UNIT 12 AUDIT AND SECURITY OF COMPUTER SYSTEMS

Structure

12.0 INTRODUCTION

Every business process can experience events that can hamper and in some cases may stop normal operations of business. Even best designed system can't control the prevention of natural disaster. In today's ever-changing world of information assurance and network security, it can become extremely difficult to keep up on the latest vulnerabilities, viruses, patches, trends, technology, hacker behaviors and activity. It's easy for the information systems security professional to get caught up in attending the logical aspects of security such as reviewing log files, making configuration changes, troubleshooting, and other technical duties.

12.1 OBJECTIVES

After going through this unit, you should be able to:

- control, Assess and Monitor your organization's information and business systems;
- know Factors that are looked into , during Audit;
- learn about CAATs (Computer Assisted Audit Techniques);
- apply Information System Architecture;
- recover the Information Systems from disasters;

- plan the contingencies in the event of disasters; and
- protect Information Systems from Virus.

12.2 DEFINITION OF AUDIT

This is an assessment of an information system performed by an information systems professional or IS auditor to provide recommendations and advice to improve system performance and security. Audit should be done regularly and the result should be used to refine the system.

Is auditors are those people who make it sure that the system does what it is supposed to do. Although the audit can be carried out by the internal team of IT professionals, it is advisable that the audit is carried out by external auditors as they are neither stakeholders nor friendly with the stakeholders. Above all there is nothing like an unbiased opinion.

Information System auditor is a person who engages in Information system audits with the following knowledge and abilities:

1. Basic knowledge of information systems.
2. Knowledge of system audits.
3. Ability to perform system audits.

12.2.1 Objectives of Audit

The following are the objectives of Audit:

- To improve the quality of information systems, prevent failure and minimize the effects of failure, and speed up the process of recovery in the event of a failure. This will help Information System to be more reliable.
- To make an information system more secure from natural as well as manmade disasters, unauthorized access, and other destructive actions.
- To improve the cost performance of an information system by optimum utilization of its resources, which leads to increase in efficiency.

During the course of audit, the Information Systems Auditor will obtain sufficient, reliable, relevant and useful evidence to achieve the audit objectives effectively. The audit findings and conclusions are to be supported by appropriate analysis and interpretation of this evidence.

To achieve the above objective, the following documents should be made available to the auditors A diagram of the Information System (Application)

1. Network diagram
2. A hierarchical diagram of the project team

12.2.2 Responsibility and Authority of the System Auditor

The system auditor shall make the basis for each of his or her assessment clear. The system auditor may demand data and materials from the division being audited. The system auditor may also demand the head of an organization to issue a report on the implementation of improvement to an audited division as suggested by him.

The system auditor shall firmly maintain professional ethics as an impartial evaluator. The system auditor shall be aware of the ethical demands on himself or herself and meet the internal and external trust by performing an accurate and sincere system audit.

12.2.3 Confidentiality

The system auditor with strict adherence to professional ethics must maintain confidentiality of the information provided to him to carryout his or her activity and should not, without sufficient reason, divulge any information that is classified as confidential information by the audited organization.

12.2.4 Audit Planning

The Information Systems Auditor has to plan the information systems audit work to address the audit objectives and must comply with applicable professional auditing standards.

Check Your Progress 1

1. What are the objectives of Audit?
   ……
   ……
   ……
   ……
2. …….. are those people who make it sure that the system does what it is supposed to do.
3. CAAT stands for ……

12.3 AUDIT OF TRANSACTIONS ON COMPUTER

Audit can be broadly of two types namely auditing manual processes and audit through computer. Audit through computer is important to find out the accuracy and integrity of information system output. This types of audit are done by information system expert and use test data to check the adequacy and accuracy of control mechanism built-in to the system.

A typical audit looks at the following factors:

Audit of response time: In this audit the actual response time of the system verses the desired response time is compared to the performance of the system

Audit of broken links: This is applicable to web site and other intranet applications. The most irritating things on a web site is not finding a link document. There are automated software to find broken/unavailable links on web site.

