ITIL® Foundation Exam Cram Notes : Service Management As A Practice

examguides.com/ITILFund/itilf-2.htm

1. Service management as a practice

1.1 Why is ITIL so successful?

The following list defines the key characteristics of ITIL that contribute to its global success:

1) Vendor-neutral: ITIL service management practices are applicable in any IT organization because they are not based on any particular technology platform or industry type.

2) Non-prescriptive: ITIL offers robust, mature and time-tested practices that have applicability to all types of service organization.

3) Best practice: ITIL represents the learning experiences and thought leadership of the world's best-in-class service providers.

1.2 Concept of a service

1) A service is a means of delivering value to customers by facilitating outcomes customers want to achieve without the ownership of specific costs and risks.

Customers can be internal or external. An internal customer is a customer who works for the same business as the IT service provider. External customer is a customer who works for a different business from the IT service provider.

a) Service can be internal service or external service

- Internal service A service delivered between departments or business units in the same organizatio
- External service A service delivered to external customers.

b) Services can be discussed in terms of how they relate to one another and their customers, and can be classified as core, enabling or enhancing.

- Core Services: required directly by customers to deliver an intended outcome.
- Enabling Services: needed to ensure core services can be delivered successfully, not visible to customers
- Enhancing Services: created to add features / values to the customers, not essential.

2) IT service is a service provided by an IT service provider. The IT service is made up of a combination of information technology, people and processes. A customer-facing IT service directly supports the business processes of one or more customers and its service level targets should be defined in a service level agreement. Other IT services, called supporting services, are not directly used by the business but are required by the service provider to deliver customer-facing services. IT Services consist of taking care the design, implementation and maintenance of all the components that are required to fulfill a business objective for the users (i.e. IT and business integration, not just IT and business alignment).

a)Values of IT services

- Create values for the business by supporting business processes
- Create values for end customers
- Reduce costs / increase productivity (enhance performance)
- Manage costs / risks / issues more effectively
- Reduce / remove constraints (e.g. not enough bandwidth)
- Facilitate achievement of outcomes (e.g. students registering for a class)

b)Types of IT services:

There are three types of IT services according to customer types:

- Supporting Services (infrastructure services): not directly visible to customers, managed with operation level agreements.
- Internal Customer-facing Services: enable internal customers to carry out its business process, managed with service level agreements.
- External Customer-facing Services: used by the external customers, can be the business process itself, managed with contracts.

1.3 Service management

Service management is more than just a set of capabilities. It is also a professional practice supported by an extensive body of knowledge, experience and skills. A global community of individuals and organizations in the public and private sectors fosters its growth and maturity.

1.4 IT Service management

IT Service Management is the implementation and management of quality IT services that meet the needs of the business. IT service management is performed by IT service providers (to internal or external customers) through an appropriate mix of people, process and information technology.

IT service management make use of best practices i.e., a set of generic (high level) guidelines based on the successful experiences of a number of organizations, in service management, adapt and apply for the business to save cost and improve quality.

Good practice could be either an application of best practice, or an input into best practice.

1)Types of IT Service Providers.

- Type I: Internal Service Provider - service providers located within the business unit, maybe several internal service providers within an organization.
- Type II: Shared Services Unit - supports several business units, e.g. centralized IT department.
- Type III: External Service Provider - delivers services to external customers

1.5 Stakeholders in service management

Stakeholders are individuals or groups that have an interest in an organization, service, or project and are potentially interested or engaged in the activities, resources, targets, or deliverables from service management.

1)There are two types of stake holders they are:

- Internal stakeholders: within the service provider organization.
- External stakeholders: outside customers, users, suppliers (vendors, network providers)

1.6 Processes, functions and role

Process

1)Process is a structured set of activities designed to accomplish a specific objective. A process takes one or more defined inputs and turns them into defined outputs

a)The four key characteristics of a process are:

- Measurability: We are able to measure the process in a relevant manner. It is performance driven. Managers want to measure cost, quality and other variables while practitioners are concerned with duration and productivity.
- Specific results: The reason a process exists is to deliver a specific result. This result must be individually identifiable and countable.
- Customers Every process delivers its primary results to a customer or stakeholder. Customers may be internal or external to the organization, but the process must meet their expectations.
- Responsiveness to specific triggers While a process may be ongoing or iterative, it should be traceable to a specific trigger.

Function

1)Function is a team or group of people and the tools or other resources they use to carry out one or more processes or activities - for example, the service desk.

2)In larger organizations, a function may be broken out and performed by several departments, teams and groups, or it may be embodied within a single organizational unit

3)In smaller organizations, one person or group can perform multiple functions - for example, a technical management department could also incorporate the service desk function.

Role

1)Role is a set of responsibilities, activities and authorities granted to a person or team. One person/team can take up several roles in different context. e.g. change management role, capacity management role

a)Defined roles in ITIL:

- Group - a number of people performing similar activities, not formal structure
- Team - a more formal structure for people working together with a common objective
- Department - a formal organizational structure with a hierarchical structure
- Division - a number of departments forming a self-contained unit

Previous Contents Next

ITIL® Foundation Exam Cram Notes : The Itil Service Life Cycle

2. The ITIL Service Life Cycle

ITIL consists of the following components:

- The ITIL Core: a set of five publications containing the best practice guidance applicable to all organizations providing services
- The ITIL Complementary Guidance: a auxiliary set of publications (online or printed) detailing the application of ITIL to specific industries, organization and technology platform

The ITIL core consists of five lifecycle publications. They are as follows:

1)ITIL Service Strategy - The phase of strategic planning of service management capabilities, and the alignment of service and business strategies.

2)ITIL Service Design The phase of designing and developing appropriate IT services, including architecture, processes, policy and documents. The design goal is to meet the current and future business requirements.

3)ITIL Service Transition: The phase of realizing the requirements from previous stages, and improving the capabilities for the transition of new and modified services to production.

4)ITIL Service Operation: The phase of achieving effectiveness and efficiency in providing and supporting services in order to ensure value for the customer and the service provider.

5)ITIL Continual Service Improvement: The phase of creating and maintaining the value for the customer by design improvement, and service introduction and operation.

Figure: THE ITIL Service Life Cycle

3. Service Strategy

Service strategy shows organizations how to transform service management from an organizational capability into a strategic asset, and to then think and act in a strategic manner.

Service strategy helps clarify the relationships between various services, systems or processes and the business models, strategies or objectives they support.

3.1 Purpose of Service Strategy

The purpose of the Service Strategy is to define the perspective, position, plans and patterns that a service provider needs to be able to execute to meet an organization's business outcomes

3.2 Objectives of service Strategy

1)Provide business stakeholder value

2)Differentiate the organization

3)Make solid cases for investment

4)Resolve conflicting demands for services

5)Improve service quality by strategic planning

3.3 Scope of service Strategy

1)Generic principles and processes of service management. These generic principles are applied consistently to IT service management

2)Intended for use by both internal and external service providers, and includes guidance for organizations which are required to offer IT services as a profitable business, as well as those which are required to offer IT services to other business units within the same organization - at no profit

3)Two aspects of strategy:

- Defining a strategy whereby a service provider will deliver services to meet a customer's business outcomes
- Defining a strategy for how to manage those services

3.4 Value to business

1)Provides guidance on how to design, and put in place service management as a strategic asset

2)Sets the principles for developing service management policies, guidelines and processes across the service lifecycle.

3)Sets objectives and expectations of performance towards serving customers and market spaces.

4)Identifies and prioritizes opportunities.

5)Ensures that organizations can manage the costs and risks associated with their service portfolios.

6)Asks questions and plans a strategy for how to do something before progressing

3.5 Basic concepts in Service Strategy

1)Utility: also called 'fitness for purpose' involves the ability of the service to remove constraints or increase the performance of the customer.

2)Warranty: also called 'fitness for use' is the ability of the service to operate reliably.

3)Assets, Resources and capabilities

a)Assets: Asset is any resource or capability

- Customer asset: asset used by a customer to achieve a business outcome
- Service asset: asset used by a service provider to deliver services to a customer

b)Resources are the direct inputs for the production of services.

Example: Money, IT Infrastructure, people, or anything else that might help delivering an IT service.

c)Capabilities are the assets that represent the organization's ability/ knowledge to do something to achieve value

Example: organization, processes, management, etc.

4)Service Portfolio: is the entire set of services under management by a Service Provider. It consists of three major parts: Service Pipeline, Service Catalog, and Retired Services.

5)Governance: Governance ensures that policies and strategy are actually implemented, and that required processes are correctly followed. Governance includes defining roles and responsibilities, measuring and reporting, and taking actions to resolve any issues identified.

6)Business case: is a structured and documented justification for investment in something expected to deliver value in return. Business Cases are used during Service Strategy to evaluate the feasibility and desirability of creating and providing various IT Services

7)Risk Management: is process of identification, assessing and controlling risks through analyzing asset`s value, threats and how vulnerable each asset is to those threats.

8)Service Provider: There are three types of service providers they are :

- Internal service provider: exists within an organization and provides service solely for a unique business unit.
- External service provider: operates outside the organization.
- Shared service provider: exists within an organization, but provides service for more than one business unit.

9)Supplier: Is a third party responsible for supplying the goods or Services required to deliver IT Services.

10)Types of Services: according to the value for customers services are classified into three types they are:

- Core Services: required directly by customers to deliver an intended outcome.
- Enabling Services: needed to ensure core services can be delivered successfully, not visible to customers
- Enhancing Services: created to add features / values to the customers, not essential.

11) Patterns of Business Activities: Influence the demand patterns seen by the Service Providers.

3.6 Processes

3.6.1 Service Portfolio management:

A)Purpose of Service Portfolio Management

- Purpose of is to make sure that the service provider has got the perfect set of services so that it can balance the investment in IT with the capacity to get the desired business outcomes. It keeps a track of the investments in services throughout their lifecycle
- Service portfolio also makes sure that services are defined clearly and linked to the achievement of business outcomes, thus ensuring that all design, transition and operation activities are in line with the value of services.

B)Objectives of Service Portfolio Management

- To develop and maintain a Service Portfolio that provides a complete picture of all services including their status.
- To establish conditions and requirements for inclusion of new services in the Service Portfolio.
- To ensure a Service Catalogue is developed and managed as part of the Portfolio.
- Agree on the rules for transferring services to the Service Catalogue as they move into transition and out of the Catalogue and as they move into retirement.
- To ensure that the Service Portfolio meets the functional and performance requirements of its users and that its performance, availability and security meet agreed requirements.
- To ensure that management reports are produced in line with agreed reporting requirements.

C)Scope of Service Portfolio Management

- All services a service provider plans to deliver, those currently delivered and those that have been withdrawn from service
    - The primary concern of service portfolio management is whether the service provider is able to generate value from the services.
    - Service portfolio management will therefore track investments in services and compare them to the desired business outcomes
- Service portfolio management evaluates the value of services throughout their lifecycles, and must be able to compare what newer services have offered over the retired services they have replaced

D) Service Portfolio

A Service Portfolio is a complete list of services regardless of where they are in their life cycle (i.e. planning, development, production, retired). The Service Portfolio includes the service pipeline, a service catalog, and a list of retired services.

1)Service pipeline includes services being created for a given market space or customer.

2)Service catalog consists of services presently active in the service operation phase, as well as those approved in the pipeline. The service catalog provides a description of each service, pricing and service level commitments, and terms and conditions. The service catalog is an important tool in service strategy because it is the virtual projection of your actual and present capabilities. It also serves as a service-order and demand-channeling mechanism, as well as a visualization tool for SPM decisions. The service catalog provides a strong link between SPM and service level management (SLM).

3)Retired services are services no longer offered.

