Information system audit in indian banks

Finance

Information itself is an important asset in today’s business. If information is lost, modified, misused huge loss can occur to business. Hence information security becomes important for any business. Information system in business including that of banking is becomingtechnologyoriented. Computers are being used in all the areas of business including that of financial accounting. Internal controls used in a Computerized Information System (CIS)environmentshould aim at information security also. This aspect of internal control is mostly overlooked in a Financial Audit where evidence collection and evaluation is more important.

Audit provides the assurance to stakeholders of business. Assurance provided by a financial audit is about financial statements, which are relied upon and based on which decisions are taken by many stakeholders. However there are risks associated in any business, which is not highlighted in a financial audit. Operational Risk and Audit For example Basel II Accord mentions of ‘ operational risks’ that are due tofailureof system, process, procedure and human action/inaction (fraud) and legal restrictions, etc. in the operation of banks, some of which are not dealt in financial audit.

The Basle committee has identified people, processes, systems and external events, as potential hazards for operations. Inadequacy and failure of any of them can result into events, which cause losses. Every business has to identify events of their relevance. The events may be similar in the same industry, but vary from an organization to organization. The whole exercise of the operational risk management is to identify potential events, which are likely to cause losses.

Here is a list of some of the events, which could lead to operational risk (non exhaustive): Technology error Fraud and theft Legal, Regulatory non compliance, Transaction risk Processes, people and systems are closely linked with information systems. Even measurement and recognition of external events need information systems. Therefore, under the new Accord, the job of an audit and control practitioner shall become more onerous and challenging. Therefore a financial audit cannot assure that the information system is foolproof as financial auditor is not expert in information technology. Hence an expert should provide an opinion that information system is risk-free. This is where Information System Audit (IS Audit) comes into picture.

Meaning of IS audit Information systems audit is a part of the overall audit process, which is one of the facilitators for good corporate governance. While there is no single universal definition of IS audit, Ron Weber has defined it as " the process of collecting and evaluating evidence to determine whether a computer system (information system) Safeguards assets Maintains data integrity Achieves organizationalgoalseffectively and Consumes resources efficiently. " Key Challenge in IS Audit IS audit often involves finding and recording observations that are highly technical.

Such technical depth is required to perform effective IS audits. At the same time it is necessary to translate audit findings into vulnerabilities and businesses impacts to which operating managers and senior management can relate. Therein lies a main challenge of IS audit. Scope of IS Audit IS auditing is an integral part of the audit function because it " supports the auditor's judgment on the quality of the information processed by computer

systems. " Initially, auditors with IS audit skills are viewed as the technological resource for the audit staff. The audit staff often looks o them for technical assistance.

Within IS auditing there are many types of audit needs, such as Organizational IS audits (management control over information technology), Technical IS audits (infrastructure, data centers, datacommunication), Application IS audit (business/financial/operational), Development/implementation IS audits (specification/ requirements, design, development and post-implementation phases) Compliance IS audits involving national or international standards. The IS auditor’s role has evolved to provide assurance that adequate and appropriate controls are place.

Of course, theresponsibilityfor ensuring that adequate internal controls are in place rests with management. Audit’s primary role, except in areas of management advisory services, is to provide a statement of assurance as to whether adequate and reliable internal controls are in place and are operating in an efficient and effective manner. So, whereas management is to ensure, auditors are to assure. The breadth and depth of knowledge required to audit information technology and systems is extensive.

For example, IS auditing involves the: pplication of risk-oriented audit approaches use of computer assisted audit tools and techniques(CAATs) application of standards (national or international) such as ISO-9000/3 to improve and implement quality systems in software development understanding of business roles and expectations in the auditing of systems

under development as well as the purchase of software packaging and project management Evaluation of complex Systems Development Life Cycle (SDLC) or new development techniques (e. g. , prototyping, end-user computing, rapid systems or application development).

Evaluation of complex technologies and communications protocols involves electronic data interchange, client servers, local and wide area networks, data communications, telecommunications and integrated voice/data/video systems. Elements/components of IS Audit An information system is not just a computer. Today's information systems are complex and have many components that piece together to make a business solution. Assurances about an information system can be obtained only if all the components are evaluated and secured. The proverbial weakest link is the total strength of the chain.

The major elements of IS audit can be broadly classified: Physical and environmental review--This includes physical security, power supply, air conditioning, humidity control and other environmental factors. System administration review--This includes security review of the operating systems, database management systems, all system administration procedures and compliance. Application software review--The business application could be payroll, invoicing, a web-based customer order processing system or an enterprise resource planning system that actually runs the business.

Review of such application software includes access control and authorizations, validations, error and exception handling, business process

flows within the application software and complementary manual controls and procedures. Additionally, a review of the system development lifecycle should be completed. Network security review--Review of internal and external connections to the system, perimeter security, firewall review, router access control lists, port scanning and intrusion detection are some typical areas of coverage.

Business continuity review--This includes existence and maintenance of fault tolerant and redundant hardware, backup procedures and storage, and documented and tested disaster recovery/business continuity plan. Data integrity review--The purpose of this is scrutiny of live data to verify adequacy of controls and impact of weaknesses, as noticed from any of the above reviews. Such substantive testing can be done using generalized audit software (e. g. , computer assisted audit techniques).

It is important to understand that each audit may consist of these elements in varying measures; some audits may scrutinize only one of these elements or drop some of these elements. While the fact remains that it is necessary to do all of them, it is not mandatory to do all of them in one assignment. The skill sets required for each of these are different. The results of each audit need to be seen in relation to the other. This will enable the auditor and management to get the total view of the issues and problems. This overview is critical.