UNIT 8 SECURITY AUDITS

Structure

8.1 INTRODUCTION

An organization’s networks and computer systems (“Information Systems”) are the means, which it uses to communicate and share information with all its users. The Information Systems during this process may come under attack from both internal as well as external sources. In order to minimize these attacks and the risks associated with these attacks, organizations need to do the two most important things, which will be discussed in this unit and are also the objectives of this unit.

8.2 OBJECTIVES

After studying this unit, you should be able to:

- know the processes of conducting an assessment of risks against all Information Systems of the organization;
- explain the concept of security audit;
- discuss various Information Security policies and measures (including technological, administrative and physical); and

- appreciate the requirements to conduct regular audits to verify the effectiveness of the Information Security measures and policies.

8.3 RISK ASSESSMENT AND CLASSIFICATION OF INFORMATION SYSTEMS

The security controls to be put in place require to be identified by a methodical assessment of risks. The risk assessment techniques require to be applied to the whole organization including individual information systems, specific components of such systems or services. In fact, risk assessment is a systematic consideration of the business hardships, likely to result from security failure, together with the potential consequences of the loss of confidentiality, integrity or availability of information and the information assets and the realistic likelihood of the occurrence of such failure in the light of the prevailing threats and vulnerabilities vis-à-vis the security controls currently implemented in the organization.

The results of this assessment will help guide and determine the appropriate management action, the priorities for managing the information and the information systems security risks and for implementing security controls, selected to protect the organization against such risks. The process of assessing the risks and the selection of the security controls may require to be performed a number of times to cover different parts of the organization or the individual information systems and services. It is also important to carry out periodic reviews of the security risks and the implemented security controls in view of new threats and vulnerabilities and to confirm that the security controls in place are effective and appropriate. The reviews will require to be performed at different levels of depth, depending on the results of the previous assessments and the changing levels of risk, which the management of the organization is prepared to accept. The risk assessments will require to be carried out first at a high level for prioritizing the information and the information assets in the areas of high risk and then, at a more detailed level to address specific risks.

The assessment of the vulnerabilities in the Information Systems and the risks, which arise therefrom, are an integral part of any Information Systems security and audit programme. The process of risk assessment is a method for formulating the policies and selecting the safeguards to protect information and information system assets from security threats occurring through the vulnerabilities, inherent in the personnel, facilities and equipment, communications, applications, environmental conditions, operating systems and applications. The risk assessment should be done by assessing the security threats relating to the above vulnerabilities and based on the impact of the occurrence, assigning a high, moderate or low risk to the particular vulnerability. In this way, the possibility and the magnitude of monetary loss, productivity loss and embarrassment to the organization can be minimized. It is important that the organization addresses all the known threats prudently/judiciously. The implementation of the security controls, the execution of the insurance policy and the recognition and acceptance of the risks are preferable to ignoring the security threats, existing and the likely future ones. Once the appropriate security controls have been identified and implemented, the next step is to conduct an audit of the security contracts.

Please answer the following Self Assessment Question.

Self Assessment Question 1 *Spend 3 Min.*

What is the best process for carrying out a risk assessment?

....

....

....

....

....

....

8.4 SECURITY AUDITS

There are various kinds of security audits, which may have to be done depending upon the vulnerabilities that you want to check. SAS 70 audits, SOX compliance audits etc are a few of the more specific audits. It is also possible to have an all encompassing audit such as ISO or BS audits which are applicable organization wide. These audits look at all the relevant security controls and audit the organization on the basis of these controls. An organization can opt to have an internal audit or an external audit by an auditing firm, which will lead to a certification that the organization is compliant with a standard under which it has been audited. Typically it is advisable to conduct an internal audit to plug all loopholes before opting for an external audit. This will make the process of certification easier after the external audit. This section outlines the various parameters, which an information security audit generally looks into.

