ITIL – Service Operation
Introduction

• Name
• Professional Experience
• Expectations from this course
• Exposure to ITIL?
Guidelines

- Participants are requested to be on time
- Follow the break timings given by the trainer and adhere to the schedule.
- Stationary for the training will be made available (scribbling pad and pen).
- Please keep your cell phones on Silent mode or switched off (if possible).
- Please do not open your laptops during training
- Training Facility details to be shared by the trainer
Course Objective

• Familiarize Audience with:
  • Service operations,
  • the principles,
  • processes,
  • activities and functions of management
  • operation of ICT infrastructures.

• Use the knowledge to:
  • keep more efficient control of their operations
  • increase the quality of IT Service Management.
Target Audience

• You are a CIO, CTO, manager, team leader, designer, architect, planner, IT consultant, IT audit manager, IT security manager or ITSM trainer or a member of the supervisory staff.

• Your role involves dealing with the operational activities of services and managing, coordinating or integrating these within the Service Lifecycle.

Prerequisites

• The certificate is a follow-on after gaining the ITIL Foundation in Service Management (or V2 in combination with Bridge). You followed your training with an EXIN-accredited trainer.
Exam Details

• Number of questions: 8
• Pass mark: 28/40 or 70%.
• Execution: online or paper-based exam by EXIN-accredited trainer.
• Open book: No
• Level of qualification: Intermediate
ITIL – Service Operation

D A Y 1

• Introduction to ITIL
• What are Services?
• What is Service Management?
• Functions and Processes across Lifecycle
• Service Operation Fundamentals
• Service Operation Principles
• Case Study
• Summary Day 1
DAY 2

• Service Operation Processes
  • Event Management
  • Incident Management
  • Problem Management

• Case Study

• Summary Day 1
DAY 3

- Service Operation Processes
  - Access Management
  - Request Fulfillment
  - Common Service Operation activities

- Case Study

- Summary Day 3
ITIL – Service Operation

DAY 4

• Organizing for Service Operation
• Technology considerations
• Implementing Service Operation
• Challenges, Critical Success Factors and risks
• Summary Day 4
• Exercises
DAY 1

• Introduction to ITIL

• What are Services?

• What is Service Management?

• Functions and Processes across Lifecycle

• Service Operation Fundamentals

• Case Study

• Summary Day 1
ITIL Qualification Roadmap

ITIL Master

ITIL Expert

Minimum 22 credits needed to achieve Diploma

Managing through the Lifecycle

15 Credits

ITIL Service Lifecycle Modules

3 SS
3 SD
3 ST
3 SO
3 CSI

ITIL Service Capability Modules

4 P&R
4 O&S
4 M&C
4 D&O

16 Credits

ITIL Foundation for Service Management

2 credits
What is ITIL?

• ITIL (Information Technology Infrastructure Library) was published between 1989 and 1995
• Public Framework
• Best Practices in IT
• Five core Books
• Latest Version is ITIL
• Focus on both business and customer Prospective
SERVICE

• What is a Service?

• Define in your own words the meaning of Service

• Difference between Service and Product
Definition and Meaning of Service

Service
Service is a means of delivering value to customers by facilitating outcomes customer want to achieve without the ownership of specific costs and risks.

Store What?
- Store Information
- Store Files
- Store equipment

Store How?
- Online Databases
- Portable Devices
- Secure Cabinets

Storage Service
Utility is what the customer receives and Warranty is how it is provided.
**Service Management** is a set of specialised organizational capabilities for providing values in the form of services.

**Organizational capabilities are** : Functions and processes for managing services throughout a lifecycle

The act of transforming **resources into services** is the core of Service Management.

The inputs to service management are **the resources and capabilities** that represent the assets of the service provider. The outputs are the services that provide value to the customers.
Service Assets

Resources
- Information
- Applications
- Infrastructure
- Financial Capital

Capabilities
- Management
- Organization
- Process
- Knowledge

People

© Crown copyright 2007. Reproduced under license from OGC.
A Process: Structured set of activities designed to accomplish a specific objective. A Process takes one or more defined inputs and turns them into defined outputs.

