WEEK 5 IT INFRASTRUCTURE MANAGEMENT

1.Discuss in detail about the Release Management.

Release management refers to the process of planning, designing, scheduling, testing, deploying, and controlling software releases. It ensures that release teams efficiently deliver the applications and upgrades required by the business while maintaining the integrity of the existing production environment.

Release and Deployment management is one of the main processes under the Service Transition section of the Information Technology Infrastructure Library (ITIL) framework. ITIL is the most widely adopted framework for the governance of technology products and services. It helps organizations deliver their products and services in a quality-driven, customer-centric and cost-conscious way.

Release the Management Process

The specific steps of release management will vary depending on the unique dynamics of each organization or application. Nevertheless, the following sequence is the most common.

Request

Release management starts with requests for new features or changes to existing functions. There's no guarantee that all requests made will eventually translate into a new release. Each request is evaluated for its rationale, feasibility, and whether there's a way to fulfill it by reconfiguring the application version already in production.

Plan

This is the most important step in a release's evolution. It's here that the release's structure is defined. A robust plan ensures the release team stays on track and that requirements are satisfied. Create or reuse a workflow or checklist that can be referred to by stakeholders throughout the release process. The workflow should detail not just scope and milestones but responsibilities.

Design and Build

This is the programming phase where the requirements are converted to code. The release is designed and built into executable software.

Testing

Once the release is deemed ready for testing, it's deployed to a test environment where it's subjected to non-functional and functional testing (including user acceptance testing or UAT). If bugs are found, it's sent back to developers for tweaking then subjected to testing again. This iterative process continues until the release is cleared for production deployment by both the development team and the product owner.

Deployment

The release is implemented in the live environment and made available to users. Deployment is more than just installing the release. It entails educating users on the changes and training them on how to operate the system in the context of the new features.

Post-Deployment

Post-deployment, the release moves to the support phase where any bugs are recorded that will eventually necessitate a request for changes. The cycle thus begins again.

For a release to be deemed successful, it must attain the following objectives:

- It's deployed on time.
- It's deployed within budget.
- It has little to no impact on current users.
- It satisfies the needs of current and new users, technological advances and/or competitive demands.

2. What are the processes involved in Capacity Management?

Process involved in Capacity Management

- Capacity management aims to prevent surprises and rushed purchases by making better use of the available resources and to increase capacity at the right time.
- Implementation of capacity management helps in preventing unnecessary investments and adhoc capacity changes.
- There are three main sub-processes involved in capacity management.

1 Business Capacity Management

- ❑ It is a part of capacity management activity which is responsible for ensuring that the future business requirements for IT services are well considered, planned and implemented in a cost effective and timely manner.
- ❑ Business capacity management is strongly connected to service level management and works jointly with the business planning efforts of the organization.

2 Service Capacity Management

- ❑ Service capacity management addresses the issues of IT services.
- ❑ It is responsible for ensuring that the performance of all services is monitored and measured properly, as discussed in service level management.

3 Resource Capacity Management

- ❑ Resource capacity management concentrates on the technology components and supports the service provisions.
- ❑ It ensures that all components with declared finite resources are monitored and measured accurately.
- ❑ Also, Resource capacity management is referred as component capacity management in ITIL version 3.

3. Write down the advantages of IT Service Continuity Management?

ADVANTAGE :

- IT service continuity management is the process by which plans are formulated and managed to ensure that IT services can recover and continue in case of a serious incident.
- The guidelines of IT service level management can be used to limit and manage the impact of disasters.
- If a disaster occurs, businesses with an IT service continuity management process have the following advantages:
    - Organizations implementing service continuity management can manage recovery of their systems.
    - Organizations lose less time for service availability and offer better continuity to the users if they use IT service continuity management.
    - It minimizes the interruption to their business activities.
    - It defines proactive measures to reduce the risk of a disaster in the first instance.
    - It is regarded as the recovery of the IT infrastructure used to deliver IT services.

4. Classify the four important process involved in implementation of IT service continuity management.

The process flowchart of IT service continuity management process is given in below figure.

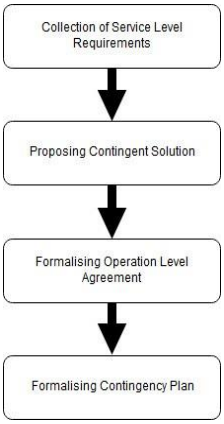

Figure 1 Process Flowchart of IT Service Continuity Management

- **Collection of Service Level Requirements**
  - Once risks are known, users take the help of IT to decide which risks are to be minimized and which ones are to be assumed.
  - Since, in order to reduce a risk, one needs to handle many resources like people, time and money; IT management takes the necessary steps to determine a risk which is so small that it does not want to incur much cost to minimize it.
  - IT service continuity management begins by cautiously agreeing to availability targets with the customer and determining the cost of downtime or unavailability of the concerned IT service, so that a realistic and effective IT budget can be setup.
  - It is also desirable that the negotiation contains realistic expectations of reduced system availability while the contingency plan is in place.
  - This process needs an element of education and negotiation on both sides, i.e., the customer and the IT organization.
  - To implement IT service continuity management effectively, customers need to understand the methods that they can use to define their availability requirements, and IT organization needs to understand the functions required for providing IT services and which of them are the most critical.
  - Effective implementation of IT service continuity management requires consideration of following two steps.
  - Identify Information Technology Service Layers

- To find out the probable places where risk may be introduced, IT environment needs to be broken down into some logical components.
- To do this, services provided by an organization can be divided into layers.