Database Audit: Database audits involve checking the database integrity and availability. The information that is sent to the database should be checked with the information actually stored on the database.

Network audit: Network audit involves checking the venerability of network. It checks whether the network configuration is giving optimal performance or not.

12.3.1 Transaction Audit

Transaction audit is a process to find –

- Who did changes?
- What changes are made?
- Whether the changes are authorized or not as per the security policy of the Organization?

The details of the above transactions are written to either a media or printed. This allows Database Administrators to track changes and helps the organization to satisfy regulatory requirements such as tracking specific users actions, general security screening, validating user permissions etc.

12.3.2 Audit of Computer Security

Issues of security of computer involve both physical and logical security. Physical security involves restricting physical access to the computing resources from unauthorized person. Logical security involves restricting the use of computing resources by unauthorized person by providing logical control mechanism (e.g. password protection). The audit of computer security involves review of physical and logical security measures. Review of parameters, plans, practices, and policies that are developed and implemented by the organization over the computer resources, and how security measures are followed for Computers, Networks and Data communication. They are also included in the Audit.

12.3.3 Audit of Application

Here, both manual and programmed internal controls related to information systems are assessed. Primarily, there are four areas of audit coverage for an application being reviewed.

The four areas are given below:

Control environment: This includes reviewing the system's security, its operating platform, system documentation and the interaction it has with other systems.

Data Input Controls: This involves reviewing the controls which ensure that data that enters into the system is accurate, complete and valid as per the standard. Examples include verifying system tables, limit checks, range checks and redundant data checks.

Processing Controls: These controls ensure that the data is properly processed and that automatic calculations performed by the system are accurate. This is tested by assessing controls built into the programs and by processing test data through the system and comparing the results of processing with expected results. Also, there will be checks on currency of stored data, default values and reporting exceptions.

Output Controls: In this, review of the system generated reports to ensure that they are accurate and the reports produced are reliable, timely and relevant is done. Also, it is checked whether cost savings can be achieved by reducing the number of reports produced. Data control personnel perform visual review of computer output and reconciliation of totals.

12.3.4 Benefits of Audit

Information system audit is increasingly becoming the focal point of the independent audit, compliance audit, and operational audits. An information system audit can help the organizations in many ways:

- Improve system and process controls.
- Prevent and detect errors as well as fraud.
- Reduce risk and enhance system security.
- Plan for contingencies and disaster recovery.
- Manage information & developing systems.
- Prepare for the independent audit.
- Evaluating the effectiveness and efficiency related to the use of resources.
- Standardization.
- Improve business efficiency.

- Cost control.
- Competitive advantage.

12.4 COMPUTER ASSISTED AUDIT TECHNIQUES

The auditors use various types of automated audit software to carryout IS audit. The use of Computer Assisted Audit Tools (CAATs) should be controlled by the IS Auditor to provide reasonable assurance that the audit objectives and the detailed specifications of the CAATs have been met. There are two major types of CAATs namely *audit software* and *test data*.

12.4.1 Audit Software

This is a computer program used to process data of significance for audit from entity's accounting system. The auditor should substantiate their validity for audit purposes before making use of these tools. These include:

a) Package programs: Generalized computer programs to perform data processing functions like reading computer files, selecting info, performing calculations, etc.

b) Special purpose programs: Computer programs designed to perform audit tasks in specific business circumstances.

c) Utility tools: Used by the auditors to perform common data processing functions like sorting, creating and printing files. These tools are not designed for audit purposes specifically.

Various commercial Audit Software are available to carry out System Audit. Some of them are:

1. Visual Audit Pro
2. IDEA
3. E-Z Audit

Visual Audit Pro: It audits automatically over a network. It audits activities like, use log on/off, collects information about software and its version, collects information about hardware inventory like serial number, model, memory and associated peripheral devices, user information, registry information etc.

E-Z Audit: With this software one can know information on capacity of RAM, name of network card with its connect speed, MAC address and TCP/IP information. You can also find out how many local, removeable and network drives are there on the system, what printers are connected, both networked and local, etc.. On software front, it gives information on name and version of OS running on the system with service packs, installed programs and their names, EXE files and DLL versions.