Function: A team or group of people and the tools they use to carry out one or more Processes or Activities. For example the Service Desk.

Role: A set of responsibilities, Activities and authorities granted to a person or team. A Role is defined in a Process. One person or team may have multiple Roles.
Process Model

Process Inputs

Process Control
- Process Owner
- Process Objectives
- Process Documentation
- Process Feedback

Process
- Process Activities
- Process Metrics
- Process Roles
- Process Procedures
- Process Work Instruction
- Process Improvement

Process Enablers
- Process Resources
- Process Capabilities

Triggers

Process Outputs

Including process reports & reviews

Front Metrics Technologies

www.frontmetrics.com
### RACI Model

#### RACI Definitions

<table>
<thead>
<tr>
<th></th>
<th>Who is Responsible</th>
<th>The person who is <strong>assigned</strong> to do the work</th>
</tr>
</thead>
<tbody>
<tr>
<td>R</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th></th>
<th>Who is Accountable</th>
<th>The person who makes the <strong>final decision</strong> and has the <strong>ultimate ownership</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>A</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th></th>
<th>Who is Consulted</th>
<th>The person who must be consulted <strong>before</strong> a decision or action is taken</th>
</tr>
</thead>
<tbody>
<tr>
<td>C</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th></th>
<th>Who is Informed</th>
<th>The person who must be informed that a decision or action <strong>has</strong> been taken</th>
</tr>
</thead>
<tbody>
<tr>
<td>I</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

© Crown copyright 2007. Reproduced under license from OGC.
RACI Example

<table>
<thead>
<tr>
<th></th>
<th>Release Manager</th>
<th>Project Manager</th>
<th>Program Manager</th>
<th>Developer</th>
</tr>
</thead>
<tbody>
<tr>
<td>Plan product</td>
<td>I</td>
<td>A</td>
<td>R</td>
<td>C</td>
</tr>
<tr>
<td>Develop product</td>
<td>I</td>
<td>I</td>
<td>A</td>
<td>R</td>
</tr>
<tr>
<td>Release product</td>
<td>R</td>
<td>A</td>
<td>I</td>
<td>I</td>
</tr>
</tbody>
</table>
Key Roles In Service Management

**Process Owner**: Accountable for the overall process performance

**Service Owner**: Accountable for a specific service within an organization regardless of where the underpinning technology components, processes or professional capabilities reside.

Responsibility of owners is to:

1. be accountable for the final outcomes (End-to-end accountability)
2. identify areas of improvements and recommend appropriate changes
3. guide process and service improvement initiatives
ITIL Service Lifecycle
Goal of Service Operation

• To ensure achieving efficacies in service support and delivery
• Responsible for ‘business-as-usual’ activities
• To have an observant view on the deliveries and service quality threats
• To carry out the activities and processes required to deliver and manage services at agreed levels to:
  - business users
  - customers
  - the ongoing management of the technology that is used to deliver and support services
Scope of Service Operation

- The services themselves
- Service Management processes
- Technology
- People
Service Operation

Each stage in the ITIL Service Lifecycle provides value to Business:

• Service value is modeled in Service Strategy
• The cost of the service is designed, predicted and validated in Service Design Service Transition
• Measures for optimization are identified in Continual service Improvement
• The operation of service is where these plans, designs and optimizations are executed and measured. From a customer viewpoint, Service Operation is where actual value is seen.
Service Operation Principles

- Stability versus responsiveness

An organization here is out of balance and is in danger of ignoring changing business requirements.

An organization here is quite balanced, but may tend to overspend on change.

Extreme Focus on Stability

Extreme Focus on Responsiveness

Front Metrics Technologies

www.frontmetrics.com
Service Operation Principles

• Balancing Quality of service versus cost of service
Service Operation Principles

• Balancing Internal IT view versus external business view
Service Operation Processes

Five Processes covered in Service operation:

• Event Management
• Incident Management
• Request Fulfillment
• Problem Management
• Access Management
Service Operation Function

Functions Covered in Service operation:

• Service Desk
• Technical Management
• IT Operations Management
• Application Management
DAY 2

Service Operation Processes

• Event Management
• Incident Management
• Problem Management

• Case Study

• Summary Day 1
Event Management

**Event**: An event can be defined as any detectable or discernible 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 services.

