# **ITIL Essentials Study Guide**

### Introduction

Service Support Functions:

- Service Desk
- Incident Management
- Problem Management
- Change Management
- Configuration Management
- Release Management

Service Delivery Functions:

- Availability Management
- IT Services Continuity Management
- Capacity Management
- Financial Management
- Service Level Management

# **Configuration Management**

Objectives:

- Providing information on the IT infrastructure
  - To all other processes
  - IT Management
- Enabling control of the infrastructure by monitoring and maintaining information on:
  - o All the resources needed to deliver services
  - Configuration Item (CI) status and history
  - Configuration Item relationships

Tasks:

- Identification and naming
- Management information
- Verification
- Control
- Status Accounting

Asset: Component of a business process like people, accommodation, computer systems, paper records, fax machines, etc.

Configuration Management Database: A database, which contains all relevant details of each Configuration Item (CI) and details of the important relationships between CIs.

A Configuration Item (CI):

- Is needed to deliver a service
- Is uniquely identifiable
- Is subject to change
- Can be managed

A Configuration Item (CI) has:

- a Category
- Relationships
- Attributes
- a Status

Variant: A Configuration Item (CI) that has the same basic functionality as another Configuration Item (CI) but is different in some small way (ex: has more memory)

Baseline: A snapshot of the state of a Configuration Item and any component or related Configuration Items, frozen in time for a particular purpose (such as the ability to return a service to a trusted state if a change goes wrong)

Configuration Management supports all other processes!

Scope vs. Detail

Relationships – Common Types:

- Is a component of
- Is a copy of
- Relates to
- Relates with
- Is used by

# Service Desk

Objectives:

- To be the primary point of call for all:
  - Calls
  - o Questions
  - Requests
  - Complaints
  - o Remarks
- To restore the service as quickly as possible
- To manage the incident life-cycle (coordinating resolution)
- To support business activities
- To generate reports, to communicate and to promote

#### Different Desks

- Call Center: Handling large call volumes of telephone-based transactions.
- Help Desk: To manage, coordinate, and resolve Incidents as quickly as possible.
- Service Desk: Allowing business processes to be integrated into the Service Management infrastructure. It not only handles Incidents, Problems and questions, but also provides an interface for other activities.

Service Desk Essentials:

- Single point of contact / Restore service ASAP
- Tasks: Customer Interface, Business Support, Incident Control & Management Information
- Concentrates on incident lifecycle management
- Incident: Unexpected disruption to agreed service
- Priority determined by business impact and urgency
- Correct assessment of priorities enables the deployment of manpower and other resources to be in the best interests of the customer
- Escalation and referral

# **Incident Management**

Objectives:

- To restore normal service as quickly as possible
- Minimize the adverse impact on business operations
- Ensuring that the best possible levels of service quality and availability are maintained according to SLAs.

Incident: Any event which is not part of the standard operation of a service and which causes or may cause an interruption to or a reduction in the quality of that service.

Work-Around: Method of avoiding an Incident or Problem.

Service Request: Every Incident not being a failure in the IT Infrastructure.

Problem: The unknown root cause of one or more incidents.

Known Error: A condition that exists after the successful diagnosis of the root cause of a problem when it is confirmed that a CI (Configuration Item) is at fault.

Impact on the business + Urgency / Effect upon business deadlines = Priority

Category: Classification of a group of Incidents (Application, Hardware, etc.)

Escalation (Vertical Escalation): escalates up the management chain.

Referral (Horizontal Escalation): escalates to a different knowledge group. Routing.

Incident Life-Cycle

- Accept Service Event, Register and Consult the CMDB
- Classification
- Solve
- Closure

Reporting is VERY important.

- Daily reviews of individual Incident and Problem status against service levels
- Weekly management reviews
- Monthly management reviews
- Proactive service reports

# **Problem Management**

Objectives:

- Stabilizing IT services through:
  - Minimizing the consequences of incidents
  - Removal of the root causes of incidents
  - Prevention of incidents and problems
  - Prevent recurrence of Incidents related to errors
- Improving productive use of resources

Tasks:

- Problem Control
- Error Control (including raising RfCs Request for Change)
- Proactive Prevention
- Identifying Trends
- Management Information
- Posit Implementation Review (PIR)

Goal is to get from reactive or proactive. Stop problems from occurring / recurring.

Inputs:

- Incident details
- Configuration details
- Defined work-arounds

Outputs:

- Known Errors
- Requests for Change
- Updated Problem Records including work-arounds and/or solutions
- Response to Incident Management from Matching Management Information

#### Problem Control

- Identification
- Classification
- Assign Resources
- Investigation and Diagnosis
- Establish Known Error

Error Control

- Error Identification and Recording
- Error Assessment
- Recording Error / Resolution (Send out RfC)
- Error Closure

Known Error: An Incident or Problem for which the root cause is known and for which a temporary Work-around or a permanent alternative has been identified.

Proactive Problem Management:

- Trend Analysis
- Targeting Support Action
- Providing Information to the Organization

Known Errors resulting from Development should be made known to the Helpdesk.

Reporting is also key for Problem Management.

