Corporate leaders across the world are focusing on the implementation of corporate governance through measures that will strengthen internal checks and balances and, ultimately, corporate accountability. Regulatory requirements require senior management and business process owners not only to establish and maintain an adequate internal control structure, but also to assess its effectiveness on an annual basis. Senior management has also recognized the need to implement internal control systems and have them reviewed periodically to ensure not only conformance but also performance.

What is IS audit

Information systems (IS) audit refers to any audit that encompasses wholly or partly the review and evaluation of automated information processing systems, related nonautomated processes and the interfaces among them. IS auditors are expected to provide assurance on the internal control systems implemented through information technology. IS audit, as part of the overall audit process, is one of the facilitators for good corporate governance.

IS audit is fundamentally about how information technology is deployed to meet user requirements for information. The processes involved in planning the management of the IS function and the management issues faced in a modern IS department. The techniques used by management and the support tools and frameworks are examined with respect to the need for control within the process. Management, strategic planning, management issues, support tools and frameworks, and governance techniques.

Information systems need to be planned, acquired and developed to deliver the required information services. Securing information systems is the key to protecting information assets. IS auditors are expected to have an understanding of how information is protected and the techniques required to evaluate the availability, adequacy and appropriateness of the controls that protect information assets.

IT is critical

The critical dependency on information available in the information technology deployed and the

related risks make it imperative to have appropriate disaster recovery procedures that are part of a comprehensive business continuity plan. The need for, and techniques utilized in, the protection of IT architecture and assets through both disaster recovery planning and the transfer of risks by utilizing the appropriate insurance profile.

What we will do

IS auditing has been continuously evolving with advances in IT deployment and business practices. The requirements of technology knowledge and skill sets for IS auditors have increased but we have updated expertise and/or expert network capable to handle almost all technologies. We can cover all audit requirements from IT management and services, IT governance and IT processes to specialized areas like: auditing internet banking systems, web applications, complex applications and ERP's, e-commerce systems, electronic payments systems, auditing UNIX and Linux, auditing CISCO and networks, auditing Windows, foiling the system hackers, and investigating IT fraud.

Risk based approach

In a risk based audit approach, we are not just relying on risk. We are also relying on internal and operational controls as well as knowledge of the organisation. This type of risk assessment decision can help us relate the cost - benefit analysis of the controls to the known risk, allowing efficient choices.

By understanding the nature of the business, we can identify and categorise the types of risks that will better determine the risk model or approach used in conducting the review. The risk assessment model is an unique method developed by Blue Lab Consulting. Risk assessment is a scheme where risks have been given elaborate weights based on the nature of the business or the significance of the risk.