8.4.1 Understanding the Importance of Information to Your Business

- How does the information you use in your business relate to your primary business objectives?
- Have you identified the information that is critical for you to do business?
- What tasks do you perform that involve the creation, processing, storage, use and transmission of that business-critical information?
- What assets do you use to create process, store and transmit that business-critical information (for example computers, card-indexes, mobile phones)?
- Do you know what would happen to your business if the confidentiality of those assets was broken (if, say, a competitor gained access to them)?
- Do you know what would happen to your business if the integrity of those assets was compromised, and you were unable to trust the information in them?
- Do you know what would happen to your business if those assets were unavailable to you for a period of an hour, a day, a week or a month?
- Using what you now know about the confidentiality, integrity and availability of your company's information assets, can you prioritize them?

Once you have prioritized information assets in order of their importance to your business, you will be able to ensure that they are given an appropriate degree of protection. Failing to do this could mean that you will be wasting time and resources on assets that are not critical to your business, or worse; that business-critical information is not adequately protected. Subsequent to that is an audit process, which will essentially ask the following questions:

8.4.2 Understanding Information Security Related Assets

- Do you have a written inventory of your business-critical information assets: hardware, software and intellectual (such as patents and contracts)?
- Does that inventory tell you where the assets can be found?
- Do you regularly update the inventory and audit it to ensure that it remains comprehensive and valid?
- Are you aware of the security features in the hardware and software you use, and do you have appropriate manuals or training materials about these features?
- Has anyone in the office had previous experience with these products or taken classes on them?

8.4.3 Understanding How Assets are Used, by Whom and for What Reason

- Who in your company has access to business-critical assets?
- Do your employees use unique passwords to control access to the computer assets they use?
- Are those passwords kept secure and changed regularly?
- Do you ensure that access is given only for genuine work-related reasons?
- Do you keep the list of who has access to what, and do you regularly update those lists?
- Do you run a local- or wide-area network? If so, how do you control access to that network? If passwords are used, are these unique to each user, changed regularly and kept secure?
- Do you have Internet access? If so, do you have broadband access or dial-up?
- Which computers/devices in the company have network or Internet access, and do you know who uses these?
- Do employees have remote access to your network (either from home or on the road?)
- How do employees gain access to your network when they are working remotely?

8.4.4 Understanding Security Management

- Read the following list of security technologies and ask yourself; which are you aware of, and which do you use:
  - firewalls and VPN (Virtual Private Networks),
  - access, authorization and authentication controls,
  - anti-virus,
  - spam filters,

- Internet content control,
- network- security policy compliance tools,
- vulnerability and threat databases,
- cryptography tools such as SSL, public-key cryptography and hard-disk,
- encryption,
- intrusion detection systems.

- Do you regularly back up your business-critical data?
- Do you test the back-ups, restoring the data from them and making sure it is usable?
- Do employees using laptops or other computers for remote access have anti-virus software and firewalls on those computers?
- Do you allow employees to use the company's computers, systems or network access for non-business purposes? If so, do you make it clear to them that certain uses are unacceptable and may result in disciplinary action?
- Do you provide any security education or training for employees who use the company's computers or information systems?
- Do you have any policies, standards or procedures related to security?

8.4.5 Understanding Your Broader Obligations

- Are you familiar with legal requirements related to securing certain types of information (Financial services information, health information, personal data)?
  - This may involve privacy legislation as well as sectoral regulation.
  - In some cases, especially where personal, sensitive or confidential information is involved, you may be required to provide a minimum level of protection for that information, irrespective of the size of your company.
- Are you familiar with the rights of employees in the workplace?
  - Some laws may limit your access to certain types of employee information and communications, or require notice or consent before you are able to access real or virtual information held in an employees' workspace.
- Are you aware of your role regarding the security of others?
  - The security of information systems is complex because businesses are connected to each other directly and through the Internet, creating interdependencies and spreading risk. Failing to properly secure your system may not just compromise and potentially harm your business; it can increase the risk of other systems to which you are connected. Greater risk could result from virus programs using your contact lists to spread further, or from malicious programs using your unsecured networked computer to attack or send spam to other systems or computers.
  - Do your employees understand what is appropriate behaviour on the Internet? This goes beyond not downloading or posting illegal, inappropriate or offensive material, and includes general conduct that is in keeping with the values and ethical practices of your business.

