# V20PCA107 - IT INFRASTRUCTURE MANAGEMENT 2.0

## UNIT - II_WEEK - 5

## Scope of Financial Management for IT Services

Usually, a specifically dedicated department within the IT service provider owns financial management for IT Services. They typically report directly to the Chief Information Officer (CIO) or the Chief Financial Officer (CFO). There are 3 core aspects of financial management, each of which has an annual planning cycle and a monthly operation monitoring and reporting cycle.

**1. Accounting:** It consists of the mechanisms by which the IT service provider accounts to the organization for the money spent.

**2. Budgeting:** It involves prediction and controlling of the service provider's income and expenditure which are achieved through periodic negotiation cycles. During this period, budgets are set annually, and actual financial performance against these budgets is reported monthly.

**3. Charging:** It involves the IT service provider billing its customers for the service provided.

## Value of Financial Management for IT Services

Financial management for IT services enables and enhances the ability of the service provider to make decisions, making them more agile and effective. At the same time, it ensures that they are financially compliant and have robust control.

Service providers invest in financial management to make sure that their business is conducted in a manner which is financially responsible, which allows the organization to operate within the legal limits and in the absence of penalties for non-compliance. This results in increased accuracy in planning and forecasting and a better understanding of the actual costs and value of each IT service.

Process activities of financial management for IT services: The process activities for financial management of IT services include accounting, budgeting and charging (ABC).


1. **Accounting** of the process of accounting allows an IT organization to account for its expenditures.
    - It tracks the income from IT services against the actual costs of delivery, comparing the actual costs with budgets and managing any variance.
    - An accounting process which is efficient will increase IT service provision and define the areas where costs can be saved, and financial efficiency can be increased.
    - The cost elements used for accounting are:

    **Capital Costs:** It is the cost of making a purchase which will become a financial asset. Ex: Purchase of a server

    **Operational Costs:** It is the cost of running a service which includes the use of electricity, employee salary, etc. Ex: Cost to keep the server running

    **Direct Costs:** These are the costs which can be applied directly to a particular service or customer. Ex: Purchase of a server to be used for a particular service.

    **Indirect Costs:** These are the costs which cannot be allocated to a particular service or customer directly. Ex: Software license for a server which runs several applications.

    **Fixed Costs:** These are the costs that don't change with the usage of IT services or in the short-term. Ex: An annual lease contract.

    **Variable Costs:** The costs which vary in the short term in accordance with the service usage are variable costs. Ex: Energy utilized to run servers

2. **Budgeting**

   o Budgeting is a process which plans the income and expenditure of money in a company.

   o The activity involves predicting and controlling the spreading of money including:

   ▪ Analysis of prior budgets

   ▪ Assessment of plans

   ▪ Cost and income estimation

   ▪ Producing budgets

Based on this information, measures are taken to implement corrections to keep the budget on track.

3. **Charging**

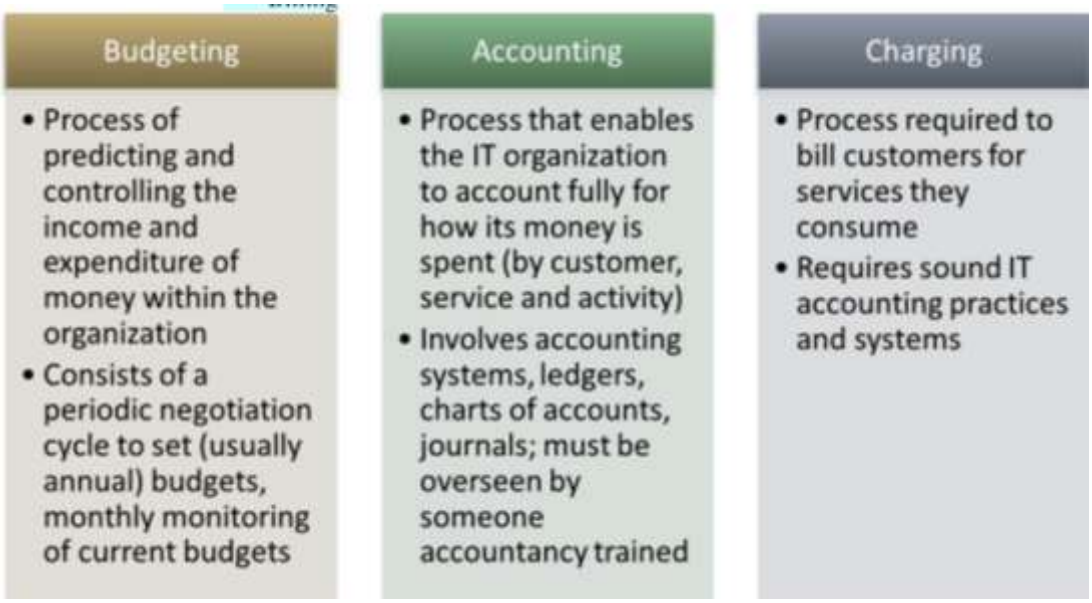
   - This is an activity where payment is needed for the services which are delivered.
   - Services are charged for depending on the type of service provider in question.
   - Charging is optional for internal providers depending on the overall financial policies of the enterprise.
   - for external service providers, charging is compulsory as is the only way by which the service provider makes a profit. o Charging encompasses the following

     ▪ Charging policies

     ▪ Chargeable items

     ▪ Pricing

     ▪ Billing




## Challenges Faced by Financial Management for IT Services

The challenges faced by financial management for IT services are:

• To shift focus from cost optimization to cost reduction.

