System Control Audit

CA Diwakar Jha
on 22 February 2017

Introduction:

Information Systems have become an integral part of our day-to-day life. From Morning till evening, all humans interact with systems, in one form or another. The increased usage of technology has its pitfalls. Organizations need to rely more on technology for their day to day jobs.

As the usage of technology and information system is increasing, associated risk with technology is also imposing several threats to the information systems. More and more use of technology and the increased instances has made it imperative for organizations to place proper controls.

As a part of compliance, an auditor evaluates the existence effectiveness and continued effectiveness of internal controls.

Need for Control and Audit of Information Systems: A control is a system that prevents, detects or corrects unlawful events.

Factors influencing an organization toward control and audit of computers and the impact of the information systems audit function on organizations are depicted below:

- **Organizational cost of data loss:** Data is a critical resource of an organization for its present and future process and its ability to adapt and survive in a changing environment.
- **Incorrect decision making:** Management and operational controls taken by managers involve direction, investigations and correction of out-of-control processes.
Cost of computer abuse: Unauthorized access to computer systems can lead to destruction of assets (hardware, software, documentation etc.)

Value of computer hardware, software & personnel: These are critical resources of an organization which has a credible impact on its infrastructure and business competitiveness.

High costs of computer error: In a computerized enterprise environment where many critical business processes are performed a data error in the entry or process would cause great damage.

Maintenance of privacy: The data were also collected before computers but now there is a fear that privacy has eroded beyond acceptable limits.

Controlled evolution of computer use: Technology use and reliability of complex computer systems cannot be guaranteed and consequences can be destructive.

Effects of computer system on Audit:

To cope up with the new technology usage in an enterprise, the auditor should be competent to provide independent evaluation as to whether the business process activities are recorded and reported according to established standards or criteria.

Two basic functions carried out to examine these changes are:

1. Changes to evidence collection:
   - Data retention and storage: Client’s storage capacity may restrict the amount of historical data retained online & readily accessible to the auditor.
   - Absence of input documents: Most of the online & system generated transactions happen without the use of any input resulting change in audit trail.
   - Non-availability of audit trail: In computer system audit trail may not exist or exists for short time.
   - Lack of availability of output: The transactions processed may not produce printed hardcopy output.
   - Audit evidence: Certain transactions which are generated automatically may not have audit evidences.
   - Legal issues: With increase in trading over internet, creates problems with contract like legal jurisdiction of contract, parties to contract etc.

2. Changes to evidence evaluation:
   - System generated transactions: They do not provide any vision to users when they are processed. They may lead to new sources of error.
   - Automatic transaction processing: It may cause problem for auditor, e.g. in case of JIT, if stock level falls below certain units, system automatically generates purchase order & send it to supplier without authorization from manager.
   - Systemic error: It means if computer program is wrong, it will continuously give wrong output till it is connected.
The Information System Audit: It is the process of assessment of internal controls within IS environment and attesting following objectives:

**Asset safeguarding:** The information system assets must be safeguarded to provide confidentiality, integrity and availability.

**Data integrity:** It is a fundamental attribute of IS auditing. The importance to maintain integrity of data of an organization depends on the value of information.

**System effectiveness:** Effectiveness of a system is evaluated by auditing the characteristics and objective of the system to meet substantial requirements.

**System efficiency:** To optimize the use of various information system resources along with the impact on its computing environment.

The set of skills expected from an Information System auditor include:

- Sound **knowledge of business** operations, practices and compliance requirements,
- Requisite **professional/technical qualification** and certifications,
- Good understanding of information **risk & controls**, 
- Knowledge of **IT strategies**, policy and procedure controls, 
- Ability to understand **technical and manual controls**, 
- Good knowledge of **professional standards and best practices**.

Functions of Information System auditor:

IS auditor often is the assessor of business risk, as it relates to the use of IT, to management. IT auditors review relating to IT systems and processes, some of them are:

- **Inadequate information security** e.g. no or outdated antivirus, no or weak password etc.
• **Inefficient use of corporate resources** e.g. huge spending on high power servers which were not required.
• **Ineffective IT strategies, policies & practices** e.g. lack of internet usage policy & security policies.
• **IT-related frauds** e.g. phishing, hacking etc.

**Categories of Information System audits:**

Information System audits have been categorized into five parts:

- **System and applications:** Systems & applications are appropriate and adequately controlled to ensure valid, reliable, timely & secure input, process & output.
- **Information processing facilities:** Facility must be controlled to ensure timely, accurate & efficient processing under normal and disruptive conditions.
- **System development:** To ensure that system under development meets organization's objective & is developed according to generally accepted standards.
- **Management of IT and enterprise architecture:** IT management has organization structure & procedure to ensure controlled & efficient environment for information processing.
- **Telecommunications, intranets and extranets:** To ensure controls are in place on client, server & networking connecting client & server.

**Steps in Information System audit:**

Information System audit can be categorized into six stages:

- **Scoping and pre-audit survey:** Auditor determines main area of focus & out of focus based on risk based assessment.
- **Planning and preparation:** It involves generation of audit work plan & risk control matrix.
- **Fieldwork:** Gathering evidencing by interviewing staff & managers, reviewing documents and observing processes.
- **Analysis:** It involves reviewing & trying to make sense of all evidences gathered.
- **Reporting:** Reporting to the management after analysis of data.
- **Closure:** It involves preparing notes for future audits.

