IT Audit : Learn, look, leap forward and grow steadily

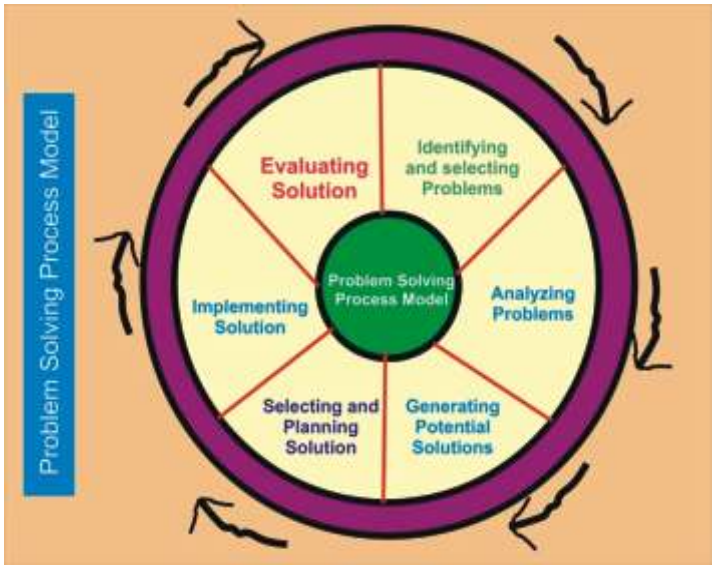
IT Governance expects to leverage technology as a competitive advantage to streamline and solve business problems and create agility and opportunities. But, at the same time it is also expecting to deliver these capabilities with smaller budgets and fewer resources. In fact, what experience has shown is that when organizations suffer loss or any compromise or any security breach, it is due to a missing control i.e. a preventive or detective or reactive.

Rajiv Ranjan,
Principal Systems Analyst, Patna
rajiv.ranjan@nic.in

The usual outcry after a loss is to rush and protect. In today's management term it is called as "fire fighting approach". Compromise can make a good umbrella but with a poor roof. The solution lies in managing the system by setting of planned and systematic activities that ensures conformance to requirements, standards and procedures.

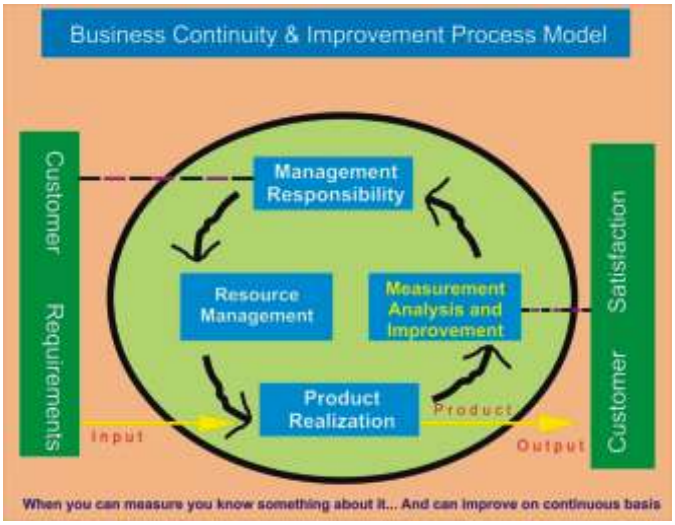
An IT Audit Review is the process of collecting and evaluating evidence of information systems, practices and operations. It evaluates and determines whether the information systems are safeguarding assets, maintaining data integrity, and operating effectively to achieve the organization's goals and objectives. The main objective of IT audit has been to look into the availability, confidentiality and integrity aspects of the information system. It is a monitoring or feedback mechanism rather a "fault finding mission".

The audit review highlights and pin-points about the organization's computer systems available for the business at all times when required; and that the information in the systems is disclosed only to the authorized users. IT Audit focuses on determining the risks and the assessment of the controls to mitigate these risks. It verifies whether IT management has developed an organizational structure and procedures to ensure a controlled and efficient environment for information processing. And, the systems and applications are adequately controlled to ensure valid, reliable, timely, and secure input, processing, and output at all levels of a system's activity.



The controls can be protective, detective and reactive. Protective or preventive controls serve to proactively define and enforce acceptable behaviors. Any control that performs a monitoring activity can likely be defined as a detective control. It also detects the deficiency i.e. some control of protective or preventive control somewhere has failed. Reactive or corrective controls typically work in response to a detective control.

With the increasing use and faster growth of e-governance initiatives, IT systems and applications have pervaded in government departments and are making them in use to leverage the technology. The scope for IT Audit has come in way for evaluation of controls and the effectiveness of IT systems investment in achieving organizational objectives and monitoring activities. This can surely help in understanding backward (what have been done?) and moving forward (what more needs to be done to mitigate the risks involved?) in improving the IT system.



The broader processes w.r.t Information Technology Audit has been the Planning, Studying & Evaluating Controls, Testing & Evaluating Controls, Reporting and Follow-up. The audit review tries to highlights about department's IT policy, about correctness and reliability of data captured in the system, about the adequacy of controls w.r.t input, process and output. Moreover it also evaluates whether relevant business rules have been duly incorporated in the application software. The audit review also evaluates the application of suitable security controls, business continuity plans and internal control and monitoring mechanism.

Audit findings arising from the review highlights the problem areas e.g. inadequacy of users' requirements specifications, training usage, IT systems acquisition and its implementation, security policy, application control, validation checks, internal controls etc. The review gives the insights of non-compliance, missing controls and risks involved in the implementation of IT system. The identification of problems gives the scope for improvement. The corrective measures can help to mitigate the risks and improve the system as a whole to benefit the organization.

IT governance is about adopting and adapting industry standards to improve business alignment, address compliance requirements, manage and preserve assets and provide technology services that can help the organization meet its business goals and objectives. This necessitates designing of controls for better management of technology risks for the improved and perceivable visibility of effective compliance and risks management.

The biggest challenge lies in the management and monitoring the various processes. The processes are quite complex, resource-intensive and time-consuming. They also involve managing frequently changing organizational structure and keeping pace with the changing business and partner relationship to assess risks. Moreover managing multiple process areas viz. policies, procedures, controls and frameworks to keep projects on track and comply the legal and regulatory requirements is another big challenge.

Overall the challenge is not only to retain the stimulus of e-governance but also making a graduated shift to adopt a single framework for managing controls and standards; application of simultaneous and consistent process across multiple regulatory, legal and audit requirements; reduction in duplication of effort to unify multiple silos and fulfill internal and external compliance requirements and ensure the visibility of core processes across the enterprise and driving down the implementation costs. Guidelines and compliance matrix for Indian Government website is one of the good examples of designing of controls for their compliance. The challenges lies in its implementation is to enhance the usability and functionality. Let the learnings coming through internal and external audit make us understand and look forward to address these challenges to grow an IT system progressively and steadily. *i*