• Financial reporting can focus too heavily on the cost of infrastructure and applications rather than the total cost of the services.

• The difficulties are involved in introducing internal charging for IT services as it will require a change in culture, the way in which IT service success is measured and the way in which value is articulated.

• The chart of accounts for financial management for IT services needs to be suitable and applicable to the requirements of an IT provider and not just conformant with the overall policies of financial management.

## Risks of Financial Management for IT Services

The risks taken by during financial management of IT services are:

- A lack of access to staff that is sufficiently skilled and qualified to understand the world of an IT service provider and the world of cost accounting.
- Exposure to penalties for not complying with legislative and regulatory requirements.

- The possibility of making ill-informed decisions due to a lack of dedicated financial management for IT service resources.

## IT Service Continuity Management

Service continuity management is a reactive and proactive process which involves contingency planning for recovery in case the Information and communication technology service is damaged or put out of action by a sudden disaster.

## Purpose of IT Service Continuity Management

The main purpose of the IT service continuity management is to support the overall business continuity management process by making sure that the IT service provider is always capable of providing minimum levels of business continuity related service.

## Objective of IT Service Continuity Management

The objectives of IT service continuity management (ITSCM) are:

- To provide advice and assistance on issues which are related to continuity and recovery.
- To maintain a set of plans on IT service continuity and IT recovery which are in support of the overall business continuity plans. They should also perform business impact analysis, risk analysis, and management activities on a regular basis.
- To minimize the costs which cannot be eliminated.
- To make sure that suitable continuity mechanisms are installed which can meet or exceed the agreed upon targets of business continuity.
- Analyze the impact which the changes have had on the IT service continuity plans.
- Make sure that proactive measures are implemented wherever it is economical, which will increase the availability of services.
- Perform negotiations and agree on contracts with the suppliers to provide the required recovery capability.

## Scope of IT Service Continuity Management

IT service continuity management supports the activities of the business continuity management process and focuses only on those events which are considered by the business to be a 'disaster.' Minor technical issues are not covered under this as they are addressed through the incident management process. Availability management also addresses these minor issues in the design of services for availability and recovery.

IT service continuity management usually does not address long-term risks such as changes in business direction, diversification, restructuring, directly. Instead, when there is time to evaluate the risk, it addresses them using an IT change management program.

## Value of IT Service Continuity Management

The following benefits are provided by implementing Service Continuity Management:

- ✓ In case of an accident or a disaster, the Information and communication technology (ICT) services can be restored in the appropriate order of importance to ensure that the most vital services are up and running soon.
- ✓ The ready nature of the contingency plan allows us to save time and react quickly or recover quickly from an accident or a disaster.
- ✓ The organization can be mentally prepared for a disaster as service continuity management allows us to project disaster scenarios beforehand.
- ✓ There is a clear understanding of the importance of Information and communication technology (ICT) services and their rank Principles and Basic Concepts of IT Service Continuity Management Business continuity plan (BCP).
- ✓ A business continuity plan outlines and defines the steps which are needed to restore the business processes after they have been disrupted.
- ✓ It also identifies the triggers for invocation, the people who need to be involved, communications, etc.
- ✓ A significant part of Business Continuity Plans consists of IT service continuity plans. Business continuity management (BCM).
- ✓ The role of business continuity management is to manage risks which can have a serious impact on the business, bring them down to an acceptable level and

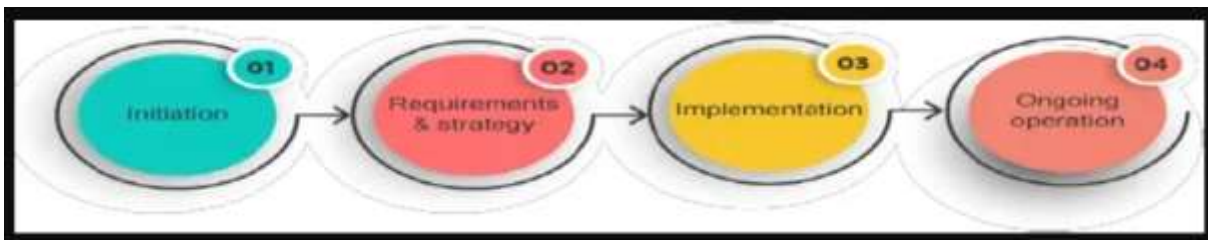
plan for the recovery of business processes if a business disruption occurs. Business impact analysis (BIA).