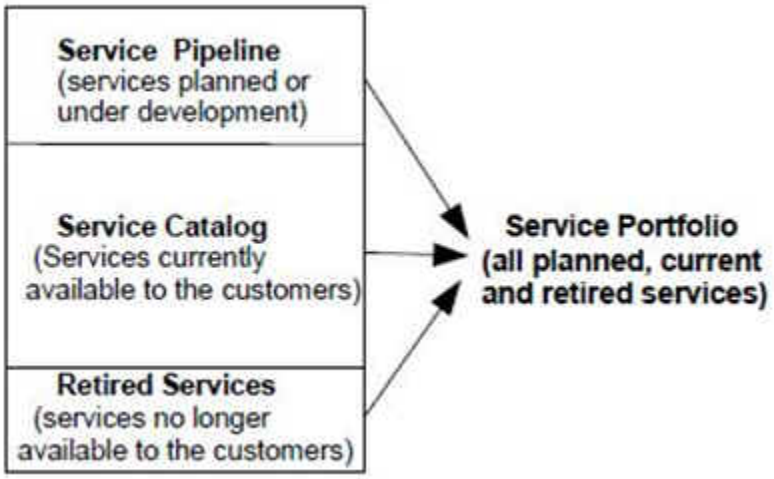


Figure: Service Portfolio

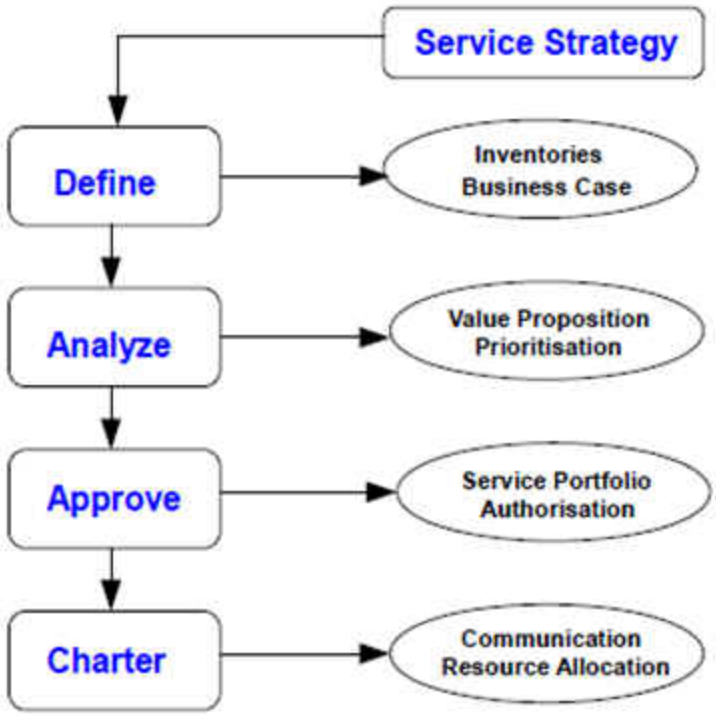
Previous Contents Next

ITIL® Foundation Exam Cram Notes : Service Portfolio Management, Financial Management, Brm, And Service Design

examguides.com/ITILFund/itilf-4.htm

E) Activities of Service Portfolio management process are:

- Define: collates information from all existing services as well as every proposed service (this includes any services in the conceptual phase). The scope covers all the services the organization would provide if it had unlimited resources, capabilities and time.
- Analyze: the analyze exercise is performed to find the perspectives, plans, patterns and positions. This information is used to guide the analysis and the desired outcomes of service portfolio management. Understanding their options helps senior management to make informed investment decisions, with regards to service initiatives
- Approve: is concerned with completing the final draft of the portfolio. Approve is concerned with completing the final draft of the portfolio.
- Charter: Charter is concerned with communicating decisions and allocating sufficient resources and charter services. Decisions will be communicated via a clear and unambiguous report that includes detailed action points for implementation.



3.6.2 Financial Management for IT services

A) Purpose of Financial Management Process

- Secure the appropriate level of funding to design, develop and deliver services that meet the strategy of the organization.
- Act as a gatekeeper that ensures that the service provider does not commit to services that they are not able to provide.
- Identify the balance between the cost and quality of service and maintain the balance of supply and demand between the service provider and their customers

B) The Objectives of Financial Management Process

- Reduce long term costs - empower management.
- Declares Added Value of IT.
- Improved Total cost of ownership and return on investment.
- Forces business to make service levels and their costs more visible.
- Assures senior management/stakeholders that IT is well managed and meeting business needs.
- Assists change management processes.

C) Scope of Financial Management Process

Ensures the financial practices within IT is consistent with organizational standards so that other business units will have an understanding of how IT is funded

D) Activities of Financial Management

- Budgeting: is the predicting the expected future requirements for funds to deliver the agreed upon IT services to the service customers. Budgets are typically created on an annual basis. The activity requires careful monitoring of agreed budgets against the actual spend (accounting).
- Accounting: enables the IT organization to account fully for the way its money is spent (the practices allow identification of costs by customer, service and/or activity). The activity is not simple and this is one area that should involve some outside expertise usually provided from within the Finance Department.
- Charging: is an optional activity within financial management for IT services. The decision whether the IT department will charge customers for the actual provision of IT services is made at a strategic level - not from within the IT department. Charging must be linked to controllable aspects for customers/users as they may wish to alter their behavior/usage of services based on the charges they incur.

E) Business Case

- A business case is the justification for a significant item of expenditure. The business case includes information about costs, benefits, options, issues, risks and possible problems.
- A business case is a tool for decision planning and support for understanding the likely consequences of a business decision in quantitative or qualitative terms.
- Information can be captured from the Service Portfolio with sound financial management.
- Business cases are built in Business Relationship Management process and evaluated in Service Portfolio Management process.
- Example for business case structure is as follows:
    - Introduction - business objectives addressed.
    - Methods and assumptions - boundaries of the business case.
    - Business impacts - financial, non-financial results anticipated.
    - Risks and contingencies - probability that alternative results will emerge.
    - Recommendations - specific actions recommended.

3.6.3 Business Relationship Management Process (BRM)

Business Relationship Management is a process responsible for maintaining a positive relationship with customers. BRM identifies customer needs and ensures that the service provider is able to meet these needs with an appropriate catalogue of services. This process has strong links with service level management.

A)Purpose of Business Relationship Management Process : The purpose of BRM is to establish relationship between the service provider and customers and to ensure customers satisfaction by responding to changing requirements and managing customer expectation.

B)Objectives of Business Relationship Management Process

- Understand customers needs and prioritize services accordingly to meet user requirements
- Maintain good communication.
- Handle conflicts and complaints effectively
- Identify changes in business environment and technology that could impact services
- Ensure customer satisfaction.

C) Scope of Business Relationship Management Process

- BRM focuses on understanding how services meet customer requirements.
- Business outcomes that the customer wants to achieve
- Services currently offered to the customer, and how they are used by the customer
- How services are currently offered including who is responsible for them, agreed
- levels of service, quality of services delivered and any changes that are anticipated
- Technology trends that could impact current services and the customer, and how

- Levels of customer satisfaction; action plans in place to deal with the causes
- How to optimize services for the future
- How the service provider is represented to the customer

4. Service Design

4.1 Purpose of Service Design

The purpose of Service Design is to deliver a new service / service amendment that can deliver the strategic outcome required the design of both the services and the service management processes need to be included.

Need to ensure the service will run within budget and meet/exceed customer requirements.

4.2 Objectives of Service Design

An objective of Service Design stage of ITIL service life cycle is to design Services that can be easily and efficiently developed and enhanced.

4.3 Scope of Service Design

Consider not only the current requirements but also future needs (e.g. take advantage of technical advancements, can be easily adapted to future needs)

Describes how to identify requirements (functional and service level) and ensure the delivery of such requirements

4.4 Value to Business

Ensuring that services are aligned with business objectives

Ensuring that services are able to provide the utility and warranty required for them to meet the objectives outlined during Service Strategy.

Ensuring that service management systems and tools are capable of supporting service offerings

Ensuring that service-e management processes are capable of supporting service offerings

Ensuring that services are constructed according to agreed architectural standards

Ensuring that services are designed so as to be implemented efficiently

Ensuring that services are designed so that their performance can be measured

4.5 Four P's of Service Design

A Service Designer need to consider the following "Four P's of Service Design" while designing a service. The Four P's are as follows:

- People: Human resources and organizational structures required to support the service
- Processes: Service Management Processes required to support the service
- Products: The products are the tools, services, and technology used in the delivery of, and support of, the services.
- Partners: When designing services, vendors, manufacturers, and suppliers should be considered as they will be utilized to support the service once it is live.

4.6 Five major Design aspects of Service Design

The 'Five Aspects of Service Design' are areas which should also receive design focus as part of the overall effort design a service. The areas include:

- Service solutions: Include all of the functional requirements, resources and capabilities needed and agreed upon
- Service Management systems and tools: these are used to support and automate processes (e.g. quality management system, information security system). To ensure consistency with other services and guarantee that supporting and dependent services are adequate to maintain on-going reliable service delivery
- Technology architectures and management systems: To ensure they are consistent with the new service and are suitable to operate and maintain it
- Architecture is defined as the fundamental organization of a system, embodied in its components, their relationships to each other and to the environment, and the principles guiding its design and evolution.
- Processes: To ensure that the process, roles and responsibilities are adequate to operate, support and maintain the new or changed service
- easurement methods and metrics: To ensure that the methods can provide the required metrics on the service.

4.7 Basic Concepts in Service Design Processes

Service catalogue: A service catalogue is a database or structured document with information about all live IT services, including those available for deployment. The service catalogue is part of the service portfolio and contains information about two types of IT service: customer-facing services that are visible to the business and supporting services required by the service provider to deliver customer-facing services.

The service catalogue has different views for different people (users, IT, etc.)

- Two-view (business service/technical service)
- Three-view (wholesale customer, retail customer and supporting services).

Service level agreement (SLA): SLA is a written agreement between the Service Provider and a customer containing mutual goals and responsibilities.

Operational level agreement (OLA): An Operational Level Agreement (OLA) is an agreement between an IT service provider and another part of the same organization. An OLA defines the goods or services to be provided from one department to the other, and the responsibilities of both parties.

Underpinning contract: An Underpinning Contract (UC) is a contract with a third party, in support of the delivery of an agreed IT service to a customer. The UC defines targets and responsibilities that are required to meet agreed service level targets in an SLA.

Service design package: The Service Design Package (SDP) that was created in the Service Design phase contains all aspects of an IT service and its requirements through each stage of its lifecycle. It includes the information about the execution of activities of the Service Transition team.

Availability: The ability of a service, component or CI to perform its agreed function when required.

Availability is measured and reported as a percentage.

Previous Contents Next

ITIL® Foundation Exam Cram Notes : Processes (slm, Scm), Availability, And It Service Continuity Management

4.8 Processes

4.8.1 Service Level Management (SLM)

Service level management principles form the basis on how to contribute to an ITSM culture to ensure that the right services with the appropriate quality are delivered, at the right cost to end users.

A) Purpose of Service Level Management Process

- Ensure all current / planned services are delivered to agreed achievable targets
- Accomplished through a constant cycle of negotiating, agreeing, monitoring, reporting on and reviewing IT service targets and achievements, and through instigation of actions to correct or improve the level of service delivered

B) Objectives of Service Level Management Process

- Define, document, agree, monitor, measure, report and review the level of IT services provided; instigate corrective measures whenever appropriate
- Provide and improve a relationship / communication with the business and customers in conjunction with business relationship management
- Ensure specific and measurable targets are developed for all IT services
- Monitor and improve customer satisfaction with quality of service delivered
- Ensure IT and customers have a clear expectation of service levels to be delivered
- Ensure that even when all agreed targets met, the levels of service delivered are subject to proactive, cost-effective continual improvement.

C) Scope of Service Level Management Process

- Establishing service level requirements
- Establishing Service level agreements
- Monitoring service performance.
- Measuring customer satisfaction.
- Reporting on service performance and customer satisfaction.
- Maintaining customer relationships.

D) Key Activities of Service Level Management Process

- Identify IT services and service requirements
- Define, build and manage the IT Service Catalog
- Define, build and negotiate Service Level Agreements (SLAs)
- Define, build and negotiate Operational Level Agreements (OLAs)
- Identify Underpinning Contract service requirements (UCs)
- Monitor and manage SLAs, OLAs and UCs
- Initiate service improvement actions
- Provide management information about Service Level Management quality and operations

4.8.2 Service Catalogue Management (SCM)

A service catalogue is a database or structured document with information about all live IT services, including those available for deployment. The service catalogue is part of the service portfolio and contains information about two types of IT service: customer-facing services that are visible to the business and supporting services required by the service provider to deliver customer-facing services.

Service Catalogue Management is a process responsible for providing and maintaining the service catalogue and for ensuring that it is available to those who are authorized to access it.

The service catalogue has different views for different people (users, IT, etc.)

