ITIL v3

Section 1

Service Design & Service Transition

Phases of Lifecycle in ITIL

1. **Service Strategy** : Describes business goals and customer requirements and how to align objectives of both entities.
2. **Service Design** : Outlines practices for the production of IT policies, architectures and documentation.
3. **Service Transition :** Advises on change management and release practices, and also guides admins through environmental interruptions and changes.
4. **Service Operation :** Offers ways to manage IT services on a daily, monthly and yearly basis.
5. **Continual Service Improvement :** Covers how to introduce improvements and policy updates within the ITIL process framework

Service Design

- **Service Design** provides a blueprint for the services. It not only includes designing of a new service but also devises changes and improvements to existing ones.
- IT Services designed to meet business objectives.
- Services designed to be both fit for purpose and fit for use.
- Cost of ownership planned to achieve return on investment.

Design Coordination

- It deals with maintaining policies, guidelines, standards, and budget for service design activity.
- The central principles in design coordination are balance, prioritization and integration with project management.
- Balance and prioritization address the utility and warranty of a service, as well as the needs of the service throughout its lifecycle.

Design coordination handles managing resources needed by the Service Design phase of the lifecycle. This includes:

- Planning to ensure that adequate resources are available
- Design coordination is accountable for the production of the service design package (SDP)
- Scheduling access to resources among the many projects that may be in this phase at any one time

It is accountable for the performance and improvement of the Service Design phase of the lifecycle.

Service Catalogue Management

- This process is responsible for designing service catalogue containing service specific to the customer for which they are willing to pay.
- Service catalog management ensures that an accurate and up-to-date service catalog is available to all parties authorized to see it.
- All parts of IT Service Management, as well as customers and users, use the service catalog. Accuracy and availability are essential

- Service catalog management must work closely with service portfolio management as new services move from the pipeline into the catalog and older services are retired.
- It also helps define how services can be requested and what options are available (gold/silver levels, for instance). The service catalog should document all defined services.

The service catalog generally comprises two views:

- a business service view that is visible to the customer
- a technical service view that is visible only to IT personnel.

This enables the customer to choose services based on their business requirements. At the same IT personnel can use their view to determine what technical services they need to support a given business service.

Service Level Management

- The goal of this process is to ensure that quality of the services meet provisioned quality agreement

The service level management (SLM) process focuses on researching and understanding requirements. Areas include:

- Defining, negotiating, agreeing upon and documenting IT service targets
- Monitoring, measuring and reporting on how well the service provider delivered the agreed upon targets

- When targets are appropriate and met, then the business and IT have a better chance of becoming aligned.
- Agreed upon targets are often spelled out in service level agreements (SLAs). Monitoring, measuring and reporting on SLA's in this way provides close links to Continual Service Improvement (CSI).
- SLAs are agreements to provide specific services at a defined level of quality (warranty) for a specific price. SLAs typically need negotiation of agreements with other internal organizations (OLA's) or external suppliers (Underpinning Contracts).

Capacity Management

- Capacity Management ensures optimal and economic usage of existing resources and future capacity requirement planning.
- Responsible for ensuring that adequate capacity is available at all times to meet the agreed needs of the business in a cost-effective manner
- Includes component, capacity plan, capacity report, capacity management information system, and performance.

Capacity management activities

- Gather the data
- Design a service and reach agreement
- Build the service
- Operation

Availability Management

- Availability Management ensures the operative services meet all agreed availability goals.
- Availability management ensures that infrastructure, tools, roles etc. are appropriate for the agreed targets.
- It also works with the design teams to ensure that availability is designed into services.

Part of the process is to identify vital business functions (VBFs) which IT services support. This will help clarify which approach to availability to take:

- prevention (making sure, as far as possible, that unavailability never happens)
- recovery (developing plans to restore service rapidly in the event of an outage)

IT Service Continuity Management

- This process ensures continuity of IT services regardless of any disaster occurs.
- IT service continuity management (ITSCM) focuses on supporting the overall continuity of the business.
- We define ITSCM as the process responsible for managing risks that could seriously impact IT services.

- Risks so serious they could threaten the very survival of the business.
- This activity is often referred to as disaster recovery (DR). But, the use of the term ITSCM should show that there is a corresponding business continuity management (BCM) process.
- This analysis determines how different types of disruptions impact the business. The business areas determined to suffer the greatest impact need the most focus from the service continuity teams.

Information Security Management

- This process ensures confidentiality, integrity, availability of data.
- Large organizations typically appoint a Security Manager who is accountable for the ISM process, end-to-end.
- Recommended security controls : *preventative* , *Detective* , corrective measures are in place.