Please answer the following Self Assessment Question.

Self Assessment Question 2 *Spend 3 Min.*

Name a few of the standard security audit processes used in the industry.

....

....

....

....

....

....

8.5 SECURITY POLICY, STANDARDS AND PROCEDURES

Subsequent to an audit, which answers all the above questions, you will be able to formulate strategies of information security to put in place to plug in the loopholes, which the audit has revealed. This is mainly done through adopting a security policy, which lay down the parameters of information security across the organization.

8.5.1 Security Policy

The policy should include the following:

- Information is vital to our business.
- We protect the confidentiality, integrity and availability of our business-critical information.
- We have standards that help us to do this – including:
  - physical security
  - personnel security
  - access controls
  - security technology
  - security response and recovery, and
  - security audits.
- We have procedures that help us to meet our standards.
- Employees should be familiar with the procedures relevant to their roles and responsibilities.
- We take disciplinary measures against employees who persistently or deliberately flout these information security policies, standards and procedures.

The policy should say where details of the standards and procedures can be found.

8.5.2 Security Standards

The standards listed in the security policy section above are examined in more detail in this section.

- *Physical security*
  - Fit appropriate locks or other physical controls to the doors and windows of rooms where you keep your computers.
  - Physically secure lap tops when they are unattended (for example, by locking them in a drawer overnight).
  - Ensure that you control and secure all removable media, such as removable hard-drives, CDs, floppy disks and USB drives, attached to your business-critical assets.
  - Make sure that you destroy or remove all business-critical information from media such as CDs and floppy disks before disposing of them.
  - Make sure that all business-critical information is removed from the hard drives of any used computers before you dispose of them.
  - Store back-ups of your business-critical information either off-site or in a fire- and water-proof container.
- *Access controls*
  - Use unique passwords, that are not obvious (not birth dates or easily found or guessed information) and change them regularly, preferably every three months.
  - Use passwords that contain letters in both upper and lower case, numbers and special keys, and are six or more characters in length. It helps if you consider your password as a memorable sentence, rather than a single word. For example, the sentence: "at forty-two I'm a star!" could be translated into an eight-character password that looks like this: @42Ima*!
  - Don't write your password down, and never share it with anyone. If you do have to share it, make sure you change it as soon as possible — no matter how well you trust the person you shared it with!
- *Security technology*
  - All computers used in your business should have anti-virus software installed, and the virus definitions must be updated at least once a week (many providers have a one-click update). All incoming and outgoing traffic should be scanned for viruses, as should any disk or CD that is used, even if it is from a 'trusted' source. At least once a month, computers should be scanned for viruses.
  - If your computers are connected to the Internet, and especially if you use a broadband connection, you must deploy a software firewall. This will help to prevent malicious code from entering your computer and potentially compromising the confidentiality, integrity and availability of your network. It will also help to stop your system being used to attack other systems without your knowledge. Software firewalls for use by non-professionals are readily available at a reasonable cost. Your operating system, virus control software or ISP may also offer a firewall. Consumer and popular trade magazines compare firewall functions and features of well-known products, and so are a good source of information. Free shareware firewalls are available, but these usually require expert knowledge for correct use.
  - If your business has a small network that is connected to the Internet, you should consider deploying an 'all-in-one' hardware box that contains a firewall, anti-virus program and an intrusion detection system. This will greatly simplify your use and maintenance of essential Internet security technology.