IDEA (Interactive Data Extraction and Analysis): IDEA can be used to import information from database to be audited for further analysis to auditor. It helps to corroborate audit evidence effectively. For example it can check for duplicate payment on a single invoice. It is useful to analyze system log for fraud detection.

Consider the audit of a Payroll Package. The potential fraud that can occur in a payroll system is very high. Therefore, audit software is used as detection tool for fraud. The Audit software looks for salary unusually high, extracting information without a department number, extract information on bank account number. It also can extract information on fictitious employee, compare it with personnel database. It can also compare payment details of two different months.

12.4.2 Test Data

Test data is used to test the correctness of the software. When test data is processed with the entity's normal processing systems, the auditors should ensure that the test transactions are subsequently eliminated from the system. When using the test data, the IS auditors should be aware that the test data should only point out the erroneous processing and should not change the data that is produced by the system during real life.

12.4.3 Audit Expert Systems

Some IS auditors make use of Expert Systems to assist in auditing. When using these audit expert systems, the IS Auditor should be thoroughly knowledgeable of the operations of the system to confirm that the decision paths followed are appropriate to the given audit environment or situation.

12.4.4 Audit Trail

Audit trail is a log of changes made in the data, settings and related changes. A security subsystem should maintain detailed logs of who did what and when and also if there are any attempted security violations. The availability of the log is extremely valuable. Log provides information for the system auditor to be able to determine who initiated the transaction, the time of the day, date of entry, the type of entry, fields of information that were affected and the terminal used.

System log should be analyzed to provide detailed information on all normal and abnormal transactions during each processing period. System access and attempted access violations can be automatically logged by the computer and can be reported for check & review. Listing of terminal addresses and locations can be used to look for incorrectly logged, missing or additional terminals.

Applying the principles of Information System Security and Audit raised in this write-up will ensure that an organization's information assets and systems are adequately controlled, monitored and assessed.

Check Your Progress 2

1. Audit through computer is important to find out the ……..…….. and ……..…….of information system output.

2. Information system audit is increasingly becoming the focal point of the ……..……..., ……...…… and …….

3. …….can be used to import information from database to be audited for further analysis to auditor.

12.5 COMPUTER SYSTEM AND SECURITY ISSUES

Security is an important issue for modern IT Systems. Even though technology provides immense possibilities to safeguard organizations computing infrastructure, there has been security lapses and security breaches which have cost the organization heavily. System administrator and security administrator have spent sleepless nights to safeguard organization's data and computing infrastructure. One can think of organization like airlines, railway and banks which are heavily dependent on computing infrastructure and unavailability of system for few hours can create havoc. Organizations can't afford to underestimate the security issues that can affect their business operations.

Degree of security = 1 - (No. of security failures / No. of attempt to breach security)

There may be security threats due to natural reasons such as Earth Quakes, Cyclones etc. Sometimes, the threats are made by people. These may be due to riots, unrest, sabotage etc. Whenever , there is an attack, immediate reactive measures are to be taken. Also, one should study various controls to find out the people or reasons behind the attack. This can be done with the help of transaction logs etc. These attacks basically become possible due to several drawbacks in the information system such as lack of proper implementation of security protocols etc. Such things are exploited by people who plan attacks. The entire situation surrounding attacks is depicted in Fig. 12.1.

