed automation opportunities. The activities under this phase are as follows –

- Identification of the current environment problems
- Identification of problem causes
- Identification of alternative solutions
- Evaluation and feasibility analysis of each solution

- Selection and recommendation of most practical and appropriate solution
- Project cost estimation and cost benefit analysis

**Results:**

- Reliable IT controls and risk management capability
- Security information management enabled
- Improved data availability and integrity
- Improved ability to enter new markets
- Enhanced reputation
- Long-term savings
- Revenue growth

## System Security

### Security

System security refers to protecting the system from theft, unauthorized access and modifications, and accidental or unintentional damage. In computerized systems, security involves protecting all the parts of computer system which includes data, software, and hardware. Systems security includes system privacy and system integrity.

1. System privacy deals with protecting individuals systems from being accessed and used without the permission/knowledge of the concerned individuals.
2. System integrity is concerned with the quality and reliability of raw as well as processed data in the system.

### Control Measures

There are variety of control measures which can be broadly classified as follows –

Backup

- Regular backup of databases daily/weekly depending on the time criticality and size.
- Incremental back up at shorter intervals.
- Backup copies kept in safe remote location particularly necessary for disaster recovery.
- Duplicate systems run and all transactions mirrored if it is a very critical system and cannot tolerate any disruption before storing in disk.

Physical Access Control to Facilities

- Physical locks and Biometric authentication. For example, finger print.
- ID cards or entry passes being checked by security staff.
- Identification of all persons who read or modify data and logging it in a file.

Using Logical or Software Control

- Password system.
- Encrypting sensitive data/programs.
- Training employees on data care/handling and security.
- Antivirus software and Firewall protection while connected to internet.

## Risk Analysis

A risk is the possibility of losing something of value. Risk analysis starts with planning for secure system by identifying the vulnerability of system and impact of this. The plan is then made to manage the risk and cope with disaster. It is done to accesses the probability of possible disaster and their cost. Risk analysis is a teamwork of experts with different backgrounds like chemicals, human error, and process equipment. The following steps are to be followed while conducting risk analysis –

- Identification of all the components of computer system.
- Identification of all the threats and hazards that each of the components faces.
- Quantify risks i.e. assessment of loss in the case threats become reality.

**Risk management steps** –Identification of security measures

- Calculation of the cost of implementation of security measures.
- Comparison of the cost of security measures with the loss and probability of threats.
- Selection and implementation of security measures.
- Review of the implementation of security measures.