- Two-view (business service/technical service)
- Three-view (wholesale customer, retail customer and supporting services).

B) Objectives of Service Catalogue Management Process

- The production and maintenance of the service catalogue.
- Documenting the details of the service, status, interfaces and dependencies (obtained from Configuration Management System), often in service packages (solution)
- Ensure the service catalogue is made available to those approved to access it in a way that supports their effective and efficient use of service catalogue information

C) Scope of Service Catalogue Management Process

- Contribution to the definition of services and service packages
- Development and maintenance of service and service package descriptions appropriate for the service catalogue
- Production and maintenance of an accurate service catalogue
- Interfaces, dependencies / consistency between the catalogue and service portfolio

- Interfaces and dependencies between all services and supporting services within the service catalogue and the CMS

D) Key Activities of Service Catalogue Management Process

- Documenting the definition of the service
- Production and maintenance of an accurate service catalogue
- Interfaces, dependencies and consistency between the service catalogue and service portfolio
- Interfaces and dependencies between all services and supporting services within the service catalogue and the CMS
- Interfaces and dependencies between all services, and supporting components and Configuration Items (CIs) within the Service Catalogue and the CMS

4.8.3 Availability Management

Availability management is a process responsible for ensuring IT services meet current and future availability needs of the business in a cost-effective and timely manner.

A) Purpose of Availability Management Process: The purpose of Availability Management is to provide a focal point and management responsibility for all availability-related activities in respect of both resources and services

B) Objectives of Availability Management process

- To prepare and maintain the Availability Plan.
- To monitor availability levels and the status of resources and services to identify potential and actual availability issues and prevent or minimize any consequent business interruptions.
- To manage the availability of services and resources to meet agreed service levels.
- To assist with the investigation and resolution of availability-related Incidents and Problems.
- To assess the impact of changes on availability levels and plans.
- To proactively improve availability where the cost is justified.

C) Scope of Availability Management process

- Covers the design, implementation, measurement, management, testing and improvement of IT service and component availability (reduce availability issues throughout the service lifecycle)
- Ensure that availability is duly considered in service design
- Should be applied to all operational services and technology, particularly those covered by SLAs.
- Monitor and measure availability according to SLA (if available)

- Include both reactive (monitoring by event management, investigating downtime incidences) and proactive (identifying and managing risks) activities.
- All information is recorded in the availability management information system. An ongoing process, finishing only when the IT service is decommissioned or retired

D) Key Activities of Availability Management Process

- Proactive activities:
    - Ensure that appropriate design and planning of availability takes place for all new services
    - Planning, design and improvement of availability
    - Providing cost effective availability improvements that can deliver business and customer benefits
    - Ensuring agreed level of availability is provided
    - Produce and maintain an availability plan
- Reactive activities:
    - Monitoring, measuring, analysis and management of all events, incidents and problems involving unavailability
    - Continually optimize and improve availability of IT infrastructure services
    - Assisting security and ITSCM in the assessment and management of risk
    - Attending CAB as required
- Determining availability requirements: the Availability Manager can determine the availability requirements.
- Determining Vital Business Functions (VBF's): IT systems that support VBFs should have higher availability expectations and the appropriate systems and support to achieve and sustain these higher levels at critical times which have been agreed and documented in the SLA.
- Business Impact analysis: A formal analysis of the affect on the business, if a specific set of IT services are not available.

E) Key Indicators of Availability Management

Reliability: A measure of how long a service, component or CI can perform its agreed function without Interruption. It is measured as the mean time between service incidents (MTBSI) or mean time between failures (MTBF)

$$\text{Reliability (MTBSI in hours)} = \frac{\text{Availability time in hours}}{\text{Number of breaks}}$$

$$\text{Reliability (MTBF in hours)} = \frac{\text{Availability time in hours} - \text{Total downtime in hours}}{\text{Number of breaks}}$$

2) Maintainability: A measure of how quickly and effectively a service, component or CI can be restored to normal working after a failure. It is measured as the mean time to restore service (MTRS).

3) Serviceability: Ability of a third-party supplier to meet the terms of its contract. This contract will include agreed levels of availability, reliability and/or maintainability for a supporting service.

$$\text{Maintainability (MTRS in hours)} = \frac{\text{Total downtime in hours}}{\text{Number of service breaks}}$$

4) Resilience: A measure of freedom from operational failure and a method of keeping services reliable. It minimizes the consequences of component failure; one popular method of resilience is redundancy.

5) Security: Security refers to the confidentiality, integrity, and availability of that data.

4.8.4 Information Security Management

Information security is the management process within the corporate governance framework, which provides the strategic direction for security activities and ensures objectives are achieved.

A) Purpose of Information Security Management: The purpose of the Information Security Management is to ensure that IT security meets the overall business security requirements through availability, integrity, and confidentiality.

B) 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
- Confidentiality: Information is observed by, or disclosed, to only those who have a right to know.
- Integrity: Information is complete, accurate and protected against unauthorized modification
- Authenticity and Non-repudiation: Business transactions, as well as information exchanges between partners, can be trusted.

C) Scope of Information Security Management

- Identifying information security needs.
- Establishing security policies and methods.
- Implementing security policies and methods.
- Monitoring system access and needs.

D) Elements of Information Security Management Process:

There are five elements of Information Security Management Process they are:

- Control: The objectives of control elements are:
  - Establish an organization structure to prepare, approve and implement the information security policy.
  - Establish a management framework to initiate and manage information security in the organization.
  - Allocate responsibilities establish and control documentation.
- Plan: The objectives of Plan are:
  - Devise and recommend the appropriate security measures, based on an understanding of the requirements of the organization.
  - The requirements will be gathered from such sources as business and service risk, plans and strategies, SLAs and OLAs and the legal, moral and ethical responsibilities for information security.
- Implement: The objective of the implementation element is to ensure that appropriate procedures, tools and controls are in place to underpin the Information Security Policy.
- Evaluation: The objectives of Evaluation element are:
  - Supervise and check compliance with the security policy and security requirements in SLAs and OLAs.
  - Carry out regular audits of the technical security of IT systems.
  - Provide information to external auditors and regulators, if required.
- Maintain: The objectives of Maintain element are:
  - Improve on security agreements as specified in, for example, SLAs and OLAs.
  - Improve the implementation of security measures and controls.

E) The Information Security Policy

The policy must cover all areas of security, be appropriate, meet business needs and include:

1) An overall Information Security Policy

2) Use and misuse of IT assets policy

3) An access control policy

4) A password control policy

5) An e-mail policy

6) An internet policy

7) An anti-virus policy

8) An information classification policy

9) A document classification policy

10) A remote access policy

11) A policy with regard to supplier access of IT services, information and components

12) An asset disposal policy.

4.8.5 Supplier Management

The process responsible for getting value for money from suppliers, ensuring all supplier contracts and agreements support business needs, and all suppliers meet contractual commitments.

A) Purpose of Supplier Management Process: The purpose of the supplier management process is to obtain value for money from suppliers and to ensure that suppliers perform to the targets contained within their contracts.

B) Objectives of Supplier Management Process

- Obtain value for money from suppliers and contracts.
- Work with SLM to ensure underpinning contracts support and are aligned with business needs, SLRs and SLAs.
- Negotiate and agree underpinning contracts and manage through their lifecycle.
- Manage supplier relationships and performance.
- Maintain a supplier policy and a Supplier and Contract Database (SCD).

C) Scope of Supplier Management Process

- Identifying qualified suppliers.
- Negotiating with suppliers.
- Establishing underpinning contracts.
- Monitoring supplier performance.

D) Categories of Supplier Management Process

- Strategic - for significant partnering relationships that involve senior managers sharing confidential strategic information to facilitate long-term plans
- Tactical - relationships involving significant commercial activity and business interaction.
- Operational - for suppliers of operational products or services
- Commodity - for suppliers providing low-value and/or readily available products and services.

4.8.6 Capacity Management

Capacity management process is responsible for ensuring that the capacity of IT services and the IT infrastructure is able to meet agreed capacity- and performance-related requirements in a cost-effective and timely manner.

A) Purpose of Capacity Management Process

- Ensure that the IT infrastructure and the capacity of IT services reach the agreed capacity and performance levels in a cost-effective and timely manner.
- Capacity management process should to meet both the current and future capacity and very importantly the performance needs of a business.

B) Objectives of Capacity Management Process

- Providing guidance and suggestions to other areas of the business and IT on all capacity and performance related issues
- Making sure that service performance achievements reach their agreed targets by managing the capacity and performance of both resources and services
- Helps with the diagnosis and resolution of capacity and performance related issues
- Estimating the impact of all changes on the capacity plan.
- Making sure that proactive measures are taken to improve the performance of services.

C) Scope of Capacity Management Process

- Accounting for data storage, concurrency, and service data.
- Establishing and implementing capacity designs.
- Analyzing and assessing capacity performance.

D) Activities of Capacity Management

There are mainly three activities of Capacity Management Process they are:

- Business Capacity Management: Translates business needs and plans into requirements for service and IT infrastructure, ensuring that the future business requirements for IT services are quantified, designed, planned and implemented in a timely fashion.
- Service Capacity Management: Focuses on the management, control and prediction of the end-to-end performance and capacity of the live, operational IT services usage and workloads.
- Component Capacity Management: Focuses on the management, control and prediction of the performance, utilization and capacity of individual IT technology components.

4.8.7 The IT Service Continuity Management

IT service continuity management (ITSCM) is responsible for the continuity of the IT services required by the business in times of disasters or extreme events to recover the IT services. (Less significant incidents are dealt with by Incident Management Process). ITSCM is one of the elements of business continuity plan (BCM).

A) Purpose of IT Service Continuity Management Process

- Identify and manage the risks to the IT services.
- Agree with the business for the minimum requirement of service in case of a disaster

B) Objectives of IT Service Continuity Management Process

- Maintain a set of IT Service Continuity Plans and IT recovery plans that support the overall Business Continuity Plans (BCPs) of the organization.
- Complete regular Business Impact Analysis (BIA) exercises to ensure that all continuity plans are maintained in line with changing business impacts and requirements.
- Conduct regular risk assessment and management exercises in conjunction particularly with the business and the Availability Management and Security Management processes that manages IT services within an agreed level of business risk.
- Provide advice and guidance to all other areas of the business and IT on all continuity- and recovery-related issues.
- Ensure that appropriate continuity and recovery mechanisms are put in place to meet or exceed the agreed business continuity targets.
- Assess the impact of all changes on the IT Service Continuity Plans and IT recovery plans
- Ensure that proactive measures to improve the availability of services are implemented wherever it is cost-justifiable to do so.
- Negotiate and agree the necessary contracts with suppliers for the provision of the necessary recovery capability to support all continuity plans in conjunction with the Supplier Management process.

C) Scope of IT Service Continuity Management Process

- Defining continuity needs
- Establishing Continuity Plans
- Implementing Continuity Plans
- Periodically Testing Continuity Plans.

D) Activities of IT Service Continuity Management Process

There are four stages of ITSCM, incorporating each of the activities that take place to ensure that IT organizations are as prepared and organized as possible in the event of a disaster situation. The stages are as follows:

1) Initiation defines policy, scope, allocate resources and set up project organization.

2) Requirements and strategy will need to be defined.

- A business impact analysis (BIA) has to be done.
- Service analysis will also have to be done. this will analyze essential IT services based on the SLA. Dependencies must be assessed also.
- Risks affecting the business will then have to be analyzed. The ITSC manager also has to identify the threats and vulnerabilities.
- ITSCM strategy must then be defined. The strategy can be risk reduction or recovery planning.

3) The next step is to implement the plan. This includes setting up the organization, developing the plan and testing it.

4) Operation management requires training non-IT staff on the DRP. It requires regular review and testing. Any improvements or changes have to go through the Change management process.