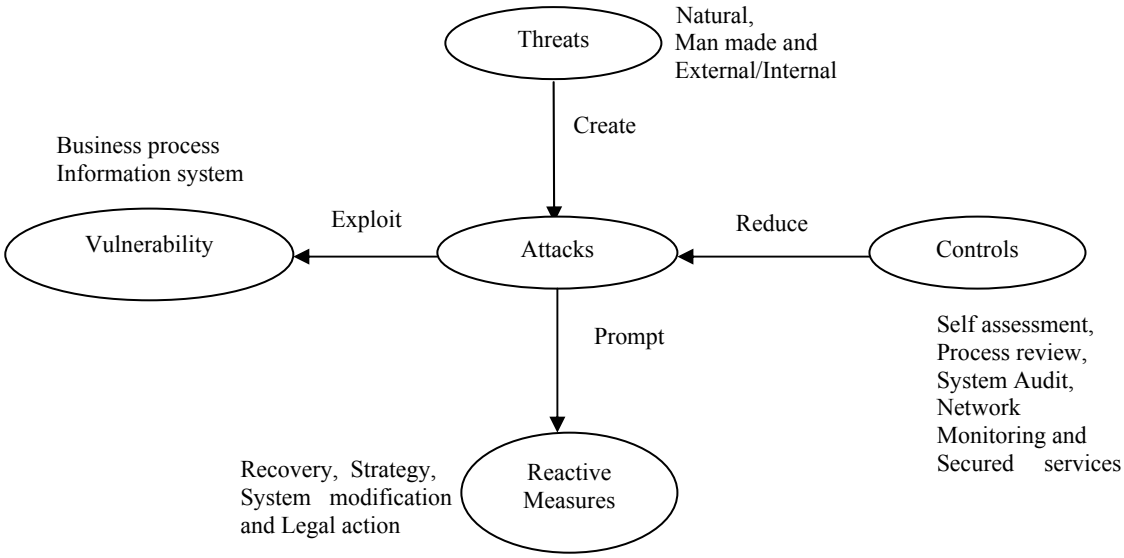

Figure 12.1: Information Security Architecture.

12.5.1 Analysis of Threats and Risks

The security of any system should be commensurate with the risk involved. Threat and risk assessment involves identification of applicable threats to IS infrastructure, recognition of vulnerability and probable loss calculation. In this context, it is necessary to identify the source of threat.

Historically, an organization's computer systems were centrally located and the management of issues related to it were responsibility of the computer center staff and as such security related issues were also the responsibility of computer center staff whose focus were to make available the application on the centrally located computer as required. In comparison, today's computing infrastructure are far more diverse and complex to manage. Business information is dispersed.

The source of threats can be either external or internal. Historically virus has been the major potential external security threat but as organizations are diversifying their activity over multiple locations and with evolution of new technology it is difficult to perceive when an unauthorized intruder may try to hack upon organization's vital information and cause damage. Internal security threats are more common although the integrity of employee is checked before being inducted into the organization. Employee of an organization can pose serious threats to information security as they are closely associated with the system and know the vulnerabilities that can be targeted.

Risk Analysis

The common questions asked in evaluating the risks are given below.

- Are the risks such as fire, earthquakes and the scope of their effects on the information system been made clear?

- Has the loss, the organization would suffer from a halt or the like of the information system been analyzed?
- Is the time permissible for recovery of operation and the order of priority of recovery been determined?

Security policy underlines an organization's holistic approach to security issues. Organizations must possess a security policy in writing, which should address the following issues:

Authentication: To see that the person is bonafide user of the resources
Authorization: Privileges of the user or who can do what?
Information integrity : Is it possible that the end user can modify the information?
Detection: Once the problem is identified, how it is handled and managed.

Risk Assessment and Management

A thorough and proactive risk assessment is the first step in establishing a sound security system. This is the ongoing process of evaluating threats and vulnerabilities, and establishing an appropriate risk management program to mitigate potential monetary losses and harm to an institution's reputation. Threats have the potential to harm an institution, while vulnerabilities are weaknesses that can be exploited.

There are different approaches followed by organizations to analyze risks. However, ultimately all the methods boil down to two types of approaches: quantitative and qualitative.

Quantitative Risk Analysis

This approach although difficult to implement gives an idea about the amount of risk involved with the event. This basically employs two fundamental elements i.e. The probability of occurrence of the loss making event and probability of occurrence of the event.

*Estimated Loss = Potential loss due to the event * probability*

It is therefore possible to rank the events in order of estimated loss. But the problem associated with the quantitative approach is estimating the probability of occurrence of the event, also in some cases the events are interrelated making the probability calculation even more difficult. Notwithstanding above difficulty, many organizations have adopted and implemented this approach successfully.

