Auditing of Information Systems:

6.2.1 Need for Audit of Information Systems

Factors influencing an organization toward controls and audit of computers and the impact of the information systems audit function on organizations are depicted in the Fig. 6.2.1.

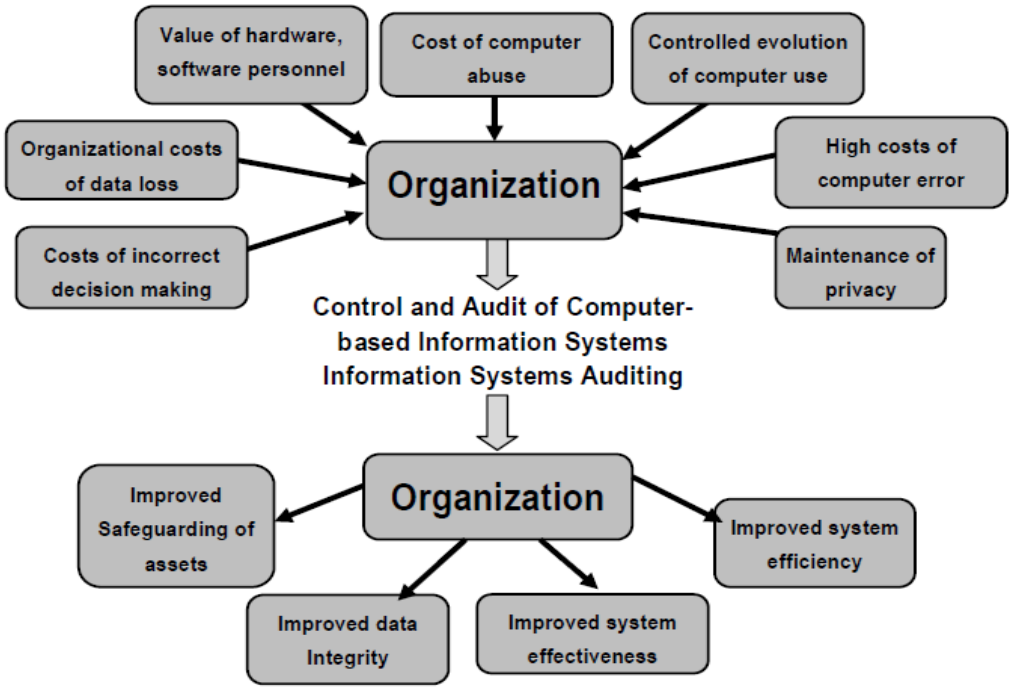

Fig. 6.2.1: Impact of Controls and Audit influencing an Organization

(i) Changes to Evidence Collection: Existence of an audit trail is a key financial audit requirement; since without an audit trail, the auditor may have extreme difficulty in gathering sufficient, appropriate audit evidence to validate the figures in the client's accounts. The performance of evidence collection and understanding the reliability of controls involves issues like-

- **Data retention and storage**: A client's storage capabilities may restrict the amount of historical data that can be retained "on-line" and readily accessible to the auditor. If the client has insufficient data retention capacities, the auditor may not be able to review a whole reporting period transactions on the computer system. For example, the client's computer system may save data on detachable storage device by summarising transactions into monthly, weekly or period end balances.
- **Absence of input documents**: Transaction data may be entered into the computer directly without the presence of supporting documentation e.g. input of telephone orders into a telesales system. The increasing use of Electronic Data Interchange (EDI) will result in less paperwork being available for audit examination.

- **Non-availability of audit trail**: The audit trails in some computer systems may exist for only a short period of time. The absence of an audit trail will make the auditor's job very difficult and may call for an audit approach which involves auditing around the computer system by seeking other sources of evidence to provide assurance that the computer input has been correctly processed and output.
- **Lack of availability of printed output**: The results of transaction processing may not produce a hard copy form of output, i.e. a printed record. In the absence of physical output, it may be necessary for an auditor to directly access the electronic data retained on the client's computer. This is normally achieved by having the client provide a computer terminal and being granted "read" access to the required data files.
- **Audit evidence**: Certain transactions may be generated automatically by the computer system. For example, a fixed asset system may automatically calculate depreciation on assets at the end of each calendar month. The depreciation charge may be automatically transferred (journalised) from the fixed assets register to the depreciation account and hence to the client's income and expenditure account.