**Goal**: The ability to detect events, make sense of them and determine the appropriate control action is provided by Event Management. Event Management is therefore the basis for Operational Monitoring and Control.
Event Management

Scope

- Event Management can be applied to any aspect of Service Management that needs to be controlled and which can be automated. These include:
  - Configuration Items
  - Environmental conditions (e.g. fire and smoke detection)
  - Software license monitoring for usage to ensure optimum/legal license utilization and allocation
  - Security (e.g. intrusion detection)
  - Normal activity (e.g. tracking the use of an application or the performance of a server).
Event Management

Difference between Monitoring and Event Management?

- Event Management is focused on generating and detecting meaningful notifications about the status of the IT Infrastructure and services.

- Monitoring is broader than Event Management. For example, monitoring tools will check the status of a device to ensure that it is operating within acceptable limits, even if that device is not generating events.
Event Management

Value to Business

• Early detection of incidents

• Removing the need for expensive and resource intensive real-time monitoring, while reducing downtime

• Improvement in Process performance by integration into other Service management processes

• Provides basis for Automated operations, thus increasing efficiency
Event Management

Basic Concepts

• Events that signify regular operation
  • notification that a scheduled workload has completed
  • an e-mail has reached its intended recipient.

• Events that signify an exception
  • a user attempts to log on to an application with the incorrect password
  • a device’s CPU is above the acceptable utilization rate

• Events that signify unusual, but not exceptional, operation.
  • A server’s memory utilization reaches within 5% of its highest acceptable performance level
  • The completion time of a transaction is 10% longer than normal
Event Management

Basic Concepts

• Events that signify regular operation
  • notification that a scheduled workload has completed
  • a user has logged in to use an application

• Events that signify an exception
  • a user attempts to log on to an application with the incorrect password
  • a device’s CPU is above the acceptable utilization rate

• Events that signify unusual, but not exceptional, operation.
  • A server’s memory utilization reaches within 5% of its highest acceptable performance level
  • The completion time of a transaction is 10% longer than normal
Event Management Process

1. Event
2. Event Notification Generated
3. Event Detected
4. Event Filtered
5. Significance?
   - Informational
   - Exception
5a. Warning
   - Event Correlation
   - Trigger
Continued on next page
Information Management

• SNMP Messages with Technical information about status of IT components
• Management information Bases (MIB) for IT Devices
• Vendor’s monitoring tools agent software
• Correlation engine with detailed rules to determine significance and appropriate response to events
• Event Record type
  • No Standard Event Record type for all Events
  • Standard data required for usually all events:
    • Device
    • Component
    • Type of failure
    • Date/time
    • Parameters in exception
    • Value
Event Management

Metrics

- Number and percentage of events:
  - that required human intervention and whether this was performed
  - resulted in incidents or changes
  - caused by existing problems or Known Errors
  - repeated or duplicated events
  - indicating performance issues
  - indicating potential availability issues
  - per platform or application
  - compared with the number of incidents

- Number of events by category
- Number of events by significance
Event Management

Challenges

• Obtain funding for the necessary tools and effort needed to install and exploit the benefits of the tools.
• Setting the correct level of filtering
• Rolling out of the necessary monitoring agents across the entire IT infrastructure may be a difficult and time consuming activity
• Acquiring the necessary skills can be time consuming and costly
Event Management

Critical Success Factors

• One of the most important CSFs is achieving the correct level of filtering.
• Three keys to the correct level of filtering:
  • Integrate Event Management into all Service Management processes.
  • Design new services with Event Management in mind.
  • Trial and error.
• Proper planning is needed for the rollout of the monitoring agent software.