Qualitative Risk Analysis

The extent of the information security program should commensurate with the degree of risk associated with the institution's systems, networks, and information assets. For example, compared to an information-only Web site, institutions offering transactional Internet banking activities are exposed to greater risks. Further, real-time funds transfers generally pose greater risks than delayed or batch-processed transactions because the items are processed immediately. The extent to which an institution contracts with third-party vendors will also affect the way the risk assessment has to be done.

Performing the Risk Assessment and Determining Vulnerabilities

Performing a sound risk assessment is critical to establishing an effective information security program. The risk assessment provides a framework for establishing policy guidelines and identifying the risk assessment tools and practices that may be appropriate for an institution. Banks still should have a written information security policy, sound security policy guidelines, and well-designed system architecture, as

well as provide for physical security, employee education, and testing, as part of an effective program.

When institutions contract with third-party providers for information system services, they should have a concrete opinion about third party provider's quality of work and loyalty to the clients. At the minimum, the security-related clauses of a written contract should define the responsibilities of both parties with respect to data confidentiality, system security, and notification procedures in the event of data or system compromise. The institution needs to conduct a comprehensive analysis of the provider's security program, including how the provider uses available risk assessment tools and practices. Institutions also should obtain copies of independent penetration tests run against the provider's system.

When assessing information security products, management should be aware that many products offer a combination of risk assessment features, and can cover single or multiple operating systems. Several organizations provide independent assessments and certifications of the adequacy of computer security products (e.g., firewalls). While the underlying product may be certified, banks should realize that the manner in which the products are configured and ultimately used is an integral part of the products' effectiveness. If relying on the certification, banks should understand the certification process used by the organization certifying the security product. Other examples of items to consider in the risk assessment process include:

- Identifying mission-critical information systems, and determining the effectiveness of current information security programs. For example, vulnerability might involve critical systems that are not reasonably isolated from the Internet and external access via modem. Up-to-date inventory listings of hardware, software, as well as network topologies, is important in this process.
- Assessing the importance and business sensitivity of information for the likelihood of outside attacks/hacking and internal misuse of information. For example organization could be harmed if human resource data (e.g., confidential personnel information) were made public. The assessment process should identify systems that review the appropriateness of access controls and other security policy settings.
- Assessing the risks posed by service provider or business partner through electronic connections with internal IT infrastructure. The outsider may have poor access controls that could potentially lead to an indirect compromise of the organizations security system.
- Determining legal implications of security breaks and contingent liability concerns associated with any of the above factor. For example, if hackers successfully access a bank's system and withdraw money fraudulently, the bank will be liable for damage incurred to the account holder.

Potential threats

- *Denial of service (DoS),* which can be described as any action that prevent a system from normal operation. It may be the unauthorized destruction, modification, or delay of service. DoS is common where the number of requests outnumber the maximum number of connections possible. Under such circumstances, legitimate users have to wait for large amount of time for response to their request.
- Internet Protocol (IP) spoofing, which allows an intruder via the Internet/intranet to effectively impersonate a local system's IP address in an attempt to gain access to the system. The system in this case may misinterpret the incoming connection as originating from a trusted host.
- A Trojan horse program generally performs unintended destructive functions that may include destroying data, collecting invalid or falsifying data. Trojan horses can be attached to e-mails.

- Viruses are computer programs that may be embedded in other program and have the capability to self-replicate. Once active, they may result in either nondestructive or destructive invalid outcomes in the host computer. The virus program may also move into multiple platforms, data files, or devices on a system and spread through multiple systems in a network or through emails to other systems.

12.5.2 Recovering from Disasters

Natural and man-made disasters are inevitable. Earthquake, floods, fire and terrorist attack can severely damage organizations computing infrastructure. The disaster recovery plan is a document containing procedures for emergency response, extended backup operations, and recovery should a computer installation experience a partial or total loss of computing resources or physical facilities (or of access to such facilities). The primary objective of this plan, used in conjunction with the contingency plans, is to provide reasonable assurance that a computing installation can recover from disasters, continue to process critical applications in a degraded mode, and return to a normal mode of operation within a reasonable time. A key part of disaster recovery planning is to provide for processing at an alternative site during the time that the original facility is unavailable.

