Unit-4

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

**Ans:**

* **Benefits and Objectives**:
* Audit trails can provide a means to help accomplish several security-related objectives, including individual accountability, reconstruction of events, intrusion detection, and problem analysis.

**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 likely to attempt to circumvent security policy if they know that their actions will be recorded in an audit log.
* For example, audit trails can be used in concert with access controls to identify and provide information about users suspected of improper modification of data (e.g., introducing errors into a database). An audit trail may record "before" and "after" versions of records.

**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 (during which the system may have performed exactly as instructed) or system-created errors (e.g., arising from a poorly tested piece of replacement code).
* If, for example, a system fails or the integrity of a file (either program or data) is questioned, an analysis of the audit trail can reconstruct the series of steps taken by the system, the users, and the application.
* Knowledge of the conditions that existed at the time of, for example, a system crash, can be useful in avoiding future outages. Additionally, if a technical problem occurs (e.g., the corruption of a data file) audit trails can aid in the recovery process (e.g., by using the record of changes made to reconstruct the file).

**3.Intrusion Detection:**

* 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 (or through the use of other kinds of warning flags/notices), or after the fact (e.g., by examining audit records in a batch process).
* Real-time intrusion detection is primarily aimed at outsiders attempting to gain unauthorized access to the system. It may also be used to detect changes in the system's performance indicative of, for example, a virus or worm attack.
* There may be difficulties in implementing real-time auditing, including unacceptable system performance.
* After-the-fact identification may indicate that unauthorized access was attempted (or was successful). Attention can then be given to damage assessment or reviewing controls that were attacked.

**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.
* If a system or application is deemed to be critical to an organization's business or mission, real-time auditing may be implemented to monitor the status of these processes (although, as noted above, there can be difficulties with real-time analysis).
* An analysis of the audit trails may be able to verify that the system operated normally (i.e., that an error may have resulted from operator error, as opposed

to a system-originated error). Such use of audit trails may be complemented by system performance logs.

**Q.2. List the principles of Auditing.**

**Ans:**

**Principles of audit:**

### 1.Audit planning & preparation:

* The auditor should be adequately educated about the company and its critical business activities before conducting a data center review.
* The objective of the data center is to align data center activities with the goals of the business while maintaining the security and integrity of critical information and processes.
* To adequately determine whether or not the client’s goal is being achieved, the auditor should perform the following before conducting the review:
* Meet with IT management to determine possible areas of concern
* Review the current IT organization chart
* Review job descriptions of data center employees
* Research all operating systems, software applications and data center equipment operating within the data center
* Review the company’s IT policies and procedures
* Evaluate the company’s IT budget and systems planning documentation
* Review the data center’s disaster recovery plan

### 2.Establishing audit objectives:

* The next step in conducting a review of a corporate data center takes place when the auditor outlines the data center audit objectives.
* Auditors consider multiple factors that relate to data center procedures and activities that potentially identify audit risks in the operating environment and assess the controls in place that mitigate those risks.
* After thorough testing and analysis, the auditor is able to adequately determine if the data center maintains proper controls and is operating efficiently and effectively.

Following is a list of objectives the auditor should review:

* Personnel procedures and responsibilities including systems and cross-functional training
* Change management processes are in place and followed by IT and management personnel
* Appropriate back up procedures are in place to minimize downtime and prevent loss of important data
* The data center has adequate physical security controls to prevent unauthorized access to the data center
* Adequate environmental controls are in place to ensure equipment is protected from fire and flooding.

### 3.Performing the review:

* The next step is collecting evidence to satisfy data center audit objectives. This involves traveling to the data center location and observing processes and procedures performed within the data center.

The following review procedures should be conducted to satisfy the pre-determined audit objectives:

* **Data center personnel** – All data center personnel should be authorized to access the data center (key cards, login ID’s, secure passwords, etc.). Data center employees are adequately educated about data center equipment and properly perform their jobs. Vendor service personnel are supervised when doing work on data center equipment. The auditor should observe and interview data center employees to satisfy their objectives.
* **Equipment** – The auditor should verify that all data center equipment is working properly and effectively. Equipment utilization reports, equipment inspection for damage and functionality, system downtime records and equipment performance measurements all help the auditor determine the state of data center equipment. Additionally, the auditor should interview employees to determine if preventative maintenance policies are in place and performed.
* **Policies and Procedures** – All data center policies and procedures should be documented and located at the data center. Important documented procedures include: data center personnel job responsibilities, back up policies, security policies, employee termination policies, system operating procedures and an overview of operating systems.
* **Physical security / environmental controls** – The auditor should assess the security of the client’s data center. Physical security includes bodyguards, locked cages, man traps, single entrances, bolted down equipment, and computer monitoring systems. Additionally, environmental controls should be in place to ensure the security of data center equipment. These include: Air conditioning units, raised floors, humidifiers and uninterruptible power supply.
* **Backup procedures** – The auditor should verify that the client has backup procedures in place in the case of system failure. Clients may maintain a backup data center at a separate location that allows them to instantaneously continue operations in the instance of system failure.