**Audit Standards and Best Practices:**

Information System auditors need guidance and a yardstick to measure the 3E's (Economy, Efficiency and Effectiveness) of a system.

Several well known organizations have given practical and useful information on Information System audit, which are given as follows:

**Information System Audit and Control Association (ISACA):** It is a global leader in governance, security audit & control. To assist IT auditors, it has issued 16 auditing standards, 39 guidelines to apply standards, 11 IS auditing...
procedures and COBIT for best business practices relating to IT.

**ISO 27001**: International best practice, certification standards & foundation for ISMS. It defines how to organize information security in any organization.

**Internal Audit Standards**: IIA is a professional association. It provides dynamic leadership for internal auditing. IIA issued Global Technology Audit Guide.

**Standards on Internal Audit issued by ICAI**: It has issued various standards which highlights process to be adopted by internal auditor in specific situation.

**Information Technology Infrastructure Library**: It is a set of practice for ITSM. It focuses on aligning IT with the needs of business. It describes procedures, task & checklist which are not organization specific for establishing minimum level of competency.

**Concurrent or Continuous Audit**: Today, organizations produce information on a real-time, online basis. Real-time recordings needs real-time auditing to provide continuous assurance about the quality of the data, thus, continuous auditing. Continuous auditing enables auditors to significantly reduce and perhaps eliminate the time between occurrence of the client's events and the auditor's assurance services thereon.

**Types of Audit tools:**

**Snapshots**: It examines the way the transactions are processed. Selected transactions are marked with special code that triggers snapshot process. Audit module records the transactions before & after processing.

**Integrated Test Facility (ITF)**: It involves creation of dummy entity in the application system & to audit the processing of test data entered in dummy entity.

**System Control Audit Review File (SCARF)**: It involves embedding audit software module within host application to provide continuous monitoring of transactions. SCARF is like snapshot with data collection capability.

**Continuous and Intermittent Simulation (CIS)**: It examines the transactions that updates the database. It independently process the data, records the result & compare them with those obtained by DBMS.

**Audit Hooks**: It is used to flag the suspicious transactions. Auditor is informed of questionable transactions as they occur via real time notification.

**Advantages of CAT**

- Timely, comprehensive and detailed auditing
- Surprise test capability
- Information to system staff on meeting of objectives
• Training for new users

Audit Trails:

Audit trails are used as detective controls which help to accomplish security policy. Audit trails are log that can be designed to record the user activities on system and application.

Objectives of Audit Trails:

• Detecting unauthorized access to system
• Reconstruction of events
• Personal accountability

COSO Framework:

• Control environment: For each business process, an organization needs to develop a control environment including criticality & materiality of each business process.
• Risk assessment: Each business process comes with various risks. A control environment must include an assessment of risks associated with each business process.
• Control activities: Control activities must be developed to manage, mitigate & reduce the risk associated with each business process as it is unrealistic to expect to eliminate risk.
• Information and communication: Control activities are associated with information & communication systems as these systems enable an organization to capture & exchange the information to conduct, manage & control its business operations.
• Monitoring: Internal control process must be continuously monitored with modifications made as warranted by changing conditions.

Layers of security policy and audit:

Strategic Layer: At this layer, the top management takes action, in form of drawing up security policy, security training, security guidelines.

Tactical Layer: At the tactical layer, security administration is put in place.

Operational Layer: The operational layer audit issues include:

• User accounts and access rights
• Password controls
• Segregation of duties

Conclusion:
By seeing around the world, it can be clearly understood that information is blood of a business. To run business for unforeseen future, protection of information and data is very critical. And that's why organizations are expending major chunk of their budget to ensure security of information and data. It is also necessary to gain the trust of stakeholders.

In short, information lost means business gone, so, information must be protected with due and reasonable care.

Recommended Read

- GST Audit - An overview
- GST annual figures for 2018-19 to be reported in Cost Records/ Cost Audit Annexures/ Reports

Be the first to leave a comment.

Your are not logged in . Please login to post comments.

Click here to Login / Register

Related Articles

- Analysis & suggested answers of May 19 CA Final Audit (New Syllabus)
- GST Audit Check list for Composition Taxpayer
- GST Audit - Press Note/ Circular on Annual Return 3rd July - Analysed
- UDIN: Advanced idea to control malpractices
- The importance of risk based internal audit in banks
- Essence of Tax Audit vis-a-vis Revenue
- New return filing system under GST
- Dahi Handi of GST Annual Return and GST Audit

Other Latest Articles

- Independent Directors in Corporate Board - A reality check
- HC: Department can recover GST dues against Chronic Defaulting Assessee
- FAQ by NIC on Blocking of EWay Bill Facility
- Detailed analysis of outcomes of 38th GST Council Meeting
- Proportionate disallowance of interest paid on unsecured loan given to third party
- Highlights of the pre-budget memorandum 2020 submitted by ICAI