Contingency and emergency plans establish recovery procedures that address specific threats. These plans help prevent minor incidents from escalating into disasters. For example, a contingency plan might provide a set of procedures that define the condition and response required to return a computing capability to nominal operation. An emergency plan might be a specific procedure for shutting down equipment in the event of a fire or for evacuating a facility in the event of an earthquake.

During a disaster, normal operating procedures may be significantly altered. Both personnel and systems will be expected to function under conditions that are not expected under normal day-to-day operations. Security remains a requirement but techniques to apply it are altered to fit the contingency situation.

In-House Backup

This level is the minimum acceptable and is mandatory for all installations and application's systems. Define in detail all in-house back up procedures, the techniques used, files copied, frequency, etc.

Alternate Storage Area

This level of protection is necessary for mission critical components. It consists of off-site storage of at least one copy of all AIS files and databases, programs, and procedures necessary to operate the high priority application systems, either at the installation or at an alternate site of operation (including copies of contingency plans and related materials).

The alternate storage area should be located in an area reasonably accessible to the installation, but not subject to the same degree of major threat as the site. It is recommended that, as a rule of thumb, the alternate storage area be no closer than one mile from the site. However, the distance may vary from location to location.

The Disaster Recovery Toolkit

The *Disaster Recovery Toolkit* is a highly valuable collection of items and documents to assist in ensuring business continuity in the face of serious incident or disaster. Many organizations use these documents as a checklist and add element specific to their need.

Although they vary from organization to organization, they generally comprise the following:

- A contingency audit questionnaire
- A dependency analysis document - questions and guidance
- A Business Impact Analysis questionnaire.
- An audit questionnaire for disaster recovery or business continuity plan
- A checklist, action list and framework for disaster recovery

The toolkit is designed to help review the full spectrum of business continuity and disaster recovery issues.

12.5.3 Planning the Contingencies

Every business entity can and do experience events which can prevent it from normal function. The factors can range from natural events like flood, fire, earthquake etc. or a man made events like unauthorized access, serious computer malfunction or various information security accidents.

The very first step for contingency planning is to identify the contingency events covered and the appropriate actions for each. Contingency events usually refer to varying degrees of loss across six major asset categories: Data, Software, Communications, Hardware, Personnel, and Facility. The cause of the loss is dealt with in the Risk assessment, the primary concern in the contingency plan is the degree of loss, impact on the mission and techniques for coping.

Contingency management tools address basic issues such as asset identification, location, value, alternatives, replacement, and intangible costs; and most importantly, how long can the organization function without the asset? Since no asset is impervious to loss, the prudent leader will ensure that mechanisms are in place for a secure & rapid recovery. Our intent is to help managers break the cycle from normality to panic with crisis management.

Contingency Events

Loss of Data: To Identify key data and the type or degree of loss/damage that would be required for necessary recovery action. It can be done as follows:

- Identify appropriate recovery plan and procedure procedures. (Example in-house backups, etc.)
- The location of the required recovery files.
- To identify procedures for recovery of the files indicated above and include them in the contingency plan.

Loss of Software: To identify key software and the degree of criticality for necessary recovery action. It can be done as follows:

- Identify the type of software (commercial / in-house developed.)
- Identify the location where backup copies are maintained.
- In case of an emergency procurement process, the authorized person for it and any alternate source from where operational copies can be obtained.

Loss of Communications: To identify voice as well as data communications loss for necessary contingency plan and recovery action. It can be done as follows:

- Identify alternate communication facility available such as radios links or mobile phones for interim measures.
- Whether there is any service agreement in place with any party to deal with contingency issues.
- To estimate recovery time

Loss of Hardware: Inventory of required hardware must be maintained. For each hardware component, the loss which would require implementation of the contingency plan has to be found. It can be done as follows:

- Identify the hardware component and what functionalities it supports.
- Identify any alternate piece of equipment that may be used as a substitute to the equipment and it's degree of compatibility with the existing software.
- Whether the equipment is repairable?, and if so, is there maintenance agreement in place to accomplish the repairs. What is the response time to repair the equipment?
- The estimated cost and time for procurement of replacement hardware in case it is not repairable.
- Whether there are any emergency procurement procedures for key items?