Front Metrics Technologies
www.frontmetrics.com
Event Management

Designing for Event Management

- Monitoring Mechanism to be decided during Availability and Capacity Stage (SD)
- Instrumentation
- Error Messaging for all components
- Event detection and Alert mechanism
- Identification of Threshold
Incident Management
Incident Management

• **Incident**: An unplanned interruption to an IT service or reduction in the quality of an IT service.

• Failure of a configuration item that has not yet impacted service is also an incident

• **Incident Management** is the process for dealing with all incidents

• Incidents can be reported by:
  
  • questions or queries reported by the users
  
  • by technical staff
  
  • automatically detected and reported by event monitoring tools
Incident Management

Purpose/Goal

• Restore normal service operation as quickly as possible
• Minimize the adverse impact on business operations
• Ensuring that the best possible levels of service quality and availability are maintained
Incident Management

SCOPE

• Any event which disrupts, or which could disrupt, a service
• All events are not events E.g informational events
• Service requests are also do not represent disruption
Incident Management

Value to Business

The value of Incident Management includes the ability to:

• detect and resolve incidents, which results in lower downtime to the business

• align IT activity to real-time business priorities

• identify potential improvements to services

• identify additional service or training requirements
The value of Incident Management includes the ability to:

- Timescales – Resolution with SLA
- Incident Models E.g security related incidents
- Major Incidents – Shorter timescale and greater urgency
Incident Management (continued)
Incident Management

Process Activities, Methods And Techniques:

- Incident identification
- Incident logging
- Incident categorization
- Incident prioritization
- Initial diagnosis
- Incident escalation
- Investigation and Diagnosis
- Resolution and Recovery
- Incident Closure
Incident Management

Triggers, Input And Output:

1. Problem Management
2. Configuration Management
3. Change Management
4. Capacity Management
5. Availability Management
6. SLM
Incident Management

Information Management:
Most information used in Incident Management comes from the following sources:

- Average cost per incident
- Number of incidents reopened and as a percentage of the total
- Number and percentage of incidents incorrectly assigned and Categorized
- Percentage of Incidents closed by the Service Desk without reference to other levels of support (often referred to as ‘first point of contact’)
- Number and percentage of incidents processed per Service Desk agent
- Number and percentage of incidents resolved remotely, without the need for a visit
- Number of incidents handled by each Incident Model
- Breakdown of incidents by time of day, to help pinpoint peaks and ensure matching of resources.

Front Metrics Technologies  www.frontmetrics.com
Incident Management

Challenges:

- The ability to detect incidents as early as possible
- Convincing all staff that all incidents must be logged
- Encouraging the use of self-help web-based capabilities
- Availability of information about problems and Known Errors
- Integration into the CMS to determine relationships between CIs and to refer to the history of CIs
- Integration into the SLM process
Incident Management

Critical Success factors:

- The ability to detect incidents as early as possible
- Convincing all staff that all incidents must be logged
- Encouraging the use of self-help web-based capabilities
- Availability of information about problems and Known Errors
- Integration into the CMS to determine relationships between CIs and to refer to the history of CIs
- Integration into the SLM process
Problem Management
Problem Management

‘Problem’ is the unknown cause of one or more incidents.

Problem Management is the process responsible for managing the lifecycle of all problems.

Purpose/Goal

To prevent problems and resulting incidents from happening, to eliminate recurring incidents and to minimize the impact of incidents that cannot be prevented.
Problem Management

Scope

• Problem Management includes the activities required to diagnose the root cause of incidents and to determine the resolution to those problems.

• Ensuring that the resolution is implemented through the appropriate control procedures, especially Change Management and Release Management.

• Maintain information about problems and the appropriate workarounds and resolutions.

• Incident and Problem Management are separate processes, they are closely related and will typically use the same tools, and may use similar categorization, impact and priority coding systems.
Problem Management

Scope

- Activities required to diagnose the root cause of incidents
- Determination of the resolution to those problems
- Assurance of implementation of resolution through the appropriate control procedures
- Maintenance of information about problems and the appropriate workarounds and resolutions
Problem Management

Value to Business

• Problem Management works together with Incident Management and Change Management to ensure that IT service availability and quality are increased.