- *Personnel*
  - Perform integrity checks on all new employees to make sure that they have not lied about their background, experience or qualifications.
  - Give all new employees a simple introduction to information security, and make sure that they read and understand your information security policy. Make sure they know where to find details of the information security standards and procedures relevant to their role and responsibilities.
  - Ensure that employees have access only to the information assets they need to do their jobs. If they change jobs, make sure that they do not retain their access to the assets they needed for their old job. When dismissing employees, ensure that they do not take with them any business-critical information.
  - Make sure that no ex-employees have access rights to your systems.
  - Make sure your employees know about the common methods that can be used to compromise your system. These include e-mail messages that contain viruses and 'social engineering' ploys used by hackers to exploit employees' helpfulness to gain information that will give them access to your system. Examples of 'social engineering' include a hacker using the telephone to pose as a systems maintenance engineer or pretending to be a new employee.
- *Security Incident/Response*
  - A security incident is any event that can damage or compromise the confidentiality, integrity or availability of your business-critical information or systems.
  - It is important to make your staff aware of telltale signs of security incidents. These could include:
    - strange phone requests, especially for information
    - unusual visitors
    - strange patterns of computer activity
    - unusual appearance of computer screens
    - computers taking longer than usual to perform routine tasks.
  - Your staff should understand that it is always better to notify the right person if they observe anything that might be a telltale sign of a security incident.
  - If a security incident happens, employees should know who to contact and how.
  - You should have in place a plan to assure business continuity in the event of a serious security incident. The plan should specify: Designated people involved in the response, External contacts, including law enforcement, fire and possibly technical experts. Contingency plans for foreseeable incidents such as:
    - Power loss
    - Natural disasters and serious accidents
    - Data compromise
    - No access to premises
    - Loss of essential employees
    - Equipment failure.

- Your plan should be issued to all employees and should be tested at least once a year, even if you haven't had a security incident.

After every incident when the plan is used, and after every test, the plan should be re-examined and updated as necessary using the lessons learned.

After this exercise of setting in place appropriate information security policies and processes you will be ready for an external audit. Again the external audit will ask the same questions you asked yourself in the internal audit. Only now, all the loopholes will have been plugged due to the implementation of the Information Security policies and processes and certification becomes easier.

8.5.3 Protection of System Audit Tools

There should be controls to safeguard operational systems and audit tools during system audits to maximize the effectiveness of and to minimize interference to/ from the system audit process. Protection is also required to safeguard the integrity of the information systems and prevent misuse of the audit tools. Audit requirements and the activities involving checks on operational systems should be carefully planned and agreed to minimize the risk of disruption to the business processes. The following should be observed:

(a) Audit requirements should be agreed with the appropriate management.

(b) The scope of the checks should be agreed and controlled.

(c) The checks should be limited to read-only access to software and data.

(d) Access other than read-only should only be allowed for isolated copies of system files, which should be erased when the audit is completed.

(e) IT resources for performing the checks should be explicitly identified and made available.

(f) Requirements for special or additional processing should be identified and agreed.

(g) All accesses should be monitored and logged to produce a reference trail.

(h) All procedures, requirements and responsibilities should be documented.

Access to system audit tools i.e. software or data files, should be protected to prevent any possible misuse or compromise. Such tools should be separated from development and operational systems and not held in tape libraries or user areas, unless given an appropriate level of additional protection.

8.5.4 Importance of Audit Trails During Audits

Audit trails are records of activity, used to provide a means for restructuring events and establishing accountability. The audit trail information is essential for investigation of the incidents/problems. The controls, useful in the audit trail process, are described hereunder. To deter and provide early detection of unauthorized activity, the following steps should be implemented:

(a) To provide an audit trail for the computer systems and manual operations when:

   i) SENSITIVE or HIGHLY SENSITIVE information is accessed;

   ii) network services are accessed; and

   iii) special privileges or authorities such as the security administration commands, emergency USERIDs, supervisory functions etc., overriding the normal processing flow, are used.

(b) To include in the audit trail as much of the following as is practical:

i) user identification ;

ii) functions, resources and information used or changed ;

iii) date and time stamp (including time zone) ;

iv) work-station address and network connectivity path ; and

v) specific transaction or program executed.