Loss of Personnel: Loss of Personnel can result from employee leaving the organization, illness, death, family emergency and a number of other events. The following steps can be taken to minimize this type of loss:

- To identify key personnel in the organization and what their involvement/impact on major systems/programs/components.
- To identify substitutes for each personnel to handle such situation.
- Whether there are written procedures for every important function accomplished by the key personnel. Whether the substitutes use the same procedures periodically and do the assigned tasks.
- If alternates are not available within the organization replacements must be obtained from outside sources. It must be ensured that there are sufficient procedures in place and establish a training/orientation program to assign them the desired work to them.

Loss of the Facility: The loss of facility in general is due to some catastrophic natural action such as fire, flood, storm, earthquake, etc. However, a facility may become non-functional temporarily due to failure of power, or any other events that could render the facility non-functional.

- If the facility is to be out of operation beyond the maximum tolerable time, identify the procedures that are necessary for moving to the alternative facility.
- To identify all necessary hardware, software, data, and personnel required for normal functioning at the alternative location.
- To notify the alternative location to all concerned.

Any recovery procedure generally consists of following broad steps.

Preparing contingency plan involves people from all activities. The people should understand their role in the event of disaster and should be ready to react to the situation. Following are the major step involved in contingency planning :

Develop the Plan: The contingency plan is a detailed milestone to move the organization from a disrupted status to the status of normal operation. The role and responsibility of each employee and service provider are defined clearly in the event of disaster.

Testing the Plan: Once the plan is ready, it should be subjected to rigorous testing and evaluation. The plan should be initially tested in a simulated environment. Persons who would actually be involved in the event of a real disaster should test the plan.

Maintaining the Plan: Once the plan is created and tested it must be kept updated so that it remain relevant and applicable to changed business environment. The changes

in the business process must be reflected in the plan and all changes in it should be communicated to all concerned.

12.5.4 Viruses

Viruses are one of the major security threats to computer system. The first computer viruses were written in mid-eighties. The first virus written was a boot sector virus. Today, there are several tens of thousands of viruses.

Computer virus is nothing but a program that is loaded into your computer without your knowledge. This is only basic information . But, what makes people fear from Virus is the disastrous impact on remaining programs in your machine due to this program. The difference between a computer virus and other programs is that viruses are designed to self-replicate usually without the knowledge of the user. Computer viruses are called viruses because they share some of the traits of biological virus. A computer virus passes from computer to computer like a biological virus passes from person to person. A computer virus must **piggyback** on top of some other program or document in order to get executed. Once it is running, it is then able to infect other programs or documents. Obviously, the analogy between computer and biological viruses seems superficial, but, there are enough similarities as the name suggest.

Virus carries out instruction for replication. The effect of virus can vary from annoying messages, to the disastrous consequences (for example, the CIH virus, which attempts to overwrite the Flash BIOS, can cause irreparable damage to certain machines). Superficially, it looks as if virus which can format hard disk is more damaging but damage can be avoided by taking backups. Think of a virus which corrupts data by changing the numbers randomly on a spreadsheet application or changes + to –. This is certainly disastrous.

Viruses can be hidden in programs available on floppy disks or CDs, hidden in email attachments or in material downloaded from the web. If the virus has no obvious payload, a user without anti-virus software may not even be aware that a computer is infected.

A computer that has an active copy of a virus on its machine is considered infected. The way in which a virus becomes active depends on how the virus has been designed, e.g. macro viruses can become active if the user simply opens, closes or saves an infected document.