Legal issues: The use of computers to carry out trading activities is also increasing. More organisations in both the public and private sector intend to make use of EDI and electronic trading over the Internet. This can create problems with contracts, e.g. when is the contract made, where is it made (legal jurisdiction), what are the terms of the contract and are the parties to the contract.

(ii) **Changes to Evidence Evaluation**: Evaluation of audit trail and evidence is to trace consequences of control's strength and weakness throughout the system.

- **System generated transactions**: Financial systems may have the ability to initiate, approve and record financial transactions.
- **Automated transaction processing** systems can cause the auditor problems. For example when gaining assurance that a transaction was properly authorised or in accordance with delegated authorities. *Automated transaction generation* systems are frequently used in 'just in time' (JIT) inventory and stock control systems : When a stock level falls below a certain number, the system automatically generates a purchase order and sends it to the supplier (perhaps using EDI technology)
- **Systemic Error**: Computers are designed to carry out processing on a consistent basis. Given the same inputs and programming, they invariably produce the same output. This consistency can be viewed in both a positive and a negative manner.

3) Explain set of skill that are generally expected for IS auditor?

ANSWER:

The set of skills that is generally expected to be with an IS auditor include

1. **Sound knowledge** of business operations, practices and compliance requirements;
2. Should possess the **requisite professional technical qualification** and certifications;
3. A **good understanding** of information **Risks and Controls**
4. **Knowledge of IT strategies**, policy and procedural controls;
5. Ability to **understand technical and manual controls** relating to business continuity; and
6. Good **knowledge of Professional Standards and Best Practices of IT controls** and security.

Therefore, the audit process begins by defining the scope and objectives to adapt the standards and benchmarks for developing information model for collecting and evaluating evidence to execute the audit.

4)Functions of IS Auditor:

IS Auditor often is the assessor of business risk, as it relates to the use of IT, to management, The auditor can check the technicalities well enough to understand the risk (not necessarily manage the technology) and make a sound assessment and present risk-oriented advice to management. IS Auditors review risks relating to IT systems and processes; some of them are:

- **Inadequate information security controls** (e.g. *missing or out of date antivirus controls, open ports, open systems without password or weak passwords etc.)*
- **Inefficient use of resources, or poor governance** (e.g. huge spending on unnecessary IT projects like printing resources, storage devices, high power servers and workstations etc.)
- **Ineffective IT strategies, policies and practices** (including a lack of policy for use of Information and Communication Technology (ICT) resources, Internet usage policies, Security practices etc.)
- **IT-related frauds** (including phishing, hacking etc)

5) EXPLAIN MAJOR TYPES OF IS AUDIT?

(MISTS)

Information Systems Audits has been categorized into five types:

1. ***Management of IT and Enterprise Architecture:***
   An audit to verify that IT management has developed an **organizational structure and procedures to ensure a controlled** and efficient environment for information processing.
2. ***Information Processing Facilities:***
   An audit to verify that the **processing facility is controlled to ensure timely, accurate,** and efficient processing of applications under normal and potentially disruptive conditions
3. ***Systems and Application:***
   An audit to verify that **systems and applications are appropriate, are efficient, and are adequately** controlled to ensure valid, reliable, timely, and secure input, processing, and output at all levels of a system's activity.
4. ***Telecommunications, Intranets, and Extranets:***
   An audit to verify that **controls are in place on the client** (end point device), server, and on the network connecting the clients and servers.
5. ***Systems Development:***
   An audit to verify that the systems under development meet the objectives of the organization and to ensure that the **systems are developed in accordance with generally accepted standards** for systems development.

6) EXPLAIN MAJOR STAGES OF IS AUDIT?

Answer ***SPF-ARC***

Scoping and pre-audit survey:

Auditors determine the ***main area/s of focus*** and any areas that are explicitly out-of-scope, based on the scope-definitions agreed with management. Information sources at this stage include background reading and web browsing, previous audit reports, pre audit interview, observations and, sometimes, subjective impressions that simply deserve further investigation.

Planning and preparation:

During which the scope is broken down into greater levels of detail, usually involving the generation of an audit work plan or risk-control-matrix.

Fieldwork:

This step involves **gathering of evidence by interviewing staff and managers, reviewing documents, and observing processes etc**.

Analysis:

This step involves desperately sorting out, reviewing and trying to make sense of all that evidence gathered earlier. ***SWOT (Strengths, Weaknesses, Opportunities, and Threats***) or ***PEST (Political, Economic, Social, Technological) techniques*** can be used for analysis.

Reporting:

Reporting to the management is done after analysis of evidence is gathered and analyzed.