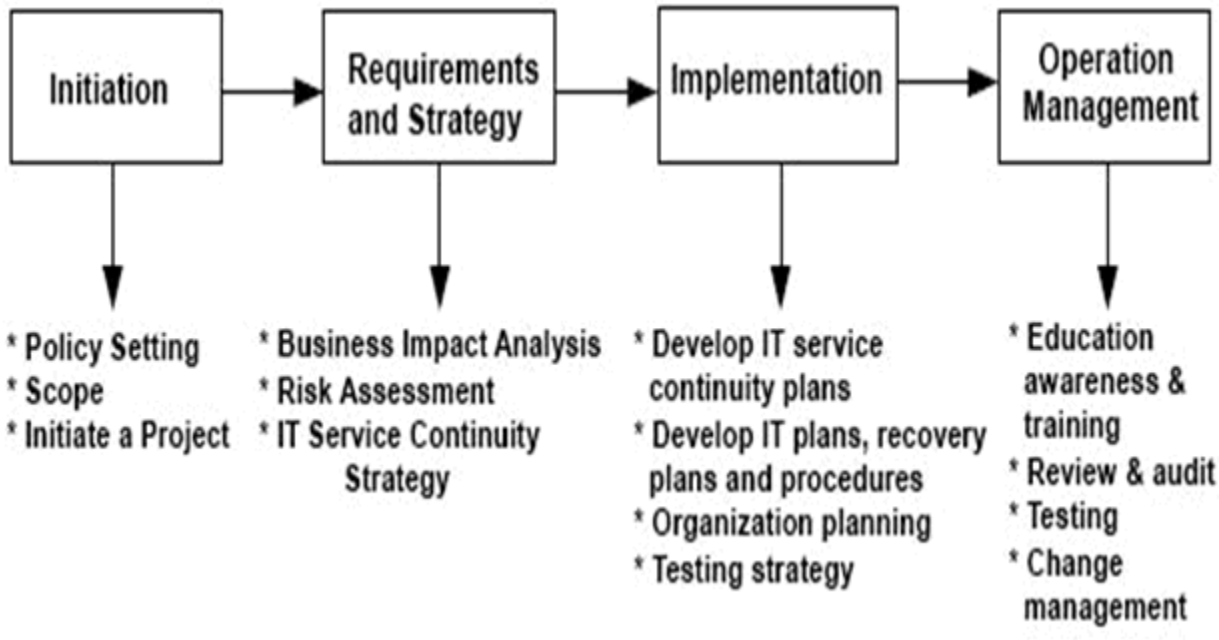


figure: Activities of an IT Service Continuity Management Process

E) Sub-process of IT Service Continuity Management Process

1) Business Impact Analysis- identify key services that need continuity at different time of the day/month/year and clarify relative importance of individual services

2) Risk Assessment - to compile a list of evaluated risks and propose counter measures. These will ensure the provision of IT service continuity in a cost-effective way

ITIL® Foundation Exam Cram Notes : Service Transition (purpose, Objectives, Scope, And Value To Business)

4.8.8 Design Co-ordination Process

Design Co-ordination is a process responsible for coordinating all service design activities, processes and resources. It ensures consistent and effective design of new or changed IT services, service management information systems, architectures, technology, processes, information and metrics

A) Purpose of Design Co-ordination Process

Ensure the goals and objectives of the service design stage are met by providing and maintaining a single point of coordination and control for all activities and processes within this stage of the service lifecycle.

B) Objectives of Design Co-ordination Process

- Ensures all aspects of the design (architecture, processes and metrics) to provide utility and warranty to meet business requirements for now and in future.
- To resolve conflicts in demand in case of simultaneous competing projects including resources and time conflicts.
- To ensure everyone is clear about the requirements for handing over between different lifecycle (e.g. service design package to transition phase)
- To check whether all requirements are met and repeatable design practices are used
- To reduce risks associated with complexity of projects.
- To compile the service design package within inputs from various processes.

C) Scope of Design Co-ordination Process : Design Co-ordination process covers all activities in design and ensure consistency across them for new, existing and retiring services.

5. Service Transition

Service Transition establishes the services as specified in the Service Design phase, based on the customer and stakeholder requirements. A Service Transition is effective and efficient if the transition delivers what the business requested within the limitations in terms of money and other necessary resources.

5.1 Purpose of Service Transition

The Purpose of Service Transition is to ensure that new, modified or retired services meet the expectations of the business as documented in the service strategy and service design stages of the lifecycle

5.2 Objectives of Service Transition

1) Plan and manage changes to services (either introducing new or retiring existing services) and to deploy the new services successfully to support business objectives while ensuring the integrity of all existing services

2) Ensure the service can be operated and supported according to the service design

3) Manage the risks associated

4) Set the expectations of the business with testing on the performance

5) Provide knowledge and info of the service / service assets to relevant people to ensure smooth operation

5.3 Scope of Service Transition

1) Provides guidance for the development and improvement of capabilities for transitioning new and changed services into supported environments, including release planning, building, testing, evaluation and deployment.

2) Considers service retirement, transfer of services between service providers

3) Focuses on how to ensure that the requirements from service strategy, developed in service design, are effectively realized in service operation while controlling the risks of failure and subsequent disruption.

4) Includes the transition of changes in the service provider's service management capabilities that will impact on the ways of working, the organization, people, projects and third parties involved in service management.

5.4 Value to Business

Service Transitions creates value for the business by improving:

1) The ability to adapt quickly to new requirements.

2) The success rate of changes and releases for an organization.

3) The predictions of service levels and warranties for new and changed services.

4) Confidence in the degree of compliance with the organization requirements during change.

5) Clarity of plans so the business can link their organization change plans to transition plans.

5.5 Basic Concepts in Service Transition Processes

1) Service knowledge management system (SKMS): It is a set of tools and databases that is used to manage knowledge, information and data. The SKMS includes the Configuration Management System (CMS), as well as other databases and information systems. The SKMS includes tools for collecting, storing, managing, updating, analyzing and presenting all the knowledge, information and data that an IT service provider will need to manage the full lifecycle of IT services.

2) Configuration item (CI): A Configuration Item (CI) is an asset, service component or other item which is, or will be, under the control of Configuration Management. CIs may vary widely in complexity, size and type, ranging from an entire service or system including all hardware, software, documentation and support staff to a single software module or a minor hardware component.

3) Configuration management system: A set of tools, data and information that is used to support service asset and configuration management.

4) Definitive media library (DML): Is defined as one or more locations that securely store the definitive and approved versions of all software CIs.

5) Change: The addition, modification or removal of anything that could have an effect on IT services. The scope should include changes to all architectures, processes, tools, metrics and documentation, as well as changes to IT services and other configuration items.

6) Change types

- Standard Change: A pre-approved Change that is low Risk, relatively common and follows a Procedure or Work Instruction. For example password reset or provision of standard equipment to a new employee. RFCs are not required to implement a Standard Change, and they are logged and tracked using a different mechanism, such as a Service Request.
- Emergency Change: A Change that must be introduced as soon as possible. For example to resolve a Major Incident or implement a Security patch.
- The Change Management Process will normally have a specific Procedure for handling Emergency Changes.

- Normal Change: Any service change that is not a standard change or an emergency change. There are three types of normal changes:
    - Minor change - authorized by change management staff directly.
    - Significant change- requires advice from change advisory board (CAB)
    - Major change -requires change proposal, business management approval

5. Service Transition

5.6.1 Change Management Process

Change Management Process is responsible for controlling the lifecycle of all changes, enabling beneficial changes to be made with minimum disruption to IT services.

A) Purpose of Change Management Process

Purpose of change management process is to control the lifecycle of all changes, enabling beneficial changes to be made with minimum disruption to IT services.

B) Objectives of Change Management Process

- Ensure that standardized methods and procedures are used for efficient and prompt handling of all changes, in order to minimize the impact of change related Incidents upon service quality, and consequently to improve the day to day operations of the organization.
- Respond to changing business requirements.
- Minimize impact/risk of implementing changes.
- Ensure all changes are approved at the appropriate level with the business and IT.
- Implement changes successfully.
- Implement changes in times that meet business needs.
- Use standard processes to record all changes.

C) Scope of Change Management Process

- Cover everything from configuration items (servers, infrastructure, documentation, services and configuration), management systems and tools, processes, metrics, solution and architecture from design strategy to continual service management excluding organization and business changes, and minor operational changes.
- Manage all changes in a controlled manner on all levels (strategic, tactical and operational) by making reference to the service portfolio.
- Change management is not responsible for the coordination of processes for the successful implementation of projects. This will be handled through the planning and transition support process.

D) Types of change request

There are three service change types they are: Standard, Emergency and Normal.

1) Standard Change: A pre-authorized change that is low risk, relatively common and follows a procedure or work instruction.

2) Emergency Change: A change that must be implemented as soon as possible, for example to resolve a major incident or implement a security patch.

3) Normal Change: Any service change that is not a standard change or an emergency change. Normal changes are often categorized into three types:

- Minor change - authorized by change management staff directly.
- Significant change- requires advice from change advisory board (CAB)
- Major change-requires change proposal, business management approval

E) Change models

Change model is a repeatable way of dealing with a particular category of change. Change Models defines specific agreed steps that will be followed for a change of this category. Change models may be very complex with many steps that require authorization (e.g. major software release) or may be very simple with no requirement for authorization (e.g. password reset).

Change models include:

- Steps to handle the change, including issues and unexpected events.
- Order steps should be taken, with dependences or co-processing defined
- Responsibilities - who should do what?
- Timescales and thresholds for completion of the actions.
- Escalation procedures - who should be contacted and when

F) Remediation Planning

Remediation is an action taken to recover after a failed change or release. Remediation may include back-out, invocation of service continuity plans, or other actions designed to enable the business process to continue.

G) Change Advisory Board and Emergency Change Advisory Board

Change Advisory Board:

- A group of people that supports the assessment, prioritization, authorization and scheduling of changes.
- A change advisory board is usually made up of representatives from: all areas within the IT service provider; the business; and third parties such as suppliers.

Emergency Change Advisory Board

- A subgroup of the change advisory board that makes decisions about emergency changes.
- Membership may be decided at the time a meeting is called, and depends on the nature of the emergency change.

H) Lifecycle of a Normal change

The Change Management Process consists of seven high-level activities specifically developed to manage the life cycle of change requests. Typical activities in managing individual changes are:

1) Create and record the Request for Change (RFC).

2) Review the RFC

Filter changes (e.g. incomplete or wrongly routed changes)

3) Assess and evaluate the change

- Establish the appropriate level of change authority
- Establish relevant areas of interest (i.e. who should be involved in the CAB)
- Evaluate justification, impact, cost, benefits, risks, and predicted performance
- Submit a request for evaluation to initiate activity from the change evaluation

4) Authorize the change

- Obtain authorization/rejection
- Communicate the decision with all stakeholders, in particular the RFC initiator

5) Plan updates

6) Coordinate change implementation

7) Review and close change

- Collate the change documentation, e.g. baselines and evaluation reports
- Review the change(s) and change documentation
- Ensure lessons learned details are recorded in the SKMS
- Close the change document when all actions are completed

5.6.2 Release and Deployment Management Process

Release and Deployment management is a process responsible for planning, scheduling and controlling the build, test and deployment of releases, and for delivering new functionality required by the business while protecting the integrity of existing services.

In the Release and Deployment management process different considerations apply in respect of the way in which the release is deployed. The most frequently occurring options for the rollout of releases are: "big bang" versus phased, "push and pull", automated or manual.

A) Purpose of Release and Deployment Management Process

- The purpose is to ensure that consistent and integral release packages are deployed in line with agreed policy and with plans agreed with the customers and stakeholders, and that this takes place under full and effective control.
- Any associated business and business process changes, including training and skills transfer, must be managed to take place in a timescale that is aligned with the release timetable.

B) Objectives of Release and Deployment Management Process

- The objective of release and deployment management is to build, test and deliver the capability to provide the services specified by service design.
- to define and agree on deployment plan with stakeholders
- Create and test release packages
- Maintain the integrity of the release packages and ensure that they are secured in DML.
- Ensure the new / changed services meets utility and warranty needs
- Capture lessons learned
- Ensure that skills and knowledge are transferred to operations and support staff

C) Scope of Release and Deployment Management Process

- The processes, systems, and functions required to deliver a release into production
- Build, ensure testing and deploy the release to the utility and warranty requirements
- Handover of service to operation teams
- 4) Manage all CIs and things related to the release.

D) Four phases of Release and Deployment Management Process

The process activities of release and deployment management are:

- Release and Deployment Planning - begins with planning a release and ends with change authorization to create the release
- Release Build and Test- the release package is built, tested, and checked into the DML, end with authorization to include the package in DML
- Deployment - deploy the package from DML and handover of service to operation, early life support might be needed for faster response and knowledge transfer

- Review and Close - experience and feedback are captured, performance targets, achievements are reviewed and lessons are learned

5.6.3 Knowledge Management Process

Knowledge Management is a process responsible for sharing perspectives, ideas, experience and information, and for ensuring that these are available in the right place and at the right time. The knowledge management process enables informed decisions, and improves efficiency by reducing the need to rediscover knowledge.