# **Change Management**

Objective: To *implement approved* changes *efficiently, cost-effectively* and with *minimal risk* to the existing and to the new IT infrastructure. Only approved changes made, risk and cost minimized.

Change Management Tasks:

- Filtering Changes
- Managing Change Process
- Managing Changes
- Chairing CAB and CAB/EC
- Review and Closure
- Management Information

Inputs:

- Requests for Change (RfC)
- CMDB
- Forward Schedule of Changes (FSC)

Outputs:

- Forward Schedule of Changes (FSC)
- Requests for Change (RFC)
- CAB minutes and actions
- Change management reports

Impact of change:

- Category 1
  - Little impact on current services. The Change Manager is entitled to authorize this RfC.
- Category 2
  - Clear impact on services. The RfC must be discussed in the Change Advisory Board. The Change Manager requests advice on authorization and planning.
- Category 3
  - Significant impact on the services and the business. Considerable manpower and/or resources needed. The RfC will have to be submitted to the board level (CAB/EC – Change Advisory Board / Executive Committee)

Priority Setting:

- Urgent
  - Change necessary now (otherwise severe business impact)
- High
  - Change needed as soon as possible (potentially damaging)
- Medium
  - Change will solve irritating errors or missing functionality (can be scheduled)
- Low
  - Change leads to minor improvements

A change backout plan must always be possible.

Change management always ends with a review of the change.

Change: The addition, modification, or removal of approved, supported or baselined hardware, network, software, application, environment, system, desktop build or associated documentation.

Request for Change: Form or screen, used to record details of a request for a change to any CI within an infrastructure or to procedures and items associated with the infrastructure.

Forward Schedule of Changes (FSC): Schedule that contains details of all the Changes approved for implementation and their proposed implementation dates.

**Change Management Process** 

- 1. Request for a Change
- 2. Registration and Classification
- 3. Monitoring and Planning
- 4. Approve
- 5. Build & Test
- 6. Authorize Implementation
- 7. Implementation
- 8. Evaluate

## **Release Management**

Objectives:

- Safeguard all software and related items
- Ensure that only tested / correct version of authorized software are in use
- Ensure that only tested / correct version of authorized hardware are in use
- Right software, right time, right place
- Right hardware, right time, right place

Tasks:

- Define the release policies
- Control of the Definitive Software Library (DSL)
- Control of the Definitive Hardware Storage (DHS)
- Distribute Software and Associated CIs
- Carry out S/W audits (using CMDB)
- Manage the software releases
- Oversee build of the software releases

Releases are done under the control of Change Management.

DSL : Definitive Software Library. Reliable versions of software in a single logical location. However, software may be physically stored at different locations.

Release Policy:

- Release Unit
- Full / Package / Delta Releases
- Numbering
- Frequency
- Emergency Change

Version Control:

- Development
- Testing
- Live
- Archive

Process:

- Software Control and Distribution (operational)
- Change Management (control)

• Configuration Management (control and administration)

Only process which creates its own policy.

# Availability Management

Objectives:

- To predict, plan for and manage the availability of services by ensuring that:
  - All services are underpinned by sufficient, reliable and properly maintained CIs
  - Where CIs are not supported internally there are appropriate contractual agreements with third party suppliers
  - Changes are proposed to prevent future loss of service availability
- Only then can IT organizations be certain of delivering the levels of availability agreed with customers in SLAs.

Aspects of Availability:

- Reliability
- Maintainability: Maintenance you do yourself, as a company
- Resilience: Redundancy
- Serviceability: Maintenance done by someone else

Availability Information is stored in an Availability Database (ADB). This information is used to create the Availability Plan. SLAs provide an input to this process.

Unavailability Lifecycle

MTTR: Mean Time to Repair (Downtime) – Time period that elapses between the detection of an Incident and it's Restoration. Includes: Incident, Detection, Diagnosis, Repair, Recovery, Restoration.

MTBF: Mean Time Between Failures (Uptime) – Time period that elapses between Restoration and a new Incident.

MTBSI: Mean Time Between System Incidents – Time period that elapses between two incidents. MTTR + MTBF.

"An IT service is *not available* to a customer if the functions that customer requires at that particular *location* cannot be used although the *agreed conditions* under which the IT service is supplied are being met"

Simplistic Availability Calculation:

Agreed Service Hours – Downtime		100
	Х	
Agreed Service Hours		1

# **IT Service Continuity Management**

Why plan?

- Increases Business dependency on IT
- Reduced cost and time of recovery
- Cost to customer relationship
- Survival

Many businesses fail within a year of suffering a major IT disaster.

Business Impact Analysis:

Risk Analysis:

- Value of Assets
- Threats
- Vulnerabilities

Risk Management:

- Countermeasures
- Planning for potential disasters
- Managing a disaster

Risk Analysis: Based on the CCTA Computer Risk Analysis and Management Methodology (CRAMM)

Options:

- 1. Do nothing
- 2. Manual workarounds
- 3. Reciprocal arrangements
- 4. Gradual Recovery (cold standby)
- 5. Intermediate Recovery (warm standby)
- 6. Immediate Recovery (hot standby)

Cold start = accommodation. Environmental controls; power and communications

Hot start = cold start + computing equipment and software

7 Sections of the Plan:

- 1. Administration
- 2. The IT Infrastructure
- 3. IT Infrastructure management & Operating procedures
- 4. Personnel
- 5. Security
- 6. Contingency site
- 7. Return to normal

Test and Review:

- Initially then every 6 to 12 months and after each disaster
- Test it under realistic circumstances
- Move / protect any live services first
- Review and change the plan
- All changes made via the CAB Change Advisory Board

Contingency Plan:

- Assists in fast, controlled recovery
- Must be given wide but controlled access
- Contents (incl. Admin, Infrastructure, People, Return to normal)
- Options (incl. Cold & Hot Start)
- Must be tested regularly without impacting the live service

# **Capacity Management**

Objective:

To determine the *right, cost justifiable, capacity* of IT resources such that the Service Levels agreed with the business are achieved at the *right time*.

Objectives:

- Demand Management
  - o Business Capacity Management
- Workload Management
  - Service Capacity Management
- Resource Management
  - Resource Capacity Management

While doing the above, also need to do:

- Performance Management
  - Internal and External Financial Data
  - o Usage Data
  - SLM Data / Response Times

CDB – Capacity Data Base – Contains all Metrics, etc. Used to create a Capacity Management Plan. Performance Management Data populates the CDB.

Essentials:

- From Customer Demands to Resources
- Demand Management
- Workload Management
- Performance Management
- Capacity Planning
- Defining Thresholds and Monitoring

Application Sizing: To estimate the resource requirements to support a proposed application change to ensure that it meets its required service levels.

#### Modeling:

- Trend Analysis
- Analytical Modeling
- Simulation Modeling
- Baseline Models
- Used to Answer the "What If... " questions
  Data for Modeling comes from the CDB

# **Financial Management**

Objectives:

To provide information about and control over the costs of delivering IT services that support customers business needs.

Costing is a must!

Input cost units recommended by ITIL:

- Equipment Cost Units (ECU)
- Organization Cost Units (OCU)
- Transfer Cost Units (TCU)
- Accommodation Cost Units (ACU)
- Software Cost Units (SCU)

Equipment = hardware Organization = staff Transfer = costs which IT incurs acting as an agent for the customer, they do not appear as a cost against the IT department's budget Accommodation = buildings Software = software

Different Cost Types:

- Fixed unaffected by the level of usage
- Variable varying according to the level of usage
- Direct usage specific to one service
- Indirect or Overhead usage not specific to one service
- Capital not diminished by usage
- Revenue or running diminish with usage

Charging Objectives:

- Recover from customers the full costs of the IT services provided
- Ensure that customers are aware of the costs they impose on IT
- Ensure that providers have an incentive to deliver and agreed quality and quantity of economic and effective services

Charging and Pricing Options:

Charging:

- No Charging IT treated as support center
- Notional Charging IT treated as cost center
- Actual Charging

Pricing:

- Recover of Costs IT treated as a service center
- Cost Price Plus IT treated as a profit center
- Market Prices IT treated as a profit center

Support and Cost centers used "soft charging" in which no money changes hands; service and profit centers use "hard costing" in which money is transferred between bank accounts

Profit centers focus on the value of the IT service to the customer

Good Financial Management minimizes the risks in decision making

3 Main Processes:

Budgeting: The process of predicting and controlling the spending of money within the enterprise and consists of periodic negotiation cycle to set budgets (usually annual) and the day-to-day monitoring of the current budgets. Key influence on strategic and tactical plans.

IT Accounting: The set of processes that enable the IT organization to fully account for the way its money is spent (particularly the ability to identify costs by customer, by service, by activity).

Charging: The set of processes required to bill a customer for the services applied to them. To achieve this requires sound IT Accounting, to a level of detail determined by the requirements of the analysis, billing, and reporting procedures.

### **Service Level Management**

Balance between the Demand for IT services and the Supply of IT services by knowing the requirements of the business and knowing the capabilities of IT.

Objectives:

- Business-like relationship between customer and supplier
- Improved specification and understanding of service requirements
- Greater flexibility and responsiveness in service provision
- Balance customer demands and cost of services provision
- Measurable service levels
- Quality improvement (continuous review)
- Objective conflict resolution

#### Tasks:

- Service Catalog
- Service Level Requirements
- Service Level Agreement
- Operational Level Agreements (OLA) and Contracts
- Service Specsheet
- Service Quality Plan
- Monitor, Review and Report
- Service Improvement Programs
- Customer Relationship Management

Minimum Requirements for an Agreement:

- Period
- Service Description
- Throughput
- Availability
- Response Times
- Signature

Other Possible Clauses:

- Contingency arrangements
- Review procedures
- Change procedures
- Support services
- Customer responsibilities
- Housekeeping
- Inputs and Outputs
- Changes

Ideally contracts are based on targets in the SLA

SLAs must be monitored regularly and reviewed regularly

- Monitor to see if service is being delivered to specification
- Review to see if service specification is still appropriate