Closure:

Closure involves preparing notes for future audits and follow up with management to complete the actions they promised after previous audits

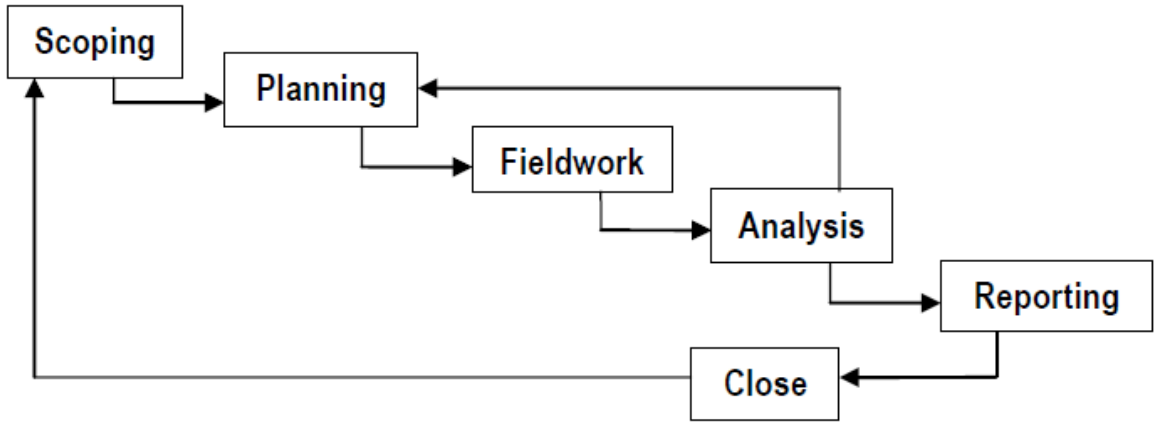

Fig. 6.3.1: Steps in IS Audit process

Types of Audit Tools:

Snapshots:
Integrated Test Facility (ITF):
System Control Audit Review File (SCARF):
Continuous and Intermittent Simulation (CIS):
Audit Hooks:

7) Snap shots

Tracing a transaction is a computerized system can be performed with help of snapshots or extended records. The snapshot software is built into the system at those points where material processing occurs which ***takes images of the flow*** of any transaction as it moves through the application. These images can be utilized to assess the **authenticity, accuracy, and completeness of the processing** carried out on the transaction.

8) Integrated Test Facility (ITF):

The ITF technique **involves the creation of a dummy entity in the application system files** and **the processing of audit test data against the entity as a means of verifying**

processing authenticity, accuracy, and completeness. This test data would be included with the normal production data used as input to the application system. In such cases the auditor has to decide what would be the method to be used to enter test data and the methodology for removal of the effects of the ITF transactions.

9) System Control Audit Review File (SCARF):

Uses the **embedded audit module to continuously monitor the transaction activity** and collect data on transaction for audit purpose. Such **data are recorded in SCARF FILE**. The transactions that are recorded include those that exceed specified limit say amount. Periodically auditor review the data collected in scarf

Auditors might use SCARF to collect the following types of information:

- **Application System Errors** - SCARF audit routines provide an independent check on the quality of system processing, whether there are any design and programming errors as well as errors that could creep into the system when it is modified and maintained.
- **Policy and Procedural Variances** - Organizations have to adhere to the policies, procedures and standards of the organization and the industry to which they belong. SCARF audit routines can be used to check when variations from these policies, procedures and standards have occurred.
- **System Exception** - SCARF can be used to monitor different types of application system exceptions. For example, salespersons might be given some leeway in the prices they charge to customers. SCARF can be used to see how frequently salespersons override the standard price.
- **Statistical Sample** -Some embedded audit routines might be statistical sampling routines, SCARF provides a convenient way of collecting all the sample information together on one file and use analytical review tools thereon.
- **Snapshots and Extended Records** - Snapshots and extended records can be written into the SCARF file and printed when required.
- **Profiling Data** - Auditors can use embedded audit routines to collect data to build profiles of system users. Deviations from these profiles indicate that there may be some errors or irregularities.
- **Performance Measurement** - Auditors can use embedded routines to collect data that is useful for measuring or improving the performance of an application system.

