COBIT

Information Security Governance and its benefits:
Information security governance is a subset of corporate governance that provides strategic direction for security activities and ensures objectives are achieved. It ensures that information security risks are appropriately managed and enterprise information resources are used responsibly.

Benefits of IT Security Governance:

- ✓ Increased predictability and reduced uncertainty of business operations.
- ✓ Protection from the potential for civil and legal liability.
- ✓ Assurance of security policy compliance.
- ✓ Foundation for effective risk management.
- ✓ Provides a level of assurance that critical decisions are not based on faulty information.
- ✓ Accountability for safeguarding information.

COBIT is an acronym for Control Objectives for Information and related Technology. It is a framework which helps meet the multiple needs of management by bridging the gaps between business risks, control needs and technical issues. It provides a set of recommended best practices for governance and control process of information systems and technology with the essence of aligning IT with business.

Four Domains of high level classification of control objectives as identified by COBIT:

Planning and organization: This domain covers strategy and tactics, and concerns the identification of the way IT can best contribute to the achievement of the business objectives. Furthermore, the realization of the strategic vision needs to be planned, communicated and managed for different perspectives. Finally, a proper organization as well as technological infrastructure must be put in place.

Acquisition and implementation: To realize the IT strategy, IT solutions need to be identified, developed or acquired, as well as implemented and integrated into the business process. In addition, changes in and maintenance of existing systems are covered by this domain to make sure that the life cycle is continued for these systems.

Delivery and support: This domain is concerned with the actual delivery of required services, which range from traditional operations over security and continuity aspects to training. In order to deliver services, the necessary support processes must be set up.

Monitoring: This domain includes the actual processing of data by application systems, often classified under application controls. All IT processes need to be regularly assessed over time for their quality and compliance with control requirements. This domain thus addresses management's oversight of the organization's control process and independent assurance provided by internal and external audit or obtained from alternative sources.

Users	Key usage
Executive Management	To obtain value from IT investments and balance risk and control investment.
IT Management	To provide IT services that the business requires to support the business strategy in a controlled and managed way.
Users	To obtain assurance on the security and controls of IT services provided by internal or third parties.
IS Auditors	To substantiate their opinions and/or provide advice to management on internal controls.

Benefits:
Implementing COBIT as an IT governance framework helps in:

- ❖ Better alignment of IT strategy with the business strategy.
- ❖ Optimizing costs and providing the intrinsic value of IT.

- Optimal investment and proper management of critical IT resources.
- Making a clear understanding of the enterprise appetite for risk, understanding of compliance requirements, and assignment of risk management responsibilities.
- Tracking and monitoring IT strategy implementation, project completion, resource usage, process performance and service delivery.

The **critical success factors** for an **effective information security management system** include:

- A strong commitment and support by the senior management.
- Comprehensive program of formal security awareness training.
- Professional risk-based approach should be used systematically to identify sensitive and critical information resources.
- Risk assessment activities should be undertaken to mitigate unacceptable risks.
- Responsibilities and accountabilities should be clearly defined in the information security policies and procedures.

Following critical success factors may be lacking:

- Lack of top management commitment to implement controls and frequent over ride of controls.
- Management is unable to clearly define what components of the processes need to be controlled. / A properly defined IT control process framework may not be in place.
- The personnel of internal audit may be lacking in knowledge and understanding of IT related controls.
- Roles and responsibilities of the internal audit department may not be clearly defined.
- Lack of coordination between internal audit and the IT department.
- A clear process may not be in place for timely reporting of internal control deficiencies.
- Lack of relevant resources.

Key performance indicators to measure the performance of IT department and IT processes are as follows:

- Cost efficiency of IT processes (costs versus deliverables).
- Frequency and effectiveness of IT action plans for process improvement initiatives.
- Levels of utilization of IT infrastructure.
- Availability of relevant knowledge and information.
- System downtime.
- Throughput and response times.
- Number of errors and rework.
- Number of non-compliance reporting.
- Development and processing time.
- Satisfaction of IT users and stakeholders (surveys and number of complaints).

Key Performance indicators in:

Project performance

- Ratio of projects completed on time.
- Ratio of projects completed within budget.
- Ratio of projects meeting functionality requirements. / Users' satisfaction rating.

IT operational support

- Average time taken to respond to customers' complaints.
- Ratio of number of problem reported and resolved/unresolved.
- Percentage of customers' satisfaction over support services. (through survey form)

IT infrastructure availability

- Number of system downtime (per unit time i.e. per hour, per day, per week etc.)
- Mean time between failures.
- Number of customers' complaints about non-availability of online facilities.

IT security environment

- Percent increase/decrease in security breaches/incidents reported.
- Mean time to resolve critical security issues.
- Level of customers' awareness of risks and controls. (through survey form)