### 3.Issuing the review report:

* The data center review report should summarize the auditor’s findings and be similar in format to a standard review report.
* The review report should be dated as of the completion of the auditor's inquiry and procedures.
* It should state what the review entailed and explain that a review provides only "limited assurance" to third parties.

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

**Ans:**

The phases of a disaster recovery plan process are

  1.Awareness and discovery

  2.Risk assessment

  3.Mitigation

  4.Preparation

  5.Testing

  6.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.

**1.Awareness and Discovery:**

* Awareness begins when a recovery planning team can identify both possible threats and plausible threats to business operations. The more pressing issue for an organization in terms of business recovery planning is that of plausible threats.
* These threats must be evaluated by recovery planners, and their planning efforts, in turn, will depend on these criteria:

**•**  The business of the company.

**•**  The area of the country in which the company is located.

**•**  The company’s existing security measures.

**•**  The level of adherence to existing policies and procedures.

**•**  Management’s commitment to existing policies and procedures.

* Awareness also implies educating all employees on existing risk exposures and briefing them on what measures have been taken to minimize those exposures.
* Each employee’s individual role in complying with these measures should be addressed at this early stage.
* For example, in an educational environment, a system that is down for two or three days may not be considered catastrophic, whereas in a process control environment (e.g., chemicals or electronics), just a few minutes of downtime may be.
* Discovery is the process in which planners must determine, based on their awareness of plausible threats, which specific operations would be affected by existing exposures.

**2.Risk assessment**:

* Risk Assessment is one of the key components of disaster recovery planning.
* A major part of the disaster recovery planning process is the assessment of the potential risks to the organization which could result in the disasters or emergency situations themselves.
* It is necessary to consider all the possible incident types, as well as and the impact each may have on the organisation's ability to continue to deliver its normal business services.

**3.Mitigation**:

* Mitigation involves steps to reduce vulnerability to disaster impacts such as injuries and loss of life and property.
* This might involve changes in local building codes to fortify buildings; revised zoning and land use management; strengthening of public infrastructure; and other efforts to make the community more resilient to a catastrophic event.

**4.Preparation**:

Preparedness focuses on understanding how a disaster might impact the community and how education, outreach and training can build capacity to respond to and recover from a disaster. This may include [engaging the business community](http://restoreyoureconomy.org/preparedness/preparation-activites/business-community-engagement/), [pre-disaster strategic planning](http://restoreyoureconomy.org/pre-disaster-2/disaster-planning-for-economic-recovery/), and other logistical readiness activities. The [disaster preparedness activities](http://restoreyoureconomy.org/pre-disaster-2/disaster-planning-for-economic-recovery/) guide provides more information on how to better prepare an organization and the business community for a disaster.

 Develop a written preparedness, response and recovery plan.

 Keep the plan up-to-date, and test it.

 Keep the plan up-to-date, and test it.

 Keep together supplies and equipment required in a disaster and maintain them.

Establish and train an in-house disaster response team. Training in :

* + Disaster response techniques
	+ Identification and marking on floor-plans and enclosures of irreplaceable and important material for priority salvage.

 Prepare and keep an up-to-date set of documentation

 Distribute the plan and documentation to appropriate locations on- and off-site.

 Institute procedures to notify appropriate people of the disaster and assemble them rapidly.

**5.Testing**:

**6.Response and recovery**:

**Response:**

Response addresses immediate threats presented by the disaster, including saving lives, meeting humanitarian needs (food, shelter, clothing, public health and safety), cleanup, damage assessment, and the start of resource distribution.

As the response period progresses, focus shifts from dealing with immediate emergency issues to conducting repairs, restoring utilities, establishing operations for public services (including permitting), and finishing the cleanup process.

Follow established emergency procedures for raising the alarm, evacuating personnel and making the disaster site safe

Contact the leader of the disaster response team to 1 direct and brief the trained salvage personnel

When permission is given to re-enter the site, make a preliminary assessment of the extent of the damage, and the equipment, supplies and services required.

Stabilize the environment to prevent the growth of mould. Photograph damaged materials for insurance claim purposes.