10)Audit Hooks:

There are audit routines that **flag suspicious transactions**. For example, internal auditors at **Insurance Company** determined that their policyholder system was vulnerable to fraud every time **a policyholder changed his or her name or address and then**

subsequently withdrew funds from the policy. They devised a system of audit hooks to tag records with a name or address change. The internal audit department will investigate these tagged records for detecting fraud. When audit hooks are employed, **auditors can be informed of questionable transactions as soon as they occur.** This approach of **real-time notification displays a message on the auditor's terminal.**

Continuous and Intermittent Simulation (CIS):

This is a variation of the SCARF continuous audit technique. This technique can be used to trap exceptions whenever the application system uses a database management system.

11) Discuss the major advantages of continuous audit techniques. **SITT**

Answer:

Some of the advantages of continuous audit techniques are given as under:

- **Timely, Comprehensive and Detailed Auditing** – Evidence would be available more timely and in a comprehensive manner. The entire processing can be evaluated and analyzed rather than examining the inputs and the outputs only.
- **Surprise test capability** – As evidences are collected from the system itself by using continuous audit techniques, auditors can gather evidence without the systems staff and application system users being aware that evidence is being collected at that particular moment. This brings in the surprise test advantages.
- **Information to system staff on meeting of objectives** - Continuous audit techniques provides information to systems staff regarding the test vehicle to be used in evaluating whether an application system meets the objectives of asset safeguarding, data integrity, effectiveness, and efficiency.
- **Training for new users** – Using the ITFs, new users can submit data to the application system, and obtain feedback on any mistakes they make via the system's error reports.

12) Discuss major disadvantages of continuous audit techniques.

Answer:

The following are some of the disadvantages and limitations of the use of the continuous audit system:

- **Auditors need the knowledge and experience of working with computer systems** to be able to use continuous audit techniques effectively and efficiently.
- Continuous audit techniques are more likely to be used if **auditors are involved in the development work associated with a new application system**

- Continuous auditing techniques are more likely to be used where the **audit trail is less visible and the costs of errors and irregularities are high**.
- Continuous audit techniques are **unlikely to be effective unless they are implemented in an application system that is relatively stable**
- ***Auditors should be able to obtain resources required from the organization*** to support **development, implementation, operation, and maintenance of continuous audit techniques.**

13) Short note on Audit Trail; and its objectives.

Answer:

It can be designed to record the activities. Audit trails acts as an important tool in detecting any error or fraud. Audit trail will have log to collect the event with sequence.

Audit Trail Objectives: Audit trails can be used to support security objectives in three ways**:** **PDF**

- Detecting unauthorized access to the system,
- Facilitating the reconstruction of events, and
- Promoting personal accountability

Detecting Unauthorized Access: Detecting unauthorized access can occur in real time or after the fact. *The primary objective of real-time detection is to protect the system from outsiders who are attempting to breach system controls*. A real-time audit trail can also be used to report on changes in system performance that may indicate infestation by virus or worm.

Reconstructing Events*:* Audit analysis can be used to reconstruct the steps that led to events such as system failures, security violations by individuals, or application processing errors. Knowledge of the conditions that existed at the time of a system failure can be used to assign responsibility and to avoid similar situations in the future. Audit trail analysis also plays an important role in accounting control. For example, by maintaining a record of all changes to account balances, the audit trail can be used to reconstruct accounting data files that were corrupted by a system failure.

Personal Accountability*:* Audit trails can be used to monitor user activity at the lowest level of detail. This capability is a preventive control that can be used to influence behavior. Individuals are likely to violate an organization's security policy if they know that their actions are not recorded in an audit log.

(c) **Audit of Environmental Controls**: Audit of environmental controls requires the IS auditor to conduct physical inspections and observe practices. The Auditor should verify that:

- The IPF (Infrastructure Planning and Facilities) and the construction with regard to the type of materials used for construction;
- The presence of water and smoke detectors, power supply arrangements to such devices, and testing logs;
- The location of fire extinguishers, firefighting equipment and refilling date of fire extinguishers;
- Emergency procedures, evacuation plans and marking of fire exists. There should be half-yearly Fire drill to test the preparedness;
- Documents for compliance with legal and regulatory requirements with regards to fire safety equipment, external inspection certificate and shortcomings pointed out by other inspectors/auditors;
- Power sources and conduct tests to assure the quality of power, effectiveness of the power conditioning equipment, and generators. Also the power supply interruptions must be checked to test the effectiveness of the back-up power;
- Environmental control equipment such as air-conditioning, dehumidifiers, heaters, ionizers etc;
- Compliant logs and maintenance logs to assess if MTBF (Mean Time Between Failures) and MTTR (Mean Time To Repair) are within acceptable levels; and
- Identify undesired activities such as smoking, consumption of eatables etc.

