UNIT- 4

Q.1 State the benefits & objectives of information security audit.

Ans: There are various benefits & objectives of information security audit are as follows:

1. Individual Accountability

- Audit trails are a technical mechanism that help managers maintain individual accountability.
- By advising users that they are personally accountable for their actions, which are tracked by an audit trail that logs user activities, managers can help promote proper user behavior.
- Users are less 129 likely to attempt to security policy if they know that their actions will be recorded in an audit log.

2. Reconstruction of Events

- Audit trails can also be used to reconstruct events after a problem has occurred.
- Damage can be more easily assessed by reviewing audit trails of system activity to pinpoint how, when, and why normal operations ceased.
- Audit trail analysis can often distinguish between operator-induced errors or system-created errors.

3. Intrusion Detection

- Intrusion detection refers to the process of identifying attempts to penetrate a system and gain unauthorized access.
- If audit trails have been designed and implemented to record appropriate information, they can assist in intrusion detection
- Although normally thought of as a real-time effort, intrusions can be detected in real time, by examining audit records as they are created.

4. Problem Analysis

- Audit trails may also be used as on-line tools to help identify problems other than intrusions as they occur. This is often referred to as real-time auditing or monitoring.
- An analysis of the audit trails may be able to verify that the system operated normally.

Q.3 List and explain the phases of a disaster recovery plan.

Ans: Refer Question no: 12

Q.4 State and explain any 4 interdependencies of audit trails.

Ans: The following paragraphs describe some of the most important interdependencies

1. Policy

- The most fundamental interdependency of audit trails is with policy.
- Policy dictates who authorized access to what system resources is.
- Therefore it specifies, directly or indirectly, what violations of policy should be identified through audit trails.

2. Assurance

- System auditing is an important aspect of operational assurance.
- The data recorded into an audit trail is used to support a system audit.
- The analysis of audit trail data and the process of auditing systems are closely linked; in some cases, they may even be the same thing.
- In most cases, the analysis of audit trail data is a critical part of maintaining operational assurance.

3. Incident Response

- If a security incident occurs, such as hacking, audit records and other intrusion detection methods can be used to help determine the extent of the incident.
- For example, was just one file browsed, or was a Trojan horse planted to collect passwords?

4. Cryptography

- Digital signatures can be used to protect audit trails from undetected modification.
- Digital signatures can also be used in conjunction with adding secure time stamps to audit records.
- Encryption can be used if confidentiality of audit trail information is important.

Q.5 Write a note on cost considerations in audit trails.

Ans: Audit trails involve many costs.

- First, some system overhead is incurred recording the audit trail. Additional system overhead will be incurred storing and processing the records.
- The more detailed the records, the more overhead is required.
- Another cost involves human and machine time required to do the analysis. This can be minimized by using tools to perform most of the analysis.
- Many simple analyzers can be constructed quickly from system utilities, but they are limited to audit reduction and identifying particularly sensitive events.

- More complex tools that identify trends or sequences of events are slowly becoming available as off-the-shelf software.
- The final cost of audit trails is the cost of investigating anomalous events.
- If the system is identifying too many events as suspicious, administrators may spend undue time reconstructing events and questioning personnel.

Q.6 what are the various types of audit trails?

Ans: There are three types of audit trails are as follows:

1. System-Level Audit Trails

- A system audit trail should be able to identify failed log-on attempts, especially if the system does not limit the number of failed log-on attempts.
- Unfortunately, some system-level audit trails cannot detect attempted logons, and therefore, cannot log them for later review.
- These audit trails can only monitor and log successful logons and subsequent activity. To effectively detect intrusion, a record of failed log-on attempts is required.

2. Application-Level Audit Trails

- System-level audit trails may not be able to track and log events within applications, or may not be able to provide the level of detail needed by application or data owners, the system administrator, or the computer security manager.
- In general, application-level audit trails monitor and log user activities, including data files opened and closed, specific actions, such as reading, editing, and deleting records or fields, and printing reports.
- Some applications may be sensitive enough from a data availability, confidentiality, and/or integrity perspective that a "before" and "after" picture of each modified record should be captured by the audit trail.

3. User Audit Trails

- User audit trails can usually log: all commands directly initiated by the user; all identification and authentication attempts; and files and resources accessed.
- It is most useful if options and parameters are also recorded from commands. It is much more useful to know that a user tried to delete a log file (e.g., to hide unauthorized actions) than to know the user merely issued the delete command, possibly for a personal data file.

Q.7 Explain Audit Trails. What are the two types of audit records explain in detail?