Set up an area for recording and packing material which requires freezing, and an area for air- drying slightly wet material and other minor treatment.

Transport water-damaged items to the nearest available freezing facility

**Recovery:**

[Recovery](http://restoreyoureconomy.org/recovery/) is the fourth phase of disaster and is the restoration of all aspects of the disaster’s impact on a community and the return of the local economy to some sense of normalcy. By this time, the impacted region has achieved a degree of physical, environmental, economic and social stability.

Establish a programme to restore both the disaster site and the damaged materials to a stable and usable condition.

Determine priorities for restoration work and seek the 1 advice of a conservator as to the best methods and options, and obtain cost estimates.

Develop a phased conservation programme where large quantities of material are involved.

Discard items not worth retaining, and replace or rebind items not justifying special conservation treatment.

 Contact insurers.

Clean and rehabilitate the disaster site. Replace treated material in the refurbished site.

Analyse the disaster and improve the plan in the light of experience.

**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 is authorized access to what system resources. 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.Identification and Authentication**:

* Audit trails are tools often used to help hold users accountable for their actions. To be held accountable, the users must be known to the system (usually accomplished through the identification and authentication process).
* However, as mentioned earlier, audit trails record events and associate them with the perceived user (i.e., the user ID).
* If a user is impersonated, the audit trail will establish events but not the identity of the user.

**4.Logical Access Control**:

* Logical access controls restrict the use of system resources to authorized users. Audit trails complement this activity in two ways.
* First, they may be used to identify breakdowns in logical access controls or to verify that access control restrictions are behaving as expected, for example, if a particular user is erroneously included in a group permitted access to a file.
* Second, audit trails are used to audit use of resources by those who have legitimate access.
* Additionally, to protect audit trail files, access controls are used to ensure that audit trails are not modified.

**5.Contingency Planning**:

* Audit trails assist in contingency planning by leaving a record of activities performed on the system or within a specific application.
* In the event of a technical malfunction, this log can be used to help reconstruct the state of the system (or specific files).

**6.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?

**7.Cryptography**:

* Digital signatures can be used to protect audit trails from undetected modification. (This does not prevent deletion or modification of the audit trail, but will provide an alert that the audit trail has been altered.)
* 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:**

* Cost Considerations 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 (and cheaply) 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.
* (If complex tools are not available for a system, development may be prohibitively expensive. Some intrusion detection systems, for example, have taken years to develop.)
* 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:**

**Refer Q.7(2)**

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

**Ans:**

* **Audit Trails:**

A record showing who has accessed a [computer system](http://www.webopedia.com/TERM/C/computer_system.html) and what operations he or she has performed during a given period of time. Audit trails are useful both for maintaining [security](http://www.webopedia.com/TERM/S/security.html) and for recovering lost transactions. Most accounting [systems](http://www.webopedia.com/TERM/S/system.html) and[database management systems](http://www.webopedia.com/TERM/D/database_management_system_DBMS.html) include an audit trail component.

A system can maintain several different audit trails concurrently. 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.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.

**2.Audit Events**:

* System audit records are generally used to monitor and fine-tune system performance.
* Application audit trails may be used to discern flaws in applications, or violations of security policy committed within an application. User audits records are generally used to hold individuals accountable for their actions.
* An analysis of user audit records may expose a variety of security violations, which might range from simple browsing to attempts to plant Trojan horses or gain unauthorized privileges.

**a.System-Level Audit Trails**:

* If a system-level audit capability exists, the audit trail should capture, at a minimum, any attempt to log on (successful or unsuccessful), the log-on ID, date and time of each log-on attempt, date and time of each log-off, the devices used, and the function(s) performed once logged on (e.g., the applications that the user tried, successfully or unsuccessfully, to invoke).
* System-level logging also typically includes information that is not specifically security-related, such as system operations, cost-accounting charges, and network performance.

**b.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 (or the data element(s) changed within a record) should be captured by the audit trail.

**c.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.8. List the steps to perform information security audit.**

**Ans:**

**1.Preparing the IS audit (Step 1)**:

* When initiating an IS audit (for example by the IT Security Officer or the person responsible for IS audits), the management of the organisation to be examined must participate. In this stage, the object to be examined is specified, the contract is awarded, and the IS audit team contracted is granted the necessary authorisations (for example authorisation to view documents).
* The following reference documents must be provided to the IS audit team by the organisation to be audited since they form the basis for the IS audit:

**Organisational documents:**

- Organigram

- IT framework concept

- Schedule of responsibilities

**Technical documents:**

- Security concept

-Export of the information security management database

-The security policy

- List of the critical business processes

- The IS audit reports from the previous six years

**2.Creating the IS audit plan and screening documents (Step 2):**

* All reference documents are to be checked for completeness and up-to-dateness. When evaluating the up-to-dateness of the documents, note that some documents are more generic than others so that updates in the documents may be required more or less often, depending on the document.
* However, the organisation must evaluate all documents regularly to see if they correspond to the current conditions.
* The IS audit team checks this procedure by screening documents and where appropriate by comparing them to the results of the on-site examination.
* In terms of completeness, the contents of the documents are to be checked to see if all major aspects have been documented and if suitable roles have been assigned.