A) Purpose of Knowledge Management Process

The purpose of Knowledge Management is to ensure that the right person has the right knowledge at the right time to enable them to make sensible decisions about courses of action.

B) Objectives of Knowledge Management Process

- Improve the quality of management decision-making by ensuring that reliable and secure knowledge, information and data is available throughout the service lifecycle
- Enable the service provider to be more efficient and improve quality of service, increase satisfaction and reduce the cost of service by reducing the need to rediscover knowledge
- Ensure staff have a clear and common understanding of the value their services provide to customers and ways in which benefits are realized from use of services
- Maintain a service knowledge management system (SKMS) that provides controlled access to knowledge, information and data that is appropriate for each audience
- Gather, analyze, store, share, use and maintain knowledge, information and data throughout the service provider organization

C) Scope of Knowledge Management Process

- the management of data and information across the service management processes share of information with customers and users
- NOT including the detailed collection and maintenance (in Service Asset and Configuration Management)

D) Data-to-Information-to-Knowledge-to-Wisdom (DIKW) structure

- Data -- discrete facts about Events. Most organizations capture significant amounts of data in highly structured databases such as service management and service asset and configuration management tools/systems and databases

- Information - comes from providing context to data. Information is typically stored in semi-structured content such as documents, email and multimedia. The key knowledge management activity around information is managing the content in a way that makes it easy to capture, query, find, re-use and learn from experiences so that mistakes are not repeated and work is not duplicated.
- Knowledge - includes tacit experiences, ideas, insights, values, and judgments of individuals. People gain knowledge both from their own and from their peers expertise, as well as from the analysis of information
- Wisdom - makes use of knowledge to create value through correct and well-informed decisions. Wisdom involves having the application and contextual awareness to provide strong common-sense judgment.

Knowledge Management is typically displayed within the Data-to-Information-to-Knowledge-to Wisdom (DIKW) structure.

E) Service knowledge Management System (SKMS)

SKMS is a set of tools and databases that are used to manage knowledge and information. The SMKS includes the Configuration Management System, as well as other tools and databases. The SKMS stores, manages, updates and presents all information that an IT Service Provider needs to manage the full Lifecycle of IT Services.

One very important part of the SKMS is the configuration management system (CMS). The CMS describes the attributes and relationships of configuration items, many of which are themselves knowledge, information or data assets stored in the SKMS.

Previous Contents Next

ITIL® Foundation Exam Cram Notes : Service Operation (purpose, Objectives, Scope, And Value To Business)

5.6.4 Service Asset and Configuration Management Process (SACM)

Service Asset and Configuration management process ensures the integrity of service assets and configurations in order to support the effective and efficient management of the IT organization.

The main reason for configuration management is to gather the information needed (in a non-duplicated manner) about the IT components and how they relate to each other. The reason for this is to ensure that the relevant information is available for all the other processes to ensure that detailed impact and risk analysis can take place.

A) Purpose of Service Asset and Configuration Management Process(SACM)

- SACM ensures that the assets required to deliver services are properly controlled, and that accurate and reliable information about those assets is available when and where it is needed.
- This information includes details of how the assets have been configured and the relationships between assets.

B) Objectives of Service Asset and Configuration Management Process(SACM)

- Account for all the IT assets and configurations within the organization and its services.
- Provide accurate information on configurations and their documentation to support all the other service management processes.
- Provide a sound basis for incident management, problem management, change management and release management.
- Verify the configuration records against the infrastructure and correct any exceptions
- Plan, identify, control, record, report, audit and verify service assets and configuration items.
- Account for manage and protect the integrity of service assets and configuration items throughout their lifecycle.
- Provide accurate information to support business and service management.
- Ensure the integrity of those items by creating and maintaining an accurate Configuration Management System (CMS) as part of the Service knowledge management System (SKMS)

C) Scope of Service Asset and Configuration Management Process(SACM)

1) Management of the complete lifecycle of every Configuration Items (CIs)

- Ensures CIs are identified, base-lined and maintained, and changes controlled
- Ensures that releases into controlled environments and operational use are done on the basis of formal authorization.
- Provides a configuration model of the services and service assets by recording the relationships between configuration items

2) Interfaces to internal and external service providers where there are assets and configuration items to be controlled, e.g. shared assets

5.6.5 Transition Planning and Support Process

Transition planning and support process is responsible for planning all service transition processes and coordinating the resources that they require.

A) Purpose of Transition Planning and Support Process

- Plan and coordinate the resources to ensure that the requirements of Service Strategy encoded in Service Design are effectively realized in Service Operations.
- Identify, manage and control the risks of failure and disruption across transition activities.

B) Objectives of Transition Planning and Support Process

- Plan and coordinate the resources to establish successfully a new or changed service into production within the predicted cost, quality and time estimates.
- Ensure that all parties adopt the common framework of standard re-usable processes and supporting systems in order to improve the effectiveness and efficiency of the integrated planning and coordination activities.
- Provide clear and comprehensive plans that enable the customer and business change projects to align their activities with the Service Transition plans.

C) Scope of Transition Planning and Support Process

- Maintaining policies, standards and models for service transition activities and processes.
- Guiding each major change or new service through all service transition processes.
- Coordinating efforts to enable multiple transitions to be managed at the same time.
- Prioritizing conflicting requirements for service transition resources.
- Planning budget and resources to fulfill future requirements for service transition.
- Reviewing and improving performance of transition planning and support activities.

- Ensuring that service transition is coordinated with program and project management, service design and service development activities.

6. Service Operation

6.1 Purpose of Service Operation

The purpose of Service Operation is to coordinate and carry out the activities and processes required to deliver and manage services at agreed levels to business users and customers. Service Operation is also responsible for the ongoing management of the technology that is used to deliver and support services.

6.2 Objectives of Service Operation

1) Maintain business satisfaction and confidence in IT through effective and efficient delivery and support of agreed IT services.

2) Minimize the impact of service outages on day-to-day business activities.

3) Ensure that access to agreed IT services is only provided to those authorized to receive those services.

6.3 Scope of Service Operation

1) The services themselves - activities that form part of a service is included in service operation, whether it is performed by the service provider, an external supplier or the user or customer of that service.

2) Service management processes - the ongoing management and execution of the many service management processes that are performed in service operation.

3) Technology - the management of the infrastructure used to deliver services

4) People - regardless of what services, processes and technology are managed, they are all about people. It is people who drive the demand for the organization's services and products and it is people who decide how this will be done.

6.4 Value to Business

1) Ensuring that services are operated within expected performance parameters

2) Restoring services quickly in the event of service interruption.

3) Minimizing impact to the business in the event of service interruption.

4) Providing a focal point for communication between users and the Service Provider organization

6.5 Processes

6.5.1 Incident Management Process

An incident is defined as an unplanned interruption to an IT service, a reduction in the quality of an IT service, or a failure of a CI (configuration item) that has not yet impacted an IT service.

Incident Management is responsible for progress of all incidents from reporting to closing - usually the responsibility of service desk.

A) Purpose of Incident Management Process

The purpose of Incident Management is to recover normal (i.e. agreed) service operation, as quickly as possible, after an incident has been detected / recorded.

B) Objectives of Incident Management Process

- Make sure that standardized procedures and methods are used for prompt and efficient response, documentation, analysis, reporting of incidents and ongoing management
- Communication and visibility of incidents should be improved.
- Improve business perception of IT with the help of a professional approach so that incidents will be resolved and reported quickly.
- Align incident management activities and priorities with those of the business.
- Maintain the user satisfaction without losing the quality of IT services.

C) Scope of Incident Management Process

Handle all incidents (event which disrupts, or which could disrupt, a service), either by service desk reports or event management tool alerts. Incidents are reported and/or logged by technical staff.

D) Basic Concepts

- Incident: An incident is defined as an unplanned interruption to an IT service, a reduction in the quality of an IT service, or a failure of a CI (configuration item) that has not yet impacted an IT service.
- Timescales: Timescales must be agreed for all incident handling according to their priority; this includes response and resolution targets. All support groups should be made fully aware of these timescales. The tool should be used to automate timescales and escalate the incident as required based on predefined rules.

- Incident Model: An incident model is a template that can be reused for recurrent incidents. It can be practical to predefine 'standard' incident models and apply them when incidents occur. They contribute to a faster entry and a more efficient treatment.
- Major Incident: define what constitutes a major incident and follow pre-defined procedures, need to inform users on the progress.
- Incident Status Tracking.

Incident status tracking field value examples:

1) New - an incident is submitted but is not assigned to a group or resource for resolution.

2) Assigned - an incident is assigned to a group or resource for resolution.

3) In process - the incident is in the process of being investigated for resolution.

4) Resolved - a resolution has been put in place.

5) Closed - the user has agreed that the incident has been resolved and that normal state operations have been restored

6) Expanded Incident Life cycle: Detailed stages in the lifecycle of an incident. The stages are detection, diagnosis, repair, recovery and restoration. The expanded incident lifecycle is used to help understand all contributions to the impact of incidents and to plan for how these could be controlled or reduced.

7) Impact: A measure of the effect of an incident, problem, or change on business processes. Impact is often based on how service levels will be affected. Impact and urgency are used to assign priority

8) Urgency - a measure of how long it will be until an incident, problem or change has a significant impact on the business.

9) Priority - a category used to identify the relative importance of an incident, problem or change, based on impact and urgency. High priority (Priority 1) is given for an incident with high impact and high urgency.

E) Incident Management Process Activities

Lifecycle of Incidents are as follows:

1) Incident Identification - realize an incident before the user notices / reports with event management (a reactive process)

2) Incident Logging - log ALL incidents for service-level management reporting and problem management. Information may include:

- unique reference number
- incident category
- impact, urgency and priority
- steps to resolution and known errors
- time from logging to closure
- Activities undertaken to resolve the incident and when these took place.
- Resolution date and time
- Closure category, date and time

3) Incident Categorization - use a simple categorization for effective implementation

4) Incident Prioritization - consider business impact and urgency, to be completed in a pre-agreed time depending on the priority, may change during the lifecycle

5) Initial Diagnosis - the service desk to diagnose the fault and try to resolve it with the known error database (by problem management), incident models or other tools (incident matching)

6) Incident Escalation - the incidents are owned by service desk (need to track till closure).

- Functional escalation - service desk unable to solve the incident within a given time.
- hierarchic escalation - inform management of major incidents / incidents not progressing based on SLA target time

7) Investigation and Diagnosis - try to find out what has happened and how to resolve

8) Resolution and Recovery - test potential resolutions to ensure the incident has been solved without causing adverse consequences

9) Incident Closure - contact user to verify and review categorization, finish documentation. Closed incidents may be re-opened if the incident re-surfaces again. Any appropriate function can close the incident.

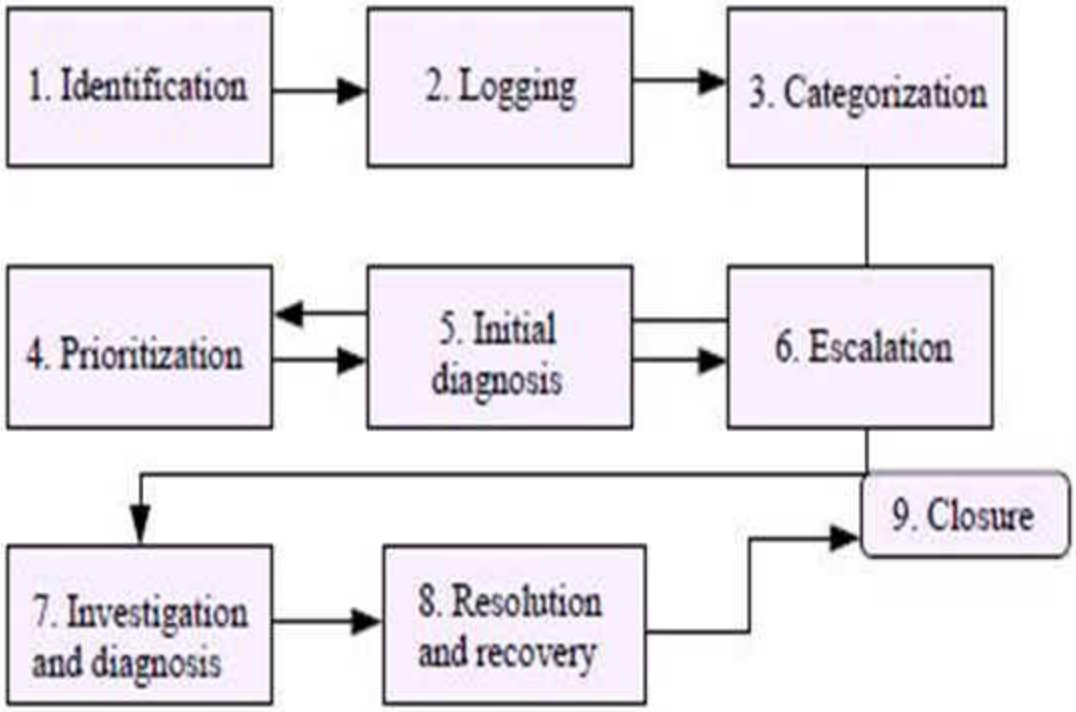


Figure: Lifecycle of Incidents

F) Incident Management Process- Interfaces with other stages of ITIL Service Lifecycle.