The main purpose of business impact analysis is to quantify the impact that loss of service would have on a business. It identifies the following:

- The form which will be taken by the damage or loss.
- The way in which the degree of loss or damage is likely to increase following a service disruption.
- The staff, skills, facilities, and services which are needed to make sure that the viral business processes continue to operate at minimum acceptable levels.
- The time within which the minimum levels of staff, facilities and services should be recovered.
- The priority assigned to each business during recovery.

## Implementation Procedure of IT Service Continuity Management

Service Continuity Management is a process which can evolve over time and not necessarily an end-to-end task which has to be finished to possess some value. Service continuity management must be developed over time. The steps taken to implement service continuity management in an organization are:




**Step 1: Identify Services and Assets** of Firstly, all the services and assets in our possession need to be identified. Assets are the main component of services.

Services and assets can be any of the following:

| Service | Assets |
|---|---|
| Printing | Printer |
| Word Processing | Computer, software |
| Internet | Computer, LAN, WAN, ISP |
| Data storage | Server, Hard disk |
| Technical Support | Procedures, Staff |

• This information is gathered in the Framework for ICT Technical Support (FITS) processes. • FITS Service Level Management should be implemented to understand the criticality of the services in possession.

• FITS Configuration Management should be implemented to get an idea about the main assets.

**Step 2: Identify Risks and Threats**

• Once the services and assets have been identified, the risks and threats should be identified.

• What can happen to the services and assets are categorized as risks and the causes which make it happen are categorized as threats.

| Risks | Threats |
|---|---|
| Loss of internal ICT services/assets | Fire, power failure, power surge, virus, accidental damage |
| Loss of external ICT services | Overload of external communication links, bankruptcy. |
| Loss of data | Technical failure, virus, human error, accidental damage |
| Unavailability of key technical and support staff | Sickness, transportation problems, resignation |
| Failure of service providers | Bankruptcy, loss of service provider's own data |

**Step 3: Make Contingency Plans**

• Contingency plans are like insurance policies.

• They can be simple & cost effective and can cover minor risks, or they can be complicated & expensive and cover major risks.

• The type of contingency plan which should be implemented depends on the level of risk which the company is taking.

• These plans involve prioritizing the services to be restored first, creating backups and storing them on-site and off-site.

**Step 4: Document the Recovery Plan**

• The recovery plan should be documented properly to ensure that all the essential information is present in it.

• This plan should be circulated among the key staff, who should be kept up to date regarding any changes in the plan.

• A copy of the plan should be given to the recovery team as well.

• Another copy of the recovery plan should be stored off-site to make it accessible in an emergency.

**ROLES AND FUNCTIONS OF IT SERVICE CONTINUITY MANAGEMENT**

1. **Service Continuity Manager**

   - Handles the responsibility of service continuity
   - Owns the service continuity management process
   - Leads the service continuity recovery plan's development
   - Invokes the service continuity recovery plan personally
   - Is a senior member of the ICT or technical support staff
   - Has no need to be technical
   - Should understand the ICT priorities of the users.
   - Should appoint someone else to cover during absence
   - Should not delegate responsibility

2. **Service Continuity Recovery Team**

- Is led by the service continuity manager
- Participates in the testing and invocation of the service continuity recovery plan.
- Includes the technical staff for technical procedures
- Includes users for testing and during the actual invocation
- Includes representatives from the departments for communication and coordination

## Process Activities of IT Service Continuity Management

To set up and operate IT service continuity management, a lifecycle approach should be adopted. The stages of the lifecycle approach from the foundation for the IT service continuity management are:


**1. Initiation**

The key activities in the initiation stage are:

- Policy setting
- Scope definition
- Initiate a project

**2. Requirements & Strategy**

The key activities in the requirements & strategy stage are:

- Business impact analysis
- Risk assessment

- IT service continuity strategy

3. **Implementation**

   The key activities in the implementation stage are:

   - Develop IT service continuity plans
   - Develop IT plans, recovery plans, and procedures
   - Organizational planning
   - Risk reduction and recovery
   - Implementation
   - Initial testing

4. **Ongoing Operation**

   The key activities in the ongoing operation stage are:

   - Education, awareness, and training
   - Review & audit
   - Testing
   - Change management

## Challenges of IT Service Continuity Management

The challenges involved in IT service continuity management are:

• Creating appropriate IT service continuity management plans when there is no overall business continuity management processes or plans.

• The IT department must educate the business to adopt the appropriate best practices the area.

• If IT plans are developed without taking business plans into account, they may be inappropriate. In the event of a disaster, the blame for failure will be placed on the IT department.

## Risk of IT Service Continuity Management

The risks faced by IT service continuity management are:

• Lack of a business continuity management process

• Lack of commitment from the business to the IT service continuity management process. • Lack of appropriate information on the future and strategies of the business.

• The plans of IT service continuity management can become outdated and misaligned with the information and plans of the business and business continuity management.

IT Service Continuity Management thus performs its role of providing advice and assistance on various continuity and recovery issues along with maintaining a set of plans on IT service continuity and IT recovery which support the overall business continuity plans. It helps to minimize the costs which cannot be eliminated and while ensuring that proactive measures are implemented wherever it is economical.