**3.Examining documents and updating the IS audit plan (Step 3):**

* The document examination is performed based on the safeguards specified in the IS audit plan. The examination of the documents focuses primarily on the completeness and understandability of the documents.
* If possible, the appropriateness of the safeguards to be examined should be evaluated. In terms of completeness, the documents must be examined to ensure all major aspects (for example systems, networks, IT applications, and rooms) were documented and if the roles described were actually assigned.
* The evaluation of the appropriateness includes an evaluation of the personnel, organisational, and technical safeguards in terms of their effectiveness.

**4.On-site examination (Step 4):**

* The goal of the on-site examination is to compare and check the documents presented, for example the concepts and guidelines, with the actual conditions on-site to see if information security is guaranteed in an adequate and practical form with the selected safeguards. The procedure follows the IS audit plan.

**5.Evaluating the on-site examination (Step 5):**

* After the on-site examination, the information obtained is consolidated further and evaluated. The evaluation can also be performed by external experts if the required expert knowledge is not covered by the IS audit team.
* If external experts are contracted, then it is necessary either to obtain the permission of the organisation audited, or to make the information anonymous so that no conclusions can be drawn regarding the organisation or its personnel.
* The evaluation of the information is incorporated into the overall evaluation of the safeguard tested.
* After the evaluation of the documentation requested and the additional information, a final evaluation of the safeguards tested is performed and the results are summarised in an IS audit report.

**6.Producing the IS audit report (Step 6):**

* The IS audit report, including the reference documents, is to be provided in writing to the management of the organisation audited or the client, the person responsible for IS audits, and the IT Security Officer.

**Part 0**: This part contains the organisational information.

**Part 1**: is the management summary.

**Part 2**: provide a graphical representation of the results of the audit

**Part 3**: This part of the IS audit report contains the detailed descriptions of the subject areas tested and the facts determined together with the technical details and recommendations.

**Q.9. What are the implementations issues regarding Audit Trail?**

**Ans:**

* **Implementation Issues:**
* Audit trail data requires protection, since the data should be available for use when needed and is not useful if it is not accurate. Also, the best planned and implemented audit trail is of limited value without timely review of the logged data.

Following are examples of 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; however, security and/or administration personnel who maintain logical access functions may have no need for access to audit logs.
* 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**.
* The audit trail files needs to be protected since, for example, intruders may try to "cover their tracks" by modifying audit trail records. Audit trail records should be protected by strong access controls to help prevent unauthorized access.
* The integrity of audit trail information may be particularly important when legal issues arise, such as when audit trails are used as legal evidence.
* The confidentiality of audit trail information may also be protected, for example, if the audit trail is recording information about users that may be disclosure-sensitive such as transaction data containing personal information (e.g., "before" and "after" records of modification to income tax data).

**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.
* Reviewers should know what to look for to be effective in spotting unusual activity. They need to understand what normal activity looks like.
* 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.
* Audit Trail Review After an Event.
* Periodic Review of Audit Trail Data.
* Real-Time Audit Analysis.

**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, as well as to distill useful information from the raw data.
* 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.

Some of the types of tools include:

**a.Audit reduction tools** are preprocessors designed to reduce the volume of audit records to facilitate manual review.

**b.Trends/variance -detection tools** look for anomalies in user or system behavior. It is possible to construct more sophisticated processors that monitor usage trends and detect major variations.

**c.Attack signature-detection tools** look for an attack signature, which is a specific sequence of events indicative of an unauthorized access attempt.

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

**Ans:**

 **Refer Q.4**

**Q.11. Explain the concept of Business Continuity Planning with its different**

 **phases.**

**Ans:**

* **Business Continuity Planning:**
* **Business continuity planning** (or **business continuity and resiliency planning**) is the process of creating systems of prevention and recovery to deal with potential threats to a company.
* A [business continuity](https://en.wikipedia.org/wiki/Business_continuity) plan is a plan to continue operations if a place of business is affected by different levels of disaster which can be localized short term disasters, to days long building wide problems, to a permanent loss of a building.
* Such a plan typically explains how the business would recover its operations or move operations to another location after damage by events like [natural disasters](https://en.wikipedia.org/wiki/Natural_disaster), [theft](https://en.wikipedia.org/wiki/Theft), or flooding.
* For example, if a fire destroys an office building or data center, the people and business or data center operations would relocate to a recovery site.