Objectives of Information Security Management

- *Information is available and usable when required, and the systems that provide it can appropriately resist attacks and recover from or prevent failures (availability)*
- *Information is observed by or disclosed to only those who have a right to know (confidentiality)*
- *Information is complete, accurate, and protected against unauthorized modification (integrity)*
- *Business transactions, as well as information exchanges between enterprises or with partners, can be trusted (authenticity and non-repudiation*

Supplier Management

- This process ensures supplier relationship & performance and also ensures management of right and relevant contracts with supplier
- Supplier management works with third parties, such as suppliers, to negotiate contracts for products or services.
- Supplier management monitor conformance to the contract conditions and address any breaches. At renewal, supplier management will determine whether to renew, renegotiate, or end the contract.

- The objectives of supplier management is to ensure alignment of contracts with the needs of the business.
- It is also responsible for ensuring suppliers are meeting their commitments. The supplier and contract management information system (SCMIS) holds supplier and contract details.

Service Transition

- Service Transition manages transition of a new or changed service. It ensures all changes to the service management processes are carried out in coordinated way
- Ensure that service can be managed, operated and supported in accordance with the requirements and constraints specified in service design

Transition Planning and Support

- This process deals with management and control of transition plan.
- At any time, there will be several projects passing through the service transition phase of the lifecycle.
- It is the responsibility of transition planning and support to coordinate service transition activities for all these projects.

Specifically, the responsibilities of transition planning and support include:

- Work with capacity management to ensure that adequate resources are available
- Where there is contention for resources, develop a schedule that meets the requirements of the stakeholders
- Ensure that all parties use a standard, reusable process framework.
- Monitor and improve the performance of the Service Transition lifecycle phase.

Change Management

This process ensures manage and control change management process. It also prevents any unauthorized changes from occurring.

ITIL change evaluation analyzes changes before they move to the next phase in their lifecycle. The lifecycle of a change includes several points at which a go/no-go decision needs to be made:

- Authorization to build and test
- Authorization to check software into the definitive media library (DML)
- Authorization to deploy

We should evaluate all changes. But, for significant changes a formal evaluation process should be invoked. Each organization must define for itself what “significant change” is.

The evaluation should include:

- Evaluating the intended effects of the change
- As far as possible, anticipating any unintended effects of the change
- Identifying risks
- Presenting a recommendation to change management on whether to proceed to the next stage

The change management process can make the go/no-go decision on proceeding to the next stage.

Service Asset and Configuration Management (SACM)

- It maintains database for configuration items such as servers, switches, routers etc.
- SACM is a combination of two important processes:
  - **Asset management** which addresses the assets you use to deliver IT services.
  - **Configuration management** which tracks the configurations of and relationships between the various components (configuration items or CIs) of your various IT services

Release and Deployment Management

- This process deals with management and control of movement of releases to test and live environment.
- Key phases to release and deployment management :
  - Release and deployment planning
  - Release building and Testing
  - Deployment
  - Reviewing and closing a deployment

- **Major releases.** To qualify as a major release, it should contain new hardware or software. More often than not, a major release equates to introducing completely new functionality. Think v1.0 and v2.0-level releases — they're major milestones.
- **Minor releases** make significant improvements to existing functionality, often packaging together a number of fixes — and are often numbered v1.1, v1.2, v1.3 etc.
- **Emergency releases** are exactly what they sound like. Something bad needs attention ASAP, so you're releasing a temporary fix — and probably numbering the release something like 1.1.1, v1.1.2, v1.1.3, etc.

Service validation and Testing

- This process deals with the quality of services offered.
- Testing can take place at any point in the service lifecycle but, it generally occurs during Service Transition.
- The service validation and testing process plans, conducts and reports on tests of new or changed services.
- The results of testing go to the change evaluation process to support a decision on whether to proceed.

- The service design package (SDP) outlines the tests to perform.
- Working with change evaluation, service validation and testing will:
  - Work with transition planning and support to plan the resources required for testing
  - Plan and design tests
  - Schedule tests
  - Prepare the test environment
  - Perform the tests
  - Evaluate exit criteria and report
  - Clean up and close tests

Service validation and test will perform different types of tests, as called for in the service design package. Types of tests include:

- Utility testing. Does the service deliver the required functionality?
- Warranty testing. Will the service deliver required levels of availability, capacity, security, and continuity?
- Usability testing. Will the service be usable by all potential users, including those with restricted abilities?

- Contract and regulation testing. Will the service conform to applicable regulatory and contract requirements?
- Operational readiness testing. Are the support functions, including the service desk, staffed and trained to support the new or changed service?

Knowledge Management

This process deals with gathering, storing, analyzing, and sharing knowledge.