(c) To provide an additional real time alarm of significant security-related events for all computer systems having on-line capabilities for enquiry or update, containing information as under :

i) access attempts that violate the access control rules ;

ii) attempts to access functions or information not authorized ;

iii) concurrent log-on attempts ; and

iv) security profile changes.

(d) To investigate and report suspicious activity immediately.

(e) To ensure that management reviews the audit trail information on a timely basis, usually daily.

(f) To investigate and report security exceptions/violations and unusual occurrences.

(g) To preserve the audit trail information for an appropriate period of time for business requirements.

(h) To protect the audit trail information from deletion, modifications, fabrications or re-sequencing by use of digital signature.

8.5.5 Sensitive System Isolation

Sensitive systems might require a dedicated (isolated) computing environment. Some application systems are sufficiently sensitive to potential loss and they require special handling. The sensitivity/criticality may be such that the application system requires to run on a dedicated computer system or that it should share resources with other trusted application systems only. The following may be considered for addressing such requirements:

(a) The sensitivity of an application system should be explicitly identified and documented by the application owner.

(b) When a sensitive application is to run in a shared environment, the other application system(s) with which it will share resources should be identified and agreed with the owner of the sensitive application.

8.5.6 Monitoring of System Use – Procedures and Areas of Risk

Procedures for monitoring the use of information processing facilities should be established. Such procedures are necessary to ensure that the users perform only those activities, for which they have been authorized. The level of monitoring required for individual facilities should be determined by a risk assessment, which should include the following :

(a) Authorized Access including details as under :

- the user ID;
- the date and time of key events;

- the types of events ;
- the files accessed; and
- the program/utilities used.

(b) All Privileged Operations as under :

- use of supervisor account;
- system start-up and stop; and
- I/O device attachment/detachment.

(c) Unauthorized Access Attempts as under :

- failed attempts;
- access policy violations and notifications for network gateways and firewalls; and
- alerts from proprietary intrusion detection systems.

(d) System Alerts or Failure as under :

- console alerts or messages;
- system log exceptions; and
- network management alarms.

Risk Factors

The result of the system monitoring activities should be reviewed regularly. The frequency of the review should depend on the risks involved. The risk factors, as under, should be considered in this regard:

(a) the criticality of the application processes ;

(b) the value, sensitivity or criticality of the information involved ;

(c) the past experience of system infiltration and misuse; and

(d) the extent of system interconnection (particularly public networks).

Operator logs

Operational staff should maintain a log of their activities. Logs should include the following:

(a) system starting and finishing times;

(b) system errors and corrective action taken;

(c) confirmation of the correct handling of data files and computer output; and

(d) the name of the person making the log entry.

Operator logs should be subject to regular, independent checks against operating procedures.

Fault Logging

Faults should be reported and corrective action taken. Faults, reported by the users regarding the problems with the information processing or communication systems, should be logged. There should be established rules and procedures for handling the reported faults, which, among others, should include:

(a) review of the fault logs to ensure that faults have been satisfactorily resolved;

(b) review of corrective measures to ensure that controls have not been compromised and that the action taken is fully authorized.

Logging and Reviewing of Events

A log review involves understanding the security threats faced by the information systems and the manner in which such threats may arise. System logs often contain a large volume of information, much of which is extraneous to security monitoring. There should be a documented plan for the volumes of information to be logged, rotation of log files, back-up archival of log files, encryption of log files and retention/disposal of log data. To help identify significant events for security monitoring purposes, the copying of appropriate message types automatically to a second log, and/or the use of suitable system utilities or audit tools to perform file interrogation should be considered. When allocating the responsibility for log review, a separation of roles should be considered between the person(s) undertaking the review and those whose activities are being monitored. Particular attention should be given to the security of the logging facility because any susceptibility to tampering thereof i.e. modifications, fabrications etc., can lead to a false sense of security. Security controls should aim to protect the logging facilities against unauthorized changes and operational problems including:

(a) the logging facility being de-activated:

(b) alterations to the message types that are recorded;

(c) log files being edited or deleted; and

(d) log file media becoming exhausted and either failing to record events or overwriting itself.