15

The Managerial controls and their Audit trails are as follows:

(a) <u>Top Management and Information Systems Management Controls</u>: The major activities that senior management must perform are – Planning, Organizing, Controlling and Leading.

- ***<u>Planning</u>: Auditors evaluate whether top management has formulated a high-quality information system's plan that is appropriate to the needs of an organization or not.***
- ***<u>Organizing</u>: Auditors should be concerned about how well top management acquires and manage staff resources.***
- ***<u>Leading</u>: Generally, the auditors examine variables that often indicate when motivation problems exist or suggest poor leadership – for example, staff turnover statistics, frequent failure of projects to meet their budget and absenteeism level to evaluate the leading function.***
- ***<u>Controlling</u>: Auditors must evaluate whether top management's choice to the means of control over the users of Information System services is likely to be effective or not.***

(b) *System Development Management Controls: Three different types of audits may be conducted during system development process as follows:*

- *Concurrent Audit: Auditors are members of the system development team. They assist the team in improving the quality of systems development for the specific system they are building and implementing.*
- *Post -implementation Audit: Auditors seek to help an organization learn from its experiences in the development of a specific application system. In addition, they might be evaluating whether the system needs to be scrapped, continued, or modified in some way.*
- *General Audit: Auditors evaluate systems development controls overall. They seek to determine whether they can reduce the extent of substantive testing needed to form an audit opinion about management's assertions relating to the financial statements for systems effectiveness and efficiency.*

(g) *Operations Management Controls: Auditors should pay concern to see whether the documentation is maintained securely and that it is issued only to authorized personnel. Auditors can use interviews, observations, and review of documentation to evaluate the activities of documentation librarians; how well operations management undertakes the capacity planning and performance monitoring function; the reliability of outsourcing vendor controls; whether operations management is monitoring compliance with the outsourcing contract; and Whether operations management regularly assesses the financial viability of any outsourcing vendors that an organization uses.*

(c) ***Programming Management Controls**: Some of the major concerns that an Auditor should address under different activities are as under:*

- ***Planning**: They should evaluate whether the nature of and extent of planning are appropriate to the different types of software that are developed or acquired and how well the planning work is being undertaken.*
- ***Control**: They must evaluate whether the nature of an extent of control activities undertaken are appropriate for the different types of software that are developed or acquired. They must gather evidence on whether the control procedures are operating reliably.*
- ***Design**: Auditors should find out whether programmers use some type of systematic approach to design. Auditors can obtain evidence of the design practices used by undertaking interviews, observations, and reviews of documentation.*
- ***Coding**: Auditors should seek evidence on the level of care exercised by programming management in choosing a module implementation and integration strategy. Auditors determine whether programming management ensures that programmers follow structured programming conventions.*
- ***Testing**: Auditors can use interviews, observations, and examination of documentation to evaluate how well unit testing is conducted. They are concerned primarily with the quality of integration testing work carried out by information systems professionals rather than end users.*
- ***Operation and Maintenance**: Auditors need to ensure effectively and timely reporting of maintenance needs occurs and maintenance is carried out in a well-controlled manner. Auditors should ensure that management has implemented a review system and assigned responsibility for monitoring the status of operational programs*

(d) ***Data Resource Management Controls**: Auditors should determine what controls are exercised to maintain data integrity. They might also interview database users to determine their level of awareness of these controls. Auditors might employ test data to evaluate whether access controls and update controls are working.*

(e) ***Quality Assurance Management Controls**: Auditors might use interviews, observations and reviews of documentation to evaluate how well Quality Assurance (QA) personnel perform their monitoring role. Auditors might evaluate how well QA personnel make recommendations for improved standards or processes through interviews, observations, and reviews of documentation.*

(f) ***Security Management Controls**: Auditors must evaluate whether security administrators are conducting ongoing, high-quality security reviews or not; check whether the organizations audited have appropriate, high-quality disaster recovery plan in place; and check whether the organizations have opted for an appropriate insurance plan or not.*

14. *Application Controls and their Audit Trail: These are categorized in the following types:*

- *Boundary Controls: IT ensures that those who are using system are authentic users.*
- *Input Controls: Responsible for bringing the data and instructions in to the information system.*
- *Communication Controls: Responsible for controls over physical components, communication line errors, flows, and links, topological controls, channel access controls, controls over subversive attacks, internetworking controls, communication architecture controls, audit trail controls, and existence controls.*
- *Processing Controls: Responsible for computing, sorting, classifying and summarizing data. It maintains the chronology of events from the time data is received from input or communication systems to the time data is stored into the database or output as results.*
- *Database Controls: Responsible to provide functions to define, create, modify, delete and read data in an information system. It maintains procedural data-set of rules to perform operations on the data to help a manager to take decisions.*
- *Output Controls: To provide functions that determine the data content available to users, data format, timeliness of data and how data is prepared and routed to users.*

State four major tasks performed by an Operating System while allowing users and their applications to share and access common resources.