1) Interfaces with Service Design

- Service Level Management: The ability to resolve incidents in a specified time is a key part of delivering an agreed level of service.
- Information Security Management: Providing security-related incident information as needed to support service design activities and gain a full picture of the effectiveness of the security measures as a whole based on an insight into all security incidents.
- Capacity Management: Incident management provides a trigger for performance monitoring where there appears to be a performance problem.
- Availability Management: Availability management will use incident management data to determine the availability of IT services and look at where the incident lifecycle can be improved.

2) Interfaces with Service Transition:

a) Service asset and configuration management:

- Provides data used to identify and progress incidents and to assess the impact of an incident; also contains information on which categories of incident to assign to which support group.

- In turn, incident management can maintain the status of faulty CIs. It can also assist service asset and configuration management to audit the infrastructure when working to resolve an incident.

b) Change Management:

- Where a change is needed to implement a workaround or resolution, it will be logged as an RFC and progressed through change management.
- In turn, incident management is able to detect and resolve incidents that arise from failed changes.

3) Interfaces with Service Operation:

a) Problem management:

- For some incidents, it will be appropriate for problem management to investigate and resolve the underlying cause to prevent or reduce the impact of recurrence.
- Incident management provides reporting point for these.
- Problem management can provide known errors for faster incident resolution through workarounds to restore service.

b) Access management:

- Incidents should be raised when unauthorized access attempts and security breaches have been detected
- A history of incidents should also be maintained to support forensic investigation activities, resolution of access breaches.

Previous Contents Next

ITIL® Foundation Exam Cram Notes : Problem Management Process (activities, Categorizing, Prioritizing, Etc.)

examguides.com/ITILFund/itilf-8.htm

6.5.2 Problem Management Process

A problem is defined as an underlying cause of one or more incidents. The cause is not usually known at the time a problem record is created, and the problem management process is responsible for further investigation.

A) Purpose of Problem Management Process

- To document, investigate, and remove causes of incidents.
- To minimize the adverse impact of incidents and problems on the business that are caused by underlying errors within the IT Infrastructure, and to proactively prevent recurrence of incidents related to these errors.

B) Objectives of Problem Management Process

- Prevent problems and resulting incidents from happening.
- Eliminate recurring incidents.
- Minimize the impact of incidents that cannot be prevented.

C) Scope of Problem Management Process

- Diagnosis the root cause of incidents
- Take steps to eliminate them (with other processes, in particular change management process).
- Document problems, workarounds and resolutions (maintain the known error database) for more effective handling of similar incidents

D) Basic concepts

1) Reactive and Proactive problem management activities:

a) Reactive problem management process

- Reactive problem management process activities will typically be triggered in reaction to an incident that has taken place.

- Reactive problem management complements incident management activities by focusing on the underlying cause of an incident to prevent its recurrence and identifying workarounds when necessary.

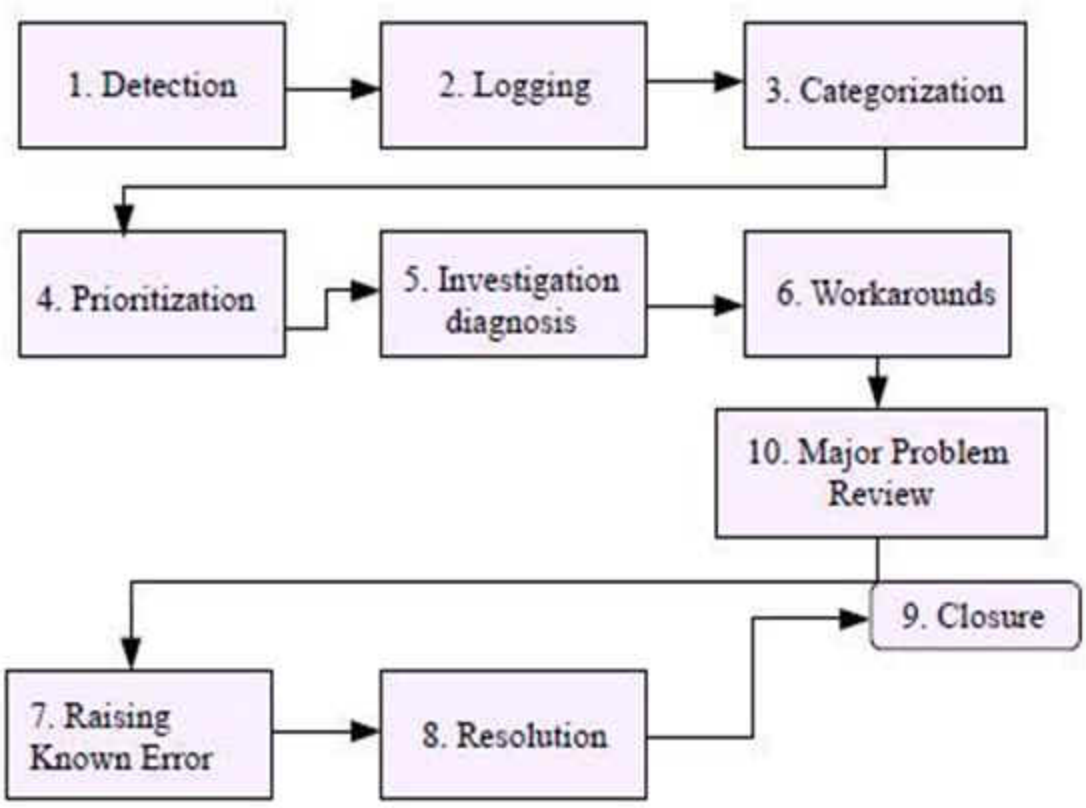
b) Proactive problem management process

- Proactive problem management process activities are triggered by activities seeking to improve services.
- Proactive problem management complements CSI activities by helping to identify workarounds and improvement actions that can improve the quality of a service.

2) Problem Models : handle problems that have not and will not be resolved (e.g. the cost of a permanent resolution is too high) by some pre-defined workaround

E) Problem Management Process Activities

Life Cycle of Problem Management is as follows:



1) Detecting Problems - identify problems in reactive / proactive ways

2) Logging Problems

- Record all relevant problem details for a full historic record
- log in the problem record (link to the incidents)

3) Categorizing Problems: Categorize Problems in the same way as incidents, using the same coding system, so the true nature of the problem can be easily traced in the future and meaningful management information can be had, and enables incidents and problems to be more readily matched.

4) Prioritizing Problems - depends on impact(number of users being affected) and urgency of the problem(how quickly the business needs resolution).

5) Investigating and Diagnosing Problems

- Apply problem-solving techniques.
- Use the CMS to help determine impact and pinpoint and diagnose the exact point of failure.
- Use the KEDB for problem-matching techniques to see if the problem has occurred before and, if so, to find the resolution

6) Identifying a Workaround - provides the workaround to service desk for resolving the incident and reassesses the priority

7) Raising a Known Error Record

- A known error is a problem with a documented root cause and workaround.
- Known error records should identify the related problem record and document the status of actions being taken to resolve the problem, its root cause and workaround.
- All known error records should be stored in the known error database (KEDB)

8) Problem Resolution - implement the solution through change management (as emergency change)

9) Problem Closure - a permanent solution has been tested and implemented so that the problem will not occur again (user confirmation NOT needed).

10) Major Problem Review

After every major problem, conduct a lessons learned review examining:

- Things done right and wrong
- What to do better in the future
- How to prevent recurrence.
- Whether there is any third-party responsibility and if follow-up actions are needed.

F) Incident Management Process- Interfaces with other stages of ITIL Service Lifecycle.

1) Interfaces with Service Design

a) Financial Management for IT services:

- Assists in assessing the impact of proposed resolutions or workarounds, and pain value analysis
- Problem management provides information about the cost of resolving and preventing problems
- Used as input into the budgeting and accounting systems and total cost of ownership calculations.

2) Interfaces with Service Design

a) Availability Management:

- Involved with seeking reduced downtime and increased uptime
- Much of the management information available in problem management will be communicated to availability management.

b) Capacity Management:

- Some problems will require investigation by capacity management teams and Techniques.
- Problem management provides management information on the quality of decisions made during the capacity planning process

c) IT Service Continuity Management:

Problem management acts as an entry point into IT service continuity management where a significant problem is not resolved before it starts to have a major impact on the business.

d) Service Level Management:

- Problem management contributes to improvements in service levels, and its information is used for some SLA review components.
- SLM provides parameters within which problem management works.

3) Interfaces with Service Transition

a) Change Management:

- Problem management ensures resolutions/workarounds that require a CI change are given to change management via RFC.
- Change management tracks changes, advises problem management

b) Service Assets and Configuration Management:

Problem management uses the CMS to identify faulty CIs and also to determine the impact of problems and resolutions.

c) Release and Deployment Management:

- Responsible for deploying problem fixes out to the live environment.
- Problem management will help resolve problems caused by faults during the release process.

d) Knowledge Management: The SKMS can be used to form the basis for the KEDB and hold or integrate with the problem records.

4) Interfaces with Service CSI

a) Seven step improvement Process:

- Incidents and problems are a basis for identifying service improvement opportunities; adding them to the CSI register.
- Proactive problem management activities may identify underlying issues that if addressed, can contribute to increases in service quality and end user/customer satisfaction

6.5.3 Event Management Process

An event can be defined as any detectable or discernable occurrence that has significance for the management of the IT infrastructure or the delivery of IT service, and evaluation of the impact a deviation might cause to the service.

Event Management is the process responsible for managing events throughout their lifecycle. Event management is one of the main activities of IT operations.

Modern systems make use of event monitoring tools to monitor configuration items for signals and irregularities. These tools are of two types they are:

a) Active Monitoring Tools: actively seek responses to confirm correctness

b) Passive Monitoring Tools: detect and correlate operational alerts or communications generated by CIs.

A) Purpose of Event Management Process

- Manage events throughout their lifecycle.
- Coordinate the lifecycle of activities to detect and make sense of events and determine appropriate control action.

B) Objectives of Event Management Process

- To provide the entry point for the execution of many service operation processes and activities.

- To provide a way of comparing actual performance and behavior against design standards and SLA's.
- Provides the ability to detect, interpret and initiate appropriate action for events.
- Is the basis for operational monitoring and control and the entry point for many service operation activities
- Provides operational information as well as warnings and exceptions to aid automation.
- Supports continual service improvement activities of service assurance and reporting.

C) Scope of Event Management Process

1) Event management can be applied to any aspect of service management that needs to be controlled and which can be automated. These include:

a) Configuration Items:

- Some configuration items will be included because they need to stay in a constant state.
- Some configuration items will be included because their status needs to change frequently and event management can be used to automate this and update the configuration management system.

2) Environmental conditions (e.g. fire and smoke detection).

3) Software license monitoring for usage to ensure optimum/legal license utilization and allocation.

4) Security (e.g. intrusion detection).

5) Normal activity (e.g. tracking the use of an application or the performance of a server)

6.5.4 Request Fulfillment Process

A Service Request is a formal request from a user for something to be provided. Request fulfillment is the process responsible for managing the lifecycle of all service requests.