System Clock Synchronization

The correct setting of computer clocks is important to ensure the accuracy of audit logs, which may be required for investigations or as evidence in legal or disciplinary cases. Inaccurate audit logs may hinder such investigations and damage the credibility of such evidence. Where a computer or communications device has the capability to operate a real-time clock, it should be set to an agreed standard, e.g. Universal coordinated Time (UCT) or local standard time. As some clocks are known to drift with time, there should be a procedure that checks for and corrects any significant variation.

Please answer the following Self Assessment Question.

Self Assessment Question 3 *Spend 3 Min.*

Should there be audit trials during the audit process? If, yes, why?

....

....

....

....

....

....

Let us now summarize the points covered in this unit.

8.6 SUMMARY

- Regular Security Audits are a must for all organizations.
- The audits can be both internal and external.
- The audits reveal the loopholes in the information security system.
- There are various kinds of security audits, which may have to be done depending upon the vulnerabilities that you want to check. SAS 70 audits, SOX compliance audits etc are a few of the more specific audits.
- Based on the audits, adequate measures and systems have to be adopted by organizations. This is mainly done through adopting a security policy.
- Security policy has certain standards to protect the confidentiality and integrity of information vital to any business. This includes:
  - physical security,
  - personnel security,
  - access controls,
  - security technology,
  - security response and recovery, and
  - security audits.
- There should be controls to safeguard operational systems and audit tools during system audits to maximize the effectiveness of and to minimize interference to/ from the system audit process.
- Audit trail are the records of activity, used to provide means for restructuring events and establishing accountability. Therefore, they are very important during audits for investigation of problems.
- Sensitive systems which are sensitive to potential laws require a special, dedicated (isolated) computing environment.
- For monitoring the use of information processing facilities, a procedure should be established to ensure that the user performs only those activities for which they have been authorized.
- The level of monitoring required for individual information processing facilities should be determined by risk assessment.

8.7 TERMINAL QUESTIONS

1. What do you mean by Risk Assessment and Classification of Information Systems and why is it important to an organization intending to conduct a Security Audit?
2. What factors need to be considered while analysing the importance of information and information systems to an organization and its functioning? Explain with examples.
3. What are the key factors in an organization, which need to be audited as a part of the Information Security Audit? Explain in detail.
4. Describe in brief the various components and parameters of an Information Security Policy, which addresses the various issues identified in the audit.

5. Why is protection of system audit tools important and what are the broad processes to ensure that such tools are well protected?
6. What are audit trails and why is it important to have audit trails?
7. What special measures need to be adopted to ensure security of sensitive systems and information?

8.8 ANSWERS AND HINTS

Self Assessment Questions

1. First at a high level for prioritising the information and the information assets in the areas of high risk and then, at a more detailed level to address specific risks.
2. SAS 70 audits and SOX.
3. Yes, because the audit trail information is essential for investigation of incidents/ problems.

Terminal Questions

1. Refer to sections 8.3 and 8.4 of the unit.
2. Refer to section 8.4 of the unit.
3. Refer to section 8.4 of the unit.
4. Refer to section 8.5 of the unit.
5. Refer to section 8.5 of the unit.
6. Refer to section 8.5 of the unit.
7. Refer to section 8.5 of the unit.

8.9 REFERENCES AND SUGGESTED READINGS

1. Banking and related Financial Services – Information Security Guidelines. Technical Report. ISO TR 13569:2005.
2. Information Security Management - Code of Practice for Information Security Management Systems. BS 7799-1:1999. Withdrawn and replaced by BS ISO IEC 17799:200, ISO/IEC 17799.
3. Information Technology Security Guidelines. Infocomm Development Authority of Singapore. Sept. 1999.
4. COBIT – Control Objectives. IT Governance Institute (ITGI). July. 2000.
5. COBIT – Management Guidelines. IT Governance Institute (ITGI). July. 2000.
6. Information Technology Act. 2000.
7. Information Technology (Certifying Authorities) Rules. 2000.