* **Phases of Business Community Planning:**

**Phase 1: Identify the risks:**

* The first phase is to conduct a risk assessment, identifying any potential hazards that could disrupt your business. Consider any type of risk your team can imagine, including natural threats, human threats and technical threats.

**Phase 2: Analyze the risks you face:**

* Next, you’ll perform a business impact analysis (BIA) to gauge the impact of each potential risk. For each risk, determine how severe the impact would be and how long your business could survive without those processes running.
* Consider what is absolutely necessary for recovery, how quickly it needs to happen, what are your minimum operating resources are and any dependencies, either internal or external.

**Phase 3: Design your strategy:**

* Now it’s time to figure out strategies to mitigate interruptions and to quickly recover from them.
* Consider everything you’ll need to protect your people, your assets and you’re your functions.
* Start by comparing your current recovery capabilities to your business requirements and plzn how you will fill that gap.

**Phase 4: Plan development and execution:**

* Finally, it’s time to create a concise, well organized and easy-to follow document or set of documents.
* Consider everyone that may use the plan, and document it in a way that will be most useful when your business is suffering an interruption. Then publish the plan, socialize it and train your staff on how to use it

**Phase 5: Measure your success by testing:**

* A plan isn’t truly a plan until it has been thoroughly tested. There are a variety of tests you should perform, with each providing different information on how to improve your plan.
* Tests can range from a checklist test, a walk-through performed by you your team as if there were an actual event, emergency evacuation drills, and when ready, a full on recovery simulation test is a bit more complex and involves your team simulating and emergency and using the actual equipment, facilities and supplies just as in a real disaster.
* After each test, you can make any necessary modifications to your plan to keep it current.

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

 **in industry.**

**Ans:**

# Business continuity planning:

* Business continuity planning involves developing a practical plan for how our business can prepare for, and continue to operate after an incident or crisis.
* A business continuity plan will help you to:
* identify and prevent risks where possible
* prepare for risks that we can't control
* respond and recover if an incident or crisis occurs.
* Preparing a business continuity plan will help our business recover quickly if an incident does happen. We may not be able to predict every kind of incident that could threaten your business, but we can develop a plan that covers a range of incidents (e.g. natural disasters, computer problems, staffing issues).
* To get the most out of a business continuity plan, we should include a schedule for testing and updating it, making sure we take into account any changes to our business, our industry, or the location we operate in.
* A business continuity plan includes information on the distribution of our plan.

### Distribution list:

The distribution list details:

* where copies of the plan are stored (including e-records stored off site), in case your original copy is destroyed or unreachable in an incident
* who needs a copy of the plan
* any other associated documents and plans (e.g. an [evacuation plan](https://www.business.qld.gov.au/business/running/disaster-resilience-and-recovery/preparing-business-natural-disaster/cyclone-evacuating-business)) and checklists for specific incidents (e.g. [natural disasters](https://www.business.qld.gov.au/business/running/disaster-resilience-and-recovery), [pandemics](https://www.business.qld.gov.au/business/running/disaster-resilience-and-recovery/pandemic-risk-management-for-business)).
* **Recovery Plan:**
* The recovery plan outlines the steps we will need to take to get our business running again after an incident or crisis. It includes a realistic time frame in which we can get our operations back on track to minimise financial losses.
* A recovery plan will help us respond effectively if an incident or crisis affects your business. It aims to shorten our recovery time and minimise losses.
* Our recovery plan contains information relating to planning for recovery as well as the resumption of critical business activities after a crisis has occurred.
* It also outlines the time frame in which we can realistically expect to resume usual business operations.
* Developing a recovery plan gives us a chance to consider how we will get our business back on track if we do experience a crisis. It should include:
* strategies to recover your business activities in the quickest possible time
* a description of key resources, equipment and staff required to recover your operations
* your recovery time objectives
* a checklist you can use after a crisis has passed and it is safe to return to your premises.

**Q.13. Explain the various backup & recovery techniques for applications.**

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

**Ans:**

### Logical security audit:

* The first step in an audit of any system is to seek to understand its components and its structure.
* 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:

**1.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.

**2.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.

**3.Special User Accounts**:

* Special User Accounts and other privileged accounts should be monitored and have proper controls in place.

**4.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 Q.7.**