*Information System Audit

In today's banking environment, most of the banks are using automated systems to support their business process; therefore, any risk associated with technology may ultimately become a business risk. IS audit function should provide assurance on technology infrastructure, application and associated internal control framework by assessing computerized information system's functionality, efficiency and security through risk assessment, internal control evaluation and detailed testing of associated data.

IS auditing is the process of collecting and evaluating evidence to determine whether information systems, related resources and the environment adequately safeguard assets, maintain data and system integrity, provide relevant and reliable information, achieve organizational/information system goals effectively, consume resources efficiently, and have in effect internal controls that provide reasonable assurance that operational & control objectives will be met, undesired events will be prevented or detected & rectified in a timely manner. The overall objective of an IS Audit is to ensure control maximization and risk mitigation.

***The Internal Audit's role in relation to I.S. Audit** may involve**:**

- Planning and conducting IS audits on continuous basis as an independent entity according to well-established & globally recognized audit standards and guidelines.
- Evaluating the IS Strategic Plan of bank/DFI and Alignment with the Business Objectives.
- Evaluating the IS Organizational Structure and Management.
- Evaluating the IS Policies, Standards, Procedures and Business processes.
- Ensuring IT is included in the audit universe and annual plan (selecting topics).
- Ensuring IT risks are considered when assigning resources and priorities to audit activities.
- Ensuring the existence of well-defined I. S. Audit Manual.
- Defining IT resources needed by the internal audit department, including specialized training of audit staff.
- Ensuring that audit planning considers IT issues for each audit.
- Liaising with audit clients to determine what they want or need to know.
- Developing & Performing Risk-based IS Audit.
- Reviewing and Evaluating the IT (Hardware, Software, Networking etc.) Acquisition process, Installation reports of individual systems or part of the system or complete system as a whole, Maintenance and Service level agreements and technology Infrastructure.
- Determining what constitutes reliable and verifiable evidence and obtaining sufficient, reliable, relevant and useful evidence to achieve the audit objectives.
- Evaluating Business Application Systems Development, Acquisition, Implementation, and Maintenance.
- Performing IT enterprise-level controls audits.
- Performing IT general controls audits.
- Performing IT applications controls audits.
- Performing specialist technical IT controls audits.

* The points listed are for general reference purpose and internal audit of information systems should not be restricted to them only.

- Evaluating the effectiveness of Disaster Recovery and Business Continuity plan.
- Making effective and efficient use of automated computer based audit techniques to assist the audit processes.
- During systems development or analysis activities, operating as Independent experts who understand how controls can be implemented & circumvented and provide opinion on the strength of controls.
- Helping to monitor and verify the proper implementation of activities that minimize all known and documented IT risks.
- Advising the audit committee and senior management on IT internal control issues and audit report to suggest controls and further improvements.

****

* The points listed are for general reference purpose and internal audit of information systems should not be restricted to them only.