A) Purpose of Request Fulfillment Process : Purpose of Request Management process is to managing the lifecycle of all user service requests.

B) Objectives of Request Fulfillment Process

- To provide a channel for users to request and receive standard services for which a predefined approval qualification process exists.
- To provide information to users and customers about the availability of services and the procedure for obtaining them.
- To source and deliver the components of requested standard services (e.g. licenses and software media).
- To assist with general information, complaints or comments.

C) Scope of Request Fulfillment Process

- Any requests or just standard IT requests may vary from organization to organization.
- Some organizations may use incident management process to handle requests

3) To provide a self-help support capability to users to improve quality and reduce costs.

6.5.5 Access Management Process

Access management is the process of granting authorized users the right to use a service, while preventing access to non-authorized users. It is, therefore, the execution of policies and actions defined in information security and availability management.

A) Purpose of Access Management Process

- To implement parts of the security policies defined in Information Security Management
- To keep the access privileges up-to-date.

B) Objectives of Access Management Process

- Manage access to services based on policies and actions defined in information security management.
- Efficiently respond to requests for granting access to services, changing access rights or restricting access, ensuring the rights provided or changed are properly granted.
- Ensure all requests for access are verified and authorized and dealt with efficiently

C) Scope of Access Management Process

- Execution of the policies in information security management, in that it enables the organization to manage the confidentiality, availability and integrity of the organization's data and intellectual property.
- Ensures that users are given the right to use a service, but it does not ensure that this access is available at all agreed times - this is provided by availability management.
- Executed by all technical and application management functions and is usually not a separate function, but there is likely a single control point of coordination, usually in IT operations management or on the service desk.
- Can be initiated by a service request.

Previous Contents Next

ITIL® Foundation Exam Cram Notes : Continual Service Improvement (CSI)

7. Continual Service Improvement (CSI)

7.1 Purpose of CSI

To align IT services with changing business needs by identifying and implementing improvements to IT services that support business processes.

7.2 Objectives of CSI

1) To measure and analyze service level achievements by comparing them to the requirements in the Service Level Agreement (SLA)

2) To recommend improvements in all phases of the lifecycle

3) To introduce activities which will increase the quality, efficiency, effectiveness and customer satisfaction of the services and the IT service management processes

4) To operate more cost effective IT services without sacrificing customer satisfaction

5) To use suitable quality management methods for improvement activities

7.3 Scope of CSI

1) The overall health of ITSM as a discipline.

2) Continual tuning of the IT services to the current and future needs of the business.

3) Continual tuning of the IT service portfolio.

4) The maturity of the IT processes which enable the services

7.4 Value to Business

1) To validate previous decisions.

2) To set direction for activities in order to meet targets.

3) To justify (with facts) that a course of action is required.

4) To identify a point of intervention including required changes and corrective actions.

7.5 Basic Concepts in CSI

1) CSI Registry:

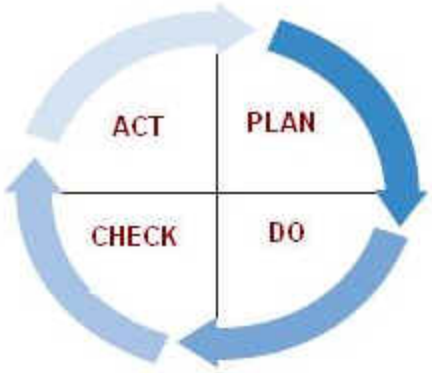
a) Is used to record all individual improvements as improvements may be made concurrently.

b) It is a service asset managed by the service knowledge management system (SKMS).

c) It includes: ID, Relative size, Timescale, Description, Priority, KPI metric and Justification

2) The Deming Cycle: The Deming Cycle is proposed by W. Edwards Deming.

The four stages of the cycle are Plan, Do, Check and Act, followed by a consolidation phase to prevent rolling backwards. PDCA sets a clear pattern for CSI efforts:



a) Plan - establish goals for improvement.

b) Do - develop and implement a project to close the gap.

c) Check - compare the implemented environment to the measures of success established in the Plan phase.

d) Act - determine if further work is required to close remaining gaps, allocation of resources necessary to support another round of improvement

7.6 CSI Improvement approach

The figure below shows an overall approach to continual service improvement (CSI) and illustrates a continual cycle of improvement. The improvement process can be summarized in six steps:

1) Embracing the vision by understanding the high level business objectives. The vision should align the business and IT strategies.

2) Assessing the current situation to obtain an accurate, unbiased snapshot of where the organization is right now. This baseline assessment is an analysis of the current position in terms of the business, organization, people, process and technology.

3) Understanding and agreeing on the priorities for improvement based on a deeper development of the principles defined in the vision.

4) Detailing the CSI plan to achieve higher quality service provision by implementing IT service management processes.

5) Verify that measurements and metrics are in place to ensure that milestones were achieved, process compliance is high, and business objectives and priorities were met by the level of service.

6) Finally, the process should ensure that the momentum for quality improvement is maintained by assuring that changes become embedded in the organization.

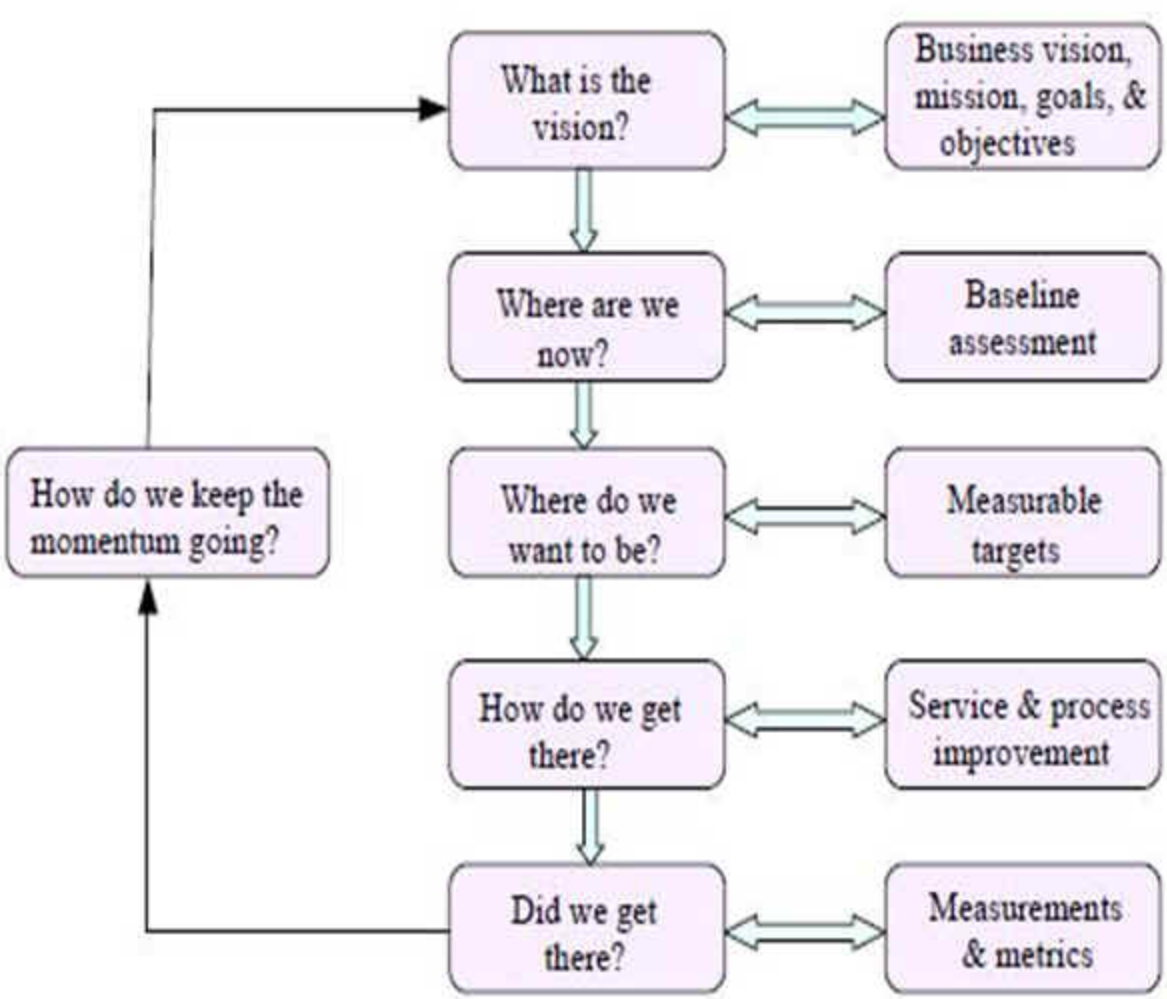


Figure: CSI Approach

7.7 Relationship between CSI and KPI's

1) Critical Success Factor (CSF) is something that must happen if an IT service, process, plan, process, or other activity is to succeed.

a) Associate no more than two to five CSFs with a service or process

2) Key Performance Indicators (KPI) are used to measure whether the critical success factors are achieved.

a) Define no more than two to five KPIs per CSF.

b) KPI's can be quantitative (e.g. cost) or qualitative (e.g. customer satisfaction)

3) Define, monitor and report on only two to three KPIs for each CSF.

a) As the maturity of a service and service management processes increase, additional KPIs can be added.

b) Based on what is important to the business and IT management, the KPIs may change over a period of time.

c) As service management processes are implemented, this will often change the KPIs of other processes.

7.8 Baselines

1) Baselines enable a view of the current situation and also a clear starting point for feature measurements.

2) Baselines need to be documented.

3) Baselines are applicable at strategic goals and objectives, tactical process maturity, and operational metrics and KPIs.

4) Baseline is an initial data point to see if a service or process needs improvement.

7.9 Types of Metrics

A metric is a scale of measure that allows you to define what is to be measured. There are three types of metrics to collect to support CSI activities, they are:

1) Service metrics - these metrics are the results of the end to end service. Technology metrics are used to produce the service metrics.

2) Process metrics - these metrics are captured in the form of Critical Success Factors (CSFs), Key Performance Indicators (KPIs) and activity metrics for the service management processes. Four key areas that KPIs can measure are quality, performance, value and compliance of following the process. CSI would use these metrics as input in identifying improvement opportunities for each process.

3) Technology metrics - these metrics are often associated with component and application based metrics such as performance and availability

7.10 Processes

7.10.1 The Seven Step Improvement Process

A) Purpose of Seven Step Improvement Process

- To define and manage the steps required to implement improvements successfully.
- To identify and define the measurements and metrics.
- To gather, analyze and report the data.
- To manage the implementation

B) Objectives of Seven Step Improvement Process

- Identify improvement opportunities in cost and quality with financial justification (a business case if more complex).
- Identify the measurements and metrics.
- Continually review services to ensure they are aligned with business objectives.
- Understanding what to measure, why it is being measured and carefully defining the successful outcome.

C) Scope of Seven Step Improvement Process

- Analyze performance and capabilities throughout the lifecycle.
- Make the best use of latest technology.
- Improve organizational structures.
- Continual alignment of the portfolio of IT services with the current and future business needs as well as the maturity of the enabling IT processes for each service.