Ans:

- Audit trails maintain a record of system activity both by system and application processes and by user activity of systems and applications.
- In conjunction with 127 appropriate tools and procedures, audit trails can assist in detecting security violations, performance problems, and flaws in applications.
- Audit trails may be used as either a support for regular system operations or a kind of insurance policy or as both of these.
- There are typically two kinds of audit records, (1) an event-oriented log and (2) a record of every keystroke, often called keystroke monitoring

1. An event-oriented log

- Event-based logs usually contain records describing system events, application events, or user events.
- An audit trail should include sufficient information to establish what events occurred and who caused them
- In general, an event record should specify when the event occurred, the user ID associated with the event, the program or command used to initiate the event, and the result.

2. Keystroke Monitoring

- Keystroke monitoring is the process used to view or record both the keystrokes entered by a computer user and the computer's response during an interactive session.
- Keystroke monitoring is usually considered a special case of audit trails.
- Examples of keystroke monitoring would include viewing characters as they are typed by users, reading users' electronic mail, and viewing other recorded information typed by users.
- Keystroke monitoring is conducted in an effort to protect systems and data from intruders who access the systems without authority or in excess of their assigned authority.

Q.9 what are the implementations issues regarding Audit Trail?

Ans: Following are implementation issues that may have to be addressed when using audit trails.

1. Protecting Audit Trail Data

- Access to on-line audit logs should be strictly controlled.

- Computer security managers and system administrators or managers should have access for review purposes.
- It is particularly important to ensure the integrity of audit trail data against modification. One way to do this is to use digital signatures. Another way is to use write-once devices.

2. Review of Audit Trails

- Audit trails can be used to review what occurred after an event, for periodic reviews, and for real time analysis.
- Audit trail review can be easier if the audit trail function can be queried by user ID, terminal ID, application name, date and time, or some other set of parameters to run reports of selected information.

3. Tools for Audit Trail Analysis

- Many types of tools have been developed to help to reduce the amount of information contained in audit records.
- Especially on larger systems, audit trail software can create very large files, which can be extremely difficult to analyze manually.
- The use of automated tools is likely to be the difference between unused audit trail data and a robust program.

Q.10 Write a note on interdependences in Audit Trial.

Ans: Refer Question no: 4

Q.12 Explain the concept of Business Continuity Planning and Recovery Plan in industry.

Ans:

- Today's organizations, in their efforts to reduce costs, are streamlining layers of management while implementing more complex matrices of control and reporting.
- Distributed systems have facilitated the reshaping of these organizations by moving the control of information closer to its source, the end user.
- In this transition, however, secure management of that information has been placed at risk. Information technology departments must protect the traditional system environment within the computer room plus develop policies, standards, and guidelines for the security and protection of the company's distributed information base.
- Further, the information technology staff must communicate these standards to all users to enforce a strong baseline of controls.

- In these distributed environments, information technology personnel are often asked to develop systems recovery plans outside the context of an overall business recovery scheme. Recoverability of systems, however, should be viewed as only one part of business recovery.
- The phases of a disaster recovery plan process are
  - Awareness and discovery
  - Risk assessment
  - Mitigation
  - Preparation
  - Testing
  - Response and recovery
- Recovery planners should adapt these phases to a company's specific needs and requirements. Some of the phases may be combined, for example, depending on the size of the company and the extent of exposures to risk.
- It is crucial, however, that each phase be included in the formation of a recovery plan.

Q.14 Write a short note on logical security audit.

Ans: When auditing logical security the auditor should investigate what security controls are in place, and how they work? In particular, the following areas are key points in auditing logical security:

- **Passwords**:
  - Every company should have written policies regarding passwords, and employee's use of them.
  - Passwords should not be shared and employees should have mandatory scheduled changes.
  - Employees should have user rights that are in line with their job functions. They should also be aware of proper log on/ log off procedures. Also helpful are security tokens, small devices that authorized users of computer programs or networks carry to assist in identity confirmation.
  - They can also store cryptographic keys and biometric data. The most popular type of security token (RSA's SecurID) displays a number which changes every minute. Users are authenticated by entering a personal identification number and the number on the token.
- **Termination Procedures**:
  - Proper termination procedures so that old employees can no longer access the network. This can be done by changing passwords and codes.
  - Also, all ID cards and badges that are in circulation should be documented and accounted for.

- **Special User Accounts**:
  - Special User Accounts and other privileged accounts should be monitored and have proper controls in place.
- **Remote Access:**
  - Remote access is often a point where intruders can enter a system. The logical security tools used for remote access should be very strict. Remote access should be logged.

Q.15 Explain the system-level, application level and user audit trails.

Ans: Refer Question no: 6