• Information about the incident resolution is recorded. Over time, this information is used to speed up the resolution time and identify permanent solutions.

• This results in less downtime and less disruption to business critical systems.
Problem Management

Basic Concepts

Problem Models

- Many problems will be unique and will require handling in an individual way
- Some incidents may recur because of dormant or underlying problems
- Creating a Known Error Record in the Known Error Database to ensure quicker diagnosis, the creation of a Problem Model for handling such problems
Problem Management

Process activities, methods and techniques

Problem Management consists of two major processes:

Reactive Problem Management, which is generally executed as part of Service Operation – and is therefore covered in this publication

Proactive Problem Management which is initiated in Service Operation, but generally driven as part of Continual Service Improvement
Problem Management

Problem Management Process Flow

Continued on next page..
Problem Management

Problem Management Process Flow

Create Known Error Record

Known Error Database

Change Management

Change Needed?

Resolution

Closure

Major Problem?

Major Problem Review

End
Problem Management

Triggers, input and output/ interprocess interfaces

Key interfaces between problem management and other processes include:

• **Service Transition**
  - Change Management
  - Configuration Management
  - Release and Deployment Management

• **Service Design**
  - Availability Management
  - Capacity Management
  - IT Service Continuity

• **Continual Service Improvement**
  - Service Level Management

• **Service Strategy**
  - Financial Management
Problem Management
METRICS used to judge the effectiveness and efficiency of the Problem Management process:

- The total number of problems recorded in the period
- The percentage of problems resolved within SLA targets
- The number and percentage of problems that exceeded their target resolution times
- The backlog of outstanding problems and the trend
- The average cost of handling a problem
- The number of major problems
- The percentage of Major Problem Reviews successfully performed
- The number of Known Errors added to the KEDB
- The percentage accuracy of the KEDB (from audits of the database)
- The percentage of Major Problem Reviews completed successfully and on time.
Problem Management

Challenges, Critical Success Factors and Risks

A major dependency for Problem Management is the establishment of an effective Incident Management process and tools.

This implies:

- Linking Incident and Problem Management tools
- The ability to relate Incident and Problem Records
- The second- and third-line staff should have a good working relationship with staff on the first line
- Making sure that business impact is well understood by all staff working on problem resolution

Front Metrics Technologies

www.frontmetrics.com
Service Operation Processes

• Access Management
• Request Fulfillment
• Common Service Operation activities

• Case Study

• Summary Day 3
Access Management
Access Management is the process of granting authorized users the right to use a service, while preventing access to non-authorized users.

Purpose/Goal

Access Management provides the right for users to be able to use a service or group of services. It is therefore the execution of policies and actions defined in Security and Availability Management.
Access Management

**Scope** is the process of granting authorized users the right to use a service, while preventing access to non-authorized users.

**Purpose/Goal**

Access Management provides the right for users to be able to use a service or group of services. It is therefore the execution of policies and actions defined in Security and Availability Management.
Access Management

Value to Business

• Controlled access to services ensures the confidentiality of its information
• Employees have the right level of access to execute their jobs effectively
• There is less likelihood of errors for unskilled user (e.g. production control systems)
• The ability to audit the use of services and to trace the abuse of services
• The ability to revoke access rights when needed
• May be needed for regulatory compliance
Access Management

Process activities, methods and techniques

Access (or restriction) can be requested using one of any number of mechanisms, including:

• A standard request generated by the Human Resource system. This is generally done whenever a person is hired, promoted, transferred or when they leave the company
• A Request for Change
• A Service Request submitted via the Request Fulfilment system
• By executing a pre-authorized script or option
Access Management

Process activities, methods and techniques

Access (or restriction) can be requested using one of any number of mechanisms, including:

• A standard request generated by the Human Resource system. This is generally done whenever a person is hired, promoted, transferred or when they leave the company
• A Request for Change
• A Service Request submitted via the Request Fulfilment system
• By executing a pre-authorized script or option
Access Management