D) The main steps of Seven Step Improvement Process

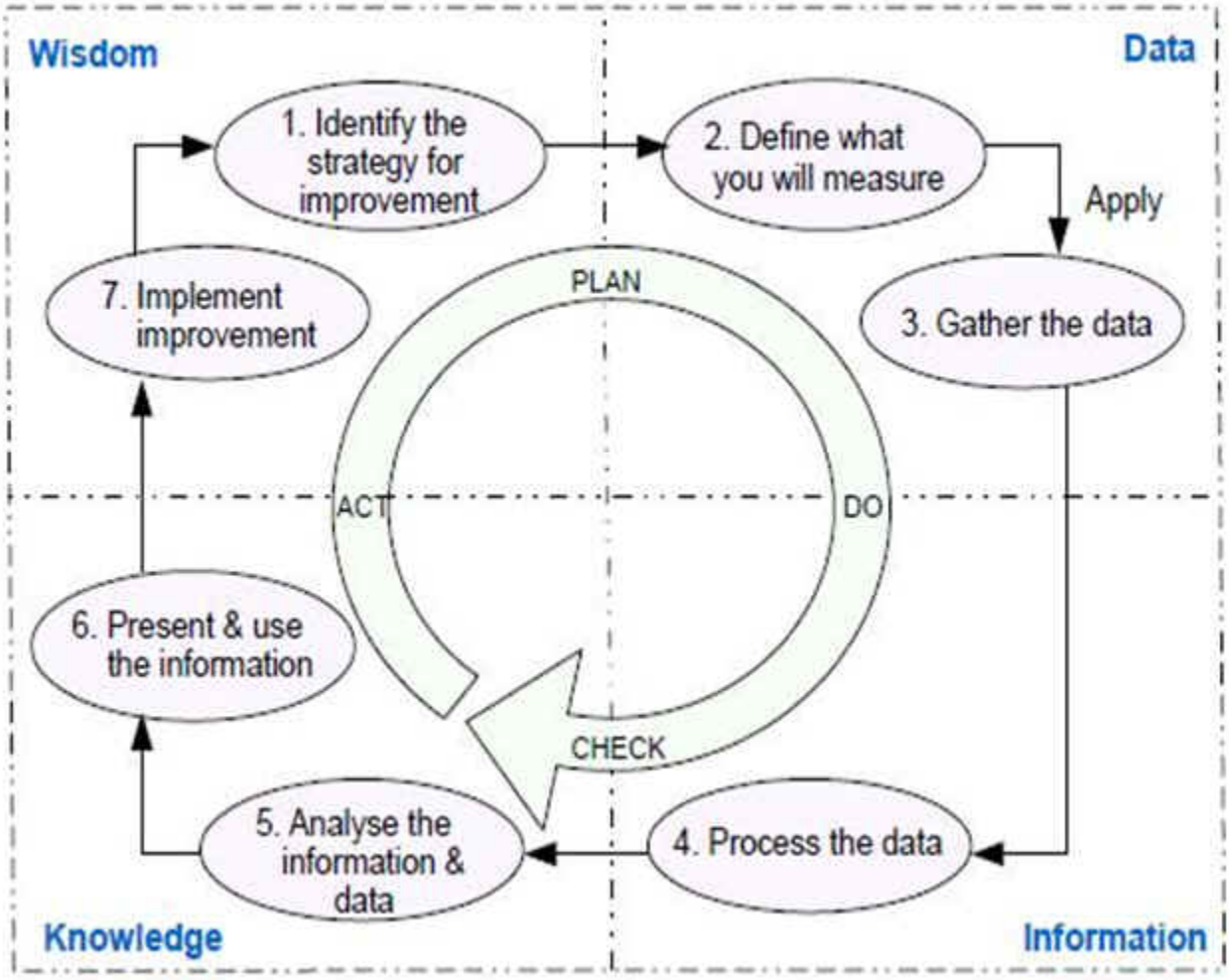


Figure: The Seven Step Improvement Process

1) Identify the strategy for improvement: Identify the overall vision, business need, the strategy and the tactical and operational goals.

2) Define what you will measure: There may be a gap between the capabilities of current tools and mechanisms to provide the necessary information. If the desired data really cannot be gathered or if the cost is prohibitive, the measures in Step 1 may need to be revisited.

3) Gather the data: monitor and capture exceptions, resolutions and trends with the data.

4) Process the data: Here the data is processed in alignment with the CSFs and KPIs specified. This means that timeframes are coordinated, unaligned data is rationalized and made consistent, and gaps in the data are identified. The simple goal of this step is to process data from multiple disparate sources to give it context that can be compared. Once we have rationalized the data we can then begin analysis.

5) Analyze the information and data: Transform the information into knowledge. Develop an understanding of the real meaning of identified patterns and trends, by querying the results to understand its intrinsic value.

6) Present and use the information: present in the correct format with the appropriate details according to audience types. Knowledge is presented to the business in a form and manner that reflects their needs and assists them in determining the next steps.

7) Implement Improvement: Knowledge gained is used to optimize, improve and correct services and processes. Issues have been identified and now solutions are implemented - wisdom is applied to the knowledge. Improvements to improve the service or process are communicated and explained to the organization, then the organization establishes a new baseline and the cycle begins anew.

Previous Contents Next

ITIL® Foundation Exam Cram Notes : Service Desk Function,Roles,Technology And Architecture

8. Functions

8.1 Service Desk Function

A) Role of Service desk function

- Handles incidents, escalates incidents to problem management staff, manages service requests and answers questions.
- Provides an interface for other activities such as customer change requests, maintenance contracts, software licenses, SLM, service asset and configuration management, availability management, financial management for IT services, and IT service continuity management.

B) Objectives of Service desk function

- Logging all relevant incident/service request details, and allocating categorization and prioritization codes.
- Providing first line investigation and diagnosis.
- Resolving those incidents/service requests that do not need escalating across IT.
- Escalating incidents/service requests that the service desk cannot resolve within agreed timescales.
- Closing all resolved incidents, service requests and other calls.
- Conducting customer/user satisfaction call backs/surveys as agreed.
- Communication with users - keeping them informed of incident progress, notifying them of impending changes or agreed outages, etc.
- Updating the configuration management system under the direction and approval of configuration management if so agreed

C) Organizational structures of Service desk function

- Local Service Desk - co-located with users in the office, efficient but expensive, need more coordination among different service desks within the organization.
- Centralized Service Desk - economy of scale, better coordination, knowledge and mind sharing, no direct physical interaction with users.

- Virtual Service Desk - physically separated service desks linked together with a common system to log issues and communications, allocation of calls based on workload.
- Follow the Sun - similar to virtual service desk, allocation of calls based on time of day for 24-hour support, great for global organization.
- Specialized Service Desk Groups - need to specify the type of incidents on the user side to reach the support staff to allow faster resolution

8.2 The Technical Management Function

A) Role of Technical management function

- Manage the IT infrastructure.
- Provide enough skilled supporting staff for the whole lifecycle from strategy to operation and service improvement.
- Guide and support operations staff members

B) Objectives of Technical management function

- Well designed and highly resilient, cost-effective technical topology.
- Use of technical skills to maintain the technical infrastructure in optimum condition.
- Swift use of technical skills to speedily diagnose and resolve any technical failures

8.3 Application Management Function

A) Role of Application management function

- Manage the IT applications
- Ensures that the knowledge required to design, test, manage and improve IT services is identified, developed and refined.
- Carry out training needs analysis and provide the training to technical and operation staff

B) Objectives of Application management function

- Identify requirements for applications (utility and warranty)
- Design, assist in deployment and support applications.
- Identify and implement improvements

C) Differences between application management function and application development

- Application development is concerned with the one-time set of activities to design and construct application solutions. Whereas, application management function is concerned about the lifetime of the application.

- Application development focuses only on utility. Whereas, application management function focuses on both utility and warranty.
- Application development focuses on software development. Whereas, application management function focuses on operation and improvement.
- In application development staff is typically rewarded for creativity and for completing one project so that they can move on to the next project. Whereas, in application management staff are typically rewarded for consistency and for preventing unexpected events and unauthorized functionality.
- In application development, most development work is done in projects where the focus is on delivering specific units of work to specification, on time and within budget. Whereas, in application management most work is done as part of repeatable, ongoing processes.
- Management is needed for applications developed externally

8.4 The IT Operations Management Function

A) Role of IT operations management function

- Carry out day-to-day activities for the delivery of the services to ensure SLA is met - i.e. provide quality service in an efficient and cost effective manner.
- Technical and Application Management Functions define the activities to be carried out by Operations Management Function.

B) Objectives of IT operations management function

- Responsible for the day to day running of the IT infrastructure.
- As per performance standards created in service design.
- Maintaining the "status quo" to achieve infrastructure stability.
- Identifying opportunities to improve operational performance and save costs.
- Initial diagnosis and resolution of operational incidents

C) IT operations Control : IT operations control oversees execution and monitoring of operational activities and events in the IT infrastructure with the help of an operations bridge or network operations center.

D) Facilities Management : Facilities management refers to the management of the physical IT environment, typically a data center or computer rooms and recovery sites together with all the power and cooling equipment. Facilities management also includes the coordination of large-scale consolidation projects, e.g. data center consolidation or server consolidation projects.

9. Roles

9.1 Process owner

A) Role of Process owner

- The process owner role is accountable for ensuring that a process is fit for purpose.
- The process owner role is accountable for ensuring that their process is performed according to the agreed and documented standard and meets the aims of the process definition.

B) Responsibilities of Process owner

- Ensure the process works efficiently and effectively.
- Develop the process strategy, policies and standards.
- Design the process and improve its design, document the process.
- Design the metrics to be collected and monitor for efficiency.
- Ensure the availability of resources and capabilities to carry out the process.
- Responsible for the consistency of the process application

9.2 Process manager

A) Role of Process manager

- The process manager role is accountable for operational management of a process.
- The process manager role is often assigned to the person who carries out the process owner role, but the two roles may be separate in larger organizations.

B) Responsibilities of Process manager

- Working with the process owner to plan and coordinate all process activities.
- Ensuring that all activities are carried out as required throughout the service lifecycle.
- Appointing people to the required roles.
- Managing resources assigned to the process.
- Working with service owners and other process managers to ensure the smooth running of services.
- Monitoring and reporting on process performance.
- Identifying improvement opportunities for inclusion in the CSI register.
- Working with the CSI manager and process owner to review and prioritize improvements in the CSI register.
- Making improvements to the process implementation.

9.3 Process practitioner

A) Role of Process practitioner

- Process practitioner is responsible for carrying out one or more process activities under the guidance of process manager.

- For some process, process practitioner role may be combined with process manager role.

B) Responsibilities of Process practitioner

- Understand and complete the process activities.
- Work with process stakeholders to ensure correctness.
- Produce records of the process activities.
- Identify improvements

9.4 Service owner

A) Role of Service owner

- The service owner is accountable for the delivery of a specific IT service.
- Service owner is accountable for delivering the service across all process areas in an effective and efficient manner.
- Accountable to the IT director or service management director for the delivery of the service

B) Responsibilities of Service owner

- Service owner represents the service.
- Work with all IT groups and process owners to deliver, support and improve the service to the required standards according to business objectives.
- Work with customers to understand the requirements, raise RFC and solve issues.
- Soliciting required data, statistics and reports for analysis and to facilitate effective service monitoring and performance.
- Study impacts on the service by changes in other services / environments.
- Maintain the service catalogue entry.
- Ensure the process conforms to all policies
- As a primary stakeholder in all the processes involved with the service

9.5 RACI model

A) Acronym of RACI : RACI is an acronym for the four main roles of being:

- Responsible: The person or people responsible for correct execution - for getting the job done
- Accountable the person who has ownership of quality and the end result. Only one person can be accountable for each task.
- Consulted the people who are consulted and whose opinions are sought. They have involvement through input of knowledge and information.
- Informed the people who are kept up to date on progress. They receive information about process execution and quality.

B) RACI model- typical steps to create RACI matrix

- Identify the processes/activities.
- Identify and define the roles
- Conduct meetings and assign the RACI codes
- Identify any gaps or overlaps. E.g., Multiple R's or no R's
- Distribute the chart and incorporate feedback
- Ensure that the allocations are being followed

Typical example of a RACI Matrix is as shown below:

a) Left column in the matrix represents: activities, actions, decisions.

b) Top row in the matrix represents: functional roles responsible for process or service.

c) Cells in the matrix represents: RACI assignments

	Role 1	Role 2	Role 3	Role 4
Activity 1	AR	C	I	I
Activity 2	A	R	C	C
Activity 3	R	A	I	
Activity 4	A	R	C	I

Figure: An example of a RACI matrix

10. Technology and Architecture

10.1 Role of automation

1) The capacity of automated resources can be more easily adjusted in response to variations in demand volumes.

2) Automated resources can handle capacity with fewer restrictions on time of access, they can therefore be used to serve demand across time zones and after-hours.

3) Automated systems present a good basis for measuring and improving service processes by holding constant the factor of human resources; conversely, they can be used to measure the differential impact on service quality and costs due to varying levels of knowledge, skills and experience of human resources.

4) Many optimization problems such as scheduling, routing and allocation of resources require computing power that is beyond the capacity of human agents.

5) Automation is a means for capturing the knowledge required for a service process, codified knowledge is relatively easy to distribute in the organization in a consistent and secure manner. It reduces the depreciation of knowledge when employees move within the organization or permanently leave

Previous Contents