Prevention

The best way for users to protect themselves against viruses is to apply the following anti-virus measures:

- Make backups of all software (including operating systems). So,if a virus attack has been made, you can retrieve safe copies of your files and software.
- Inform all users that the risk of infection grows exponentially when people exchange floppy disks, download web material or open email attachments without caution.
- Have anti-virus (AV) software installed and updated regularly to detect, report and disinfect viruses.
- Visit sites which give information on the Internet about latest virus, it’s behavior and assess their potential threat.
- In case of doubt about a suspicious item that anti-virus software does not recognize, contact your anti-virus team immediately for guidance.

12.6 CONCURRENT AUDIT TECHNIQUES

Most of the Audit techniques collect data after transaction is completed. So, the outcome of the Audit is usually useful only for the future. The outcomes may be used as precautionary measures for the future.

In the case of Concurrent Audit Techniques, Data is collected while the transaction is in progress. This is very much useful for high risk transactions as they will be put on hold in case the Audit desires so. If any other Audit technique is used, then , such high risk transactions are processed after which it will be found that these transactions are invalid.

12.6.1 Need for Concurrent Audit Techniques

The following are few reasons for the need of Concurrent Audit techniques:

- Missing Audit trails.
- Need for continuously monitoring largely integrated and automated systems .

The following are various Concurrent Audit Techniques:

12.6.2 An Integrated Test Facility Technique (ITF)

In this technique , the Auditing software is embedded into the client software. Basically, what happens is that the test data of Auditor is integrated and the same is processed with Client's real life input data. ITF ensures that files of the client are unchanged and any changes, if necessary , will be made only to the dummy files of the client's files. At the end, these dummy files are studied to know the discrepancies.

12.6.3 The Snapshot Technique

In this technique, Audit software is embedded in the software that is to be audited. It is embedded at those places where critical processing takes place. Then, it takes a snapshot of the process before and after the critical processing.

12.6.4 SCARF

It stands for System Control Audit Review File. It is one of the complex Audit techniques. This technique will embed Audit software in the host application. This will enable audit software to monitor the Systems transactions uninterruptedly. The information that is collected during Audit process will be stored in a special audit file known as SCARF master file.

Usually, SCARF is used to collect the following information : Application System errors, Policy and procedural variances, System exceptions, Statistical samples, Snapshots and extended records, Data profiling, Data for performance measurement.

12.6.5 Continuous and Intermittent Simulation technique (CIS)

This technique will use the Data Base management systems to trap exceptions. Whenever , there is a need for service, DBMS will inform the same to CIS. CIS will then carry out the suitable service.

Check Your Progress 3

1. ……. and …….. assessment involves identification of applicable threats to IS infrastructure, recognition of vulnerability and probable loss calculation.
2. A …….. program generally performs unintended destructive functions that may include destroying data, collecting or falsifying data

3. In the case of ……..……, Data is collected while the transaction is in progress.

12.7 SUMMARY

Auditing IT system is a crucial activity to provide feedback to the system. The process of audit the report can be a food-for-thought for improving the information system. It is surprising that only very few companies take this activity seriously. Audits not only bring out the potentially weak areas in a system but also provide inputs for future improvement. It also helps in improving business efficiency.

Audit in generic sense refers to investigation of risks to computer as well as to processes and management of these risks through controls, proper procedures. Any one, who is doing this kind of assessment and submits a report in a sense is functioning as Auditor.

12.8 SOLUTIONS/ANSWERS

Check Your Progress 1

1. Improvement of Reliability, Security and Efficiency of Information Systems
2. Information System Auditors
3. Computer Assisted Audit Techniques

Check Your Progress 2

1. Accuracy, Integrity
2. Independent audit, compliance audit, and operational audits
3. IDEA

Check Your Progress 3

1. Threat, Risk
2. Trojan Horse
3. Concurrent Audit Techniques

12.9 FURTHER READINGS

James A. O'Brien; Mc Graw Hill Edition; *Introduction to Information Systems*, *An End user/Enterprise Perspective*;1995

Ian Somerville; Pearson Education; *Software Engineering*; Sixth Edition

James F.Peters and Witold Pedryez; John Wiley & Sons; *Software Engineering-An Engineering Approach*;2000

Reference Websites

http://www.contingency-planning-disaster-recovery-guide.co.uk
http://www.disasterrecoveryworld.com