Process activities, methods and techniques

Verification

Access Management needs to verify every request for access to an IT service from two perspectives:

• That the user requesting access is who they say they are
• That they have a legitimate requirement for that service.
Access Management

Process activities, methods and techniques

Providing Rights

Access Management:

- does not decide who has access to which IT services
- executes the policies and regulations defined during Service Strategy and Service Design
Process activities, methods and techniques

Monitoring identity status

As users work in the organization, their roles change and so also do their needs to access services

Examples of changes include:

- Job changes.
- Promotions or demotions.
- Transfers.
- Resignation or death.
- Retirement.
- Disciplinary action.
- Dismissals.
Access Management

Process activities, methods and techniques

Logging and tracking access

• Access Management should not only respond to requests. It is also responsible for ensuring that the rights that they have provided are being properly used.

• Access Monitoring and Control must be included in the monitoring activities of all Technical and Application Management functions and all Service Operation processes.

• Exceptions should be handled by Incident Management, possibly using Incident Models specifically designed to deal with abuse of access rights.

• Information Security Management plays a vital role in detecting unauthorized access and comparing it with the rights that were provided by Access Management.

• Access Management may also be required to provide a record of access for specific Services during forensic investigations.
Access Management

Process activities, methods and techniques

Removing access is usually done in the following circumstances:

• Death
• Resignation
• Dismissal
• When the user has changed roles and no longer requires access to the service
• Transfer or travel to an area where different regional access applies

Situations in which access should be restricted include:

• When the user has changed roles or been demoted
• No longer requires the same level of access
• When the user is under investigation, but still requires access to basic services, e.g., e-mail.
• When a user is away from the organization on temporary assignment and will not require access to that service for some time.
Access Management

Triggers, input and output/interprocess interfaces

Access Management is triggered by a request for a user or users to access a service or group of services. This could originate from:

- RFC
- Service Request
- Request from Human resource Management
- Request from Manager of Department
Access Management

Information Management

- The identity of a user is the information about them that distinguishes them as an individual and which verifies their status within the organization. Example
  - Name
  - Address
  - Contact details etc.

A user identity is provided to anyone with a legitimate requirement to access IT services or organizational information. Example

- Users, groups, roles and service groups
  - Standard Services for new users
  - Services as per the specialized role
  - Unique requirements
Access Management

**Metrics** that can be used to measure the efficiency and effectiveness of Access Management include:

- Number of requests for access (Service Request, RFC, etc.)
- Instances of access granted, by service, user, department, etc.
- Instances of access granted by department or individual granting rights
- Number of incidents requiring a reset of access rights
- Number of incidents caused by incorrect access settings.
Access Management

Challenges, Critical Success Factors and risks

• The ability to verify the identity of a user
• The ability to verify the identity of the approving person or body
• The ability to verify that a user qualifies for access to a specific service
• The ability to link multiple access rights to an individual user
• The ability to determine the status of the user at any time
• The ability to manage changes to a user’s access requirements
• The ability to restrict access rights to unauthorized users
• A database of all users and the rights that they have been granted.
Request Fulfillment
Request Fulfillment

Purpose/Goal

• Channel for users to request and receive standard services
• Pre-defined approval and qualification process
• 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
Request Fulfillment

- **Service Request** - Small changes - low risk, frequently occurring, low cost, etc.

- **Service Request Examples**:
  - a request to change a password
  - a request to install an additional software application onto a particular workstation
  - a request to relocate some items of desktop equipment
  - maybe just a question requesting information

- Service requests are better handled by a different process due to their Scale, frequency and Low risk.

- **Request Fulfillment** is the processes of dealing with Service Requests from the users

Front Metrics Technologies

www.frontmetrics.com
The process needed to fulfill a request varies depending upon exactly what is being requested.