Answer

Operating System is the computer control program that allows users and their applications to share and access common computer resources, such as processor, main memory, database and printers. Some of the major tasks performed by an Operating system are as follows:

- *Scheduling Jobs: They can determine the sequence in which jobs are executed, using priorities established.*
- *Managing Hardware and Software Resources: They can first cause the user's application program to be executed by loading it into primary storage and then cause the various hardware units to perform as specified by the application.*
- *Maintaining System Security: They may require users to enter a password - a group of characters that identifies users as being authorized to have access to the system.*
- *Enabling Multiple User Resource Sharing: They can handle the scheduling and execution of the application programs for many users at the same time, a feature called multiprogramming.*
- *Handling Interrupts: An interrupt is a technique used by the operating system to temporarily suspend the processing of one program in order to allow another program to be executed. Interrupts are issued when a program requests an operation.*
- *Maintaining Usage Records: They can keep track of the amount of time used by each user for each system unit - the CPU, secondary storage, and input and output devices.*

You are appointed to audit the Information Systems of ABC Limited. As a part of preliminary evaluation, list the major aspects which you would study to gain a good understanding of the technology environment and the related control issues.

Answer

As a part of preliminary evaluation, the major aspects which should be studied to gain a good understanding of the technology environment and related control issues are as follows:

- *Analysis of business processes and level of automation,*
- *Assessing the extent of dependence of the enterprise on Information Technology to carry on its businesses i.e. Role of IT in the success and survival of business,*
- *Understanding technology architecture which could be quite diverse such as a distributed architecture or a centralized architecture or a hybrid architecture,*
- *Studying network diagrams to understand physical and logical network connectivity,*
- *Understanding extended enterprise architecture wherein the organization systems connect seamlessly with other stakeholders such as vendors (SCM), customers (CRM), employees (ERM) and the government,*
- *Knowledge of various technologies and their advantages and limitations is a critical competence requirement for the auditor. For example, authentication risks relating to e-mail systems,*
- *And finally, studying Information Technology policies, standards, guidelines and procedures.*

NOV 16 RTP QUESTIONS

1. Security management controls and operation management controls
2. Types of is audit

MAY 16 RTP QUESTIONS

1 .need for audit of information system
2 .SCARF technique

15. Review of Controls at various Layers: For application security audit, a layered approach is used based on the functions and approach of each layer. This approach is in

line with management structure, which follows top-down approach. Various layers are:

- **Operational Layer:** The basic layer, where user access decisions are generally put in place.
- **Tactical Layer:** The next is management layer, which includes supporting functions such as security administration, IT risk management and patch management.
- **Strategic Layer:** This is the layer used by top management. It includes the overall information security governance, security awareness, supporting information security policies and standards, and the overarching an application security perspective.

Various aspects relating to each aforementioned layer are given as follows:

- **Operational Layer:** The operational layer audit issues include: *User Accounts and Access Rights, Password Controls and Segregation of Duties.*
- **Tactical Layer**: At the tactical layer, security administration is put in place. This includes: *Timely updates to user profiles, like creating/deleting and changing of user accounts, IT Risk Management, Interface Security and Audit Logging and Monitoring.*
- **Strategic Layer:** At this layer, the top management takes action, in form of drawing up security policy, security training, security guideline and reporting. A comprehensive information security programme fully supported by top management and communicated well to the organization is of paramount importance to succeed in information security. The security policy should be supported and supplemented by detailed standards and guidelines. These guidelines shall be used at the appropriate level of security at the application, database and operating system layers.

  Based on the key controls described previously, the risk assessment of failure/weakness in the operating effectiveness of key application security controls shall be made and acted upon by auditor.

MAY 16

1) Skills of an IS auditors
2) Application controls and their audit trail
3) Scarf and type of information use in scarf
4) Evidence collection and understanding the reliability of controls

Nov 15

1) Functions OF IS auditor 5) objectives of IS Auditor
2) Advantages of using continuous audit techniques
3) Factors influencing organization towards controls
4) Environmental controls and their audit