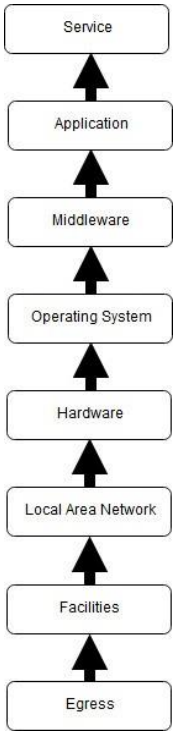

Figure 2 IT Stack for the Services

- In the layered structure, an IT service can be delivered only if all the services underneath are functioning.
- The figure below presents an example of layers (IT stack) for the services provided by an IT department.

o Identify Risk to Each Information Technology Service Layer

- Single point of failure can be identified by inspecting possible risk vulnerabilities of each layer in the IT stack.
- Also, one can identify a single layer that may address risk on the layers above.
- An example of risk assessment is given in Table below, which addresses the risk involved in some of the layers shown in above figure.

Risk	Fire	Flood	Virus	Power Outage	Logon Failure	Lack of Staff	Human Err
Egress				Medium			
Facilities	Medium	Low					
Network							
Hardware			Low				
Operating System							
Middleware							
Application							
Service							

Figure 3 Risk Assessment Table

- The first column of this table provides the names of various possible risks while rest of the columns give the level of risk present at various layers.
- Risk levels are categorized into three types, namely, Low, Medium and High, representing low, medium and high level of risk respectively.
- Empty cell in the table shows that a risk does not affect that particular layer.

❑ **Proposing Contingent Solution**

- Once the possible risk factors for the important business process have been recognized and their relative importance and financial implications are understood, one can start preparing its contingency plan.
- IT service continuity management ensures that the services are available in the case of a service interruption, irrespective of the cause of the disruption.
- Service continuity involves two main processes: Failover and Restoration.
- **Failover** - It is an act of automatic or manual movement of the operations of a component from its primary location to a secondary location.
- Following two examples illustrate automatic and manual failover.

Example 1 (Automatic Failover):

- Assume that computer has dual redundant power supplies.
- At the time of normal operation, each supply provides half the load required by the system.

- When one of the supplies fails or goes off, the other automatically starts supplying all the power to the system.
- This is an example of automatic failover.

Example 2 (Manual Failover):

- Consider a data center site which has got destroyed by a natural calamity.
- In this situation, the whole IT infrastructure must be recreated at a new place located at some distance away.
- This needs manual intervention and comes under manual failover.

- **Restoration** - It involves the act of bringing the operation of a component back from the secondary location to the primary location.
- This is an important activity and must be carefully dealt with while creating a contingency plan.
- Usually, it has been found that organizations have detailed plans for moving the service to a new location in case of an emergency, but they rarely have any plan to restore the service back to the original location when the time comes.

❑ **Formalising Operation Level Agreement**

- Once IT department of an organization and the customer agree on a cost-effective level of service continuity, an agreement needs to be formalized between various internal support groups of an organization.
- This agreement is called an Operation Level Agreement (OLA).
- The OLA is an important building block for the Service Level Agreement (SLA) and defines the interdependent relationships among the internal support groups of an IT organization working to support a service level agreement.
- The main objective of the OLA is to present a clear, concise and measurable description of the internal support relationships of the service provider.
- While SLA is a legal document formalized between IT and its customers, OLA is an agreement between the IT entities within the organization.
- It should be understood that OLA is not the substitute for SLA.
- OLA has to be considered as the basis of good practice and common agreement; however, some portions of it which may contribute to an SLA.
- Following are few important components that an OLA should include:

(i) Definition of the business processing

(ii) Impact of downtime or non-availability of IT services on business

(iii) The cost of downtime or non-availability and the way these costs can change over time

(iv) Minimum performance characteristics and hours of service required

(v) Critical periods of service, where downtime is intolerable

(vi) Less critical periods of service, where downtime is more tolerable

(vii) Scheduled downtime periods for planned maintenance

(viii) Amount of downtime can be tolerated before contingency plans should be invoked

(ix) Number of users.

- The service level manager is ultimately responsible for the agreement and the documentation (SLA, OLA) of service levels with the customers.

- **Formalising Contingency Plan**

  - The contingency plan is like a guide for the IT personnel which is to be used to failover and recover the service in case of a disaster.
  - This document includes the information on escalation and notification procedure, start up and shut down procedures, communication methods and status reporting requirements.
  - These procedures are discussed in detail below.
  - It is also required that the document containing contingency plan should discuss the levels of contingency (level increases as the severity of the problem increases) and the procedure to be used to define the levels of contingency.
  - This helps in taking the appropriate measures to handle any emergency situation.