**Note:**

However, there is a significant difference here:

- an incident is usually an unplanned event

- whereas a Service Request is usually something that can and should be planned!
Request Fulfillment

Value to Business

• Provide quick and effective access to standard services which business staff can use to improve their productivity or the quality of business services and products.
• Reduces the bureaucracy involved in requesting and receiving access to existing or new services thus also reducing the cost of providing these services.
• Centralizing fulfillment also increases the level of control over these services. This in turn can help reduce costs through centralized negotiation with suppliers, and can also help to reduce the cost of support.
Basic Concepts

- Many Service Requests will be frequently recurring, so a predefined process flow (a model) can be devised to include the stages needed to fulfill the request.
- The individuals or support groups involved, target timescales and escalation paths.
- Service Requests will usually be satisfied by implementing a Standard Change.
- The ownership of Service Requests resides with the Service Desk, which monitors, escalates, dispatches and often fulfils the user request.
Request Fulfillment

Process activities, methods and techniques

Menu selection
• Users are offered a ‘menu’-type selection via a web interface
• So that they can select and input details of Service Requests from a pre-defined list

Financial approval
• Most requests will have some form of financial implications, regardless of the type of commercial arrangements in place
• The cost of fulfilling the request must first be established
Request Fulfillment

Process activities, methods and techniques

Menu selection

• Users are offered a ‘menu’-type selection via a web interface

• So that they can select and input details of Service Requests from a pre-defined list

Financial approval

• Most requests will have some form of financial implications, regardless of the type of commercial arrangements in place

• The cost of fulfilling the request must first be established
Request Fulfillment

Process activities, methods and techniques

Other approval

In some cases further approval may be needed such as
- compliance-related or
- wider business approval

Fulfillment

- Fulfillment activity depends on the nature of the Service Request
- Simpler requests are completed by the Service Desk, acting as first-line support
- Others are forwarded to specialist groups and/or suppliers for fulfillment

Closure

- Once the Service Request is fulfilled, it is referred back to the Service Desk for closure checking
to ensure that the user is satisfied with the outcome
Request Fulfillment

Triggers, input and output/inter process interfaces

The primary interfaces with Request Fulfillment include:

• Service Desk/Incident Management

• Request Fulfillment, Release, Asset and Configuration Management
Request Fulfillment

Information Management

Request Fulfillment is dependent on information from the following sources:

- Service request
- Request for Change
- The Service Portfolio
- Security Policies
Request Fulfillment

METRICS needed to judge the effectiveness and efficiency of Request fulfillment will include the following:

- The total number of Service Requests (as a control measure)
- Breakdown of service requests at each stage (e.g. Logged, WIP, closed, etc.)
- The size of current backlog of outstanding Service Requests
- The mean elapsed time for handling each type of Service Request
- The number and percentage of Service Requests completed within agreed target times
- The average cost per type of Service Request
- Level of client satisfaction with the handling of Service Requests (as measured in some form of satisfaction survey).
Request Fulfillment

Challenges faced when introducing Request Fulfillment:

- Clearly defining and documenting the type of requests that will be handled within the Request Fulfillment process
- Defining the request that will go through the Service Desk and be handled as incidents or those that will need to go through formal Change Management
- Establishing self-help front-end capabilities that allow the users to interface successfully with the Request Fulfillment process.
Request Fulfillment

Critical Success factors

- Agreement of what services will be standardized and who is authorized to request them with the cost and variance in them
- Publication of the services to users as part of the Service Catalogue which should be easily accessible
- Definition of a standard fulfillment procedure for each of the requested services
- A single point of contact which can be used to request the service
- Self-service tools needed to provide a front-end interface to the users
Request Fulfillment

Risks

- Poorly defined scope, where people are unclear about exactly what the process is expected to handle
- Poorly designed or implemented user interfaces so that users have difficulty raising the requests that they need
- Badly designed or operated back-end fulfillment processes that are incapable of dealing with the
- Volume or nature of the requests being made
- Inadequate monitoring capabilities so that accurate metrics cannot be gathered
OPERATIONAL ACTIVITIES OF PROCESSES COVERED IN OTHER LIFECYCLE PHASES
Aspects of Change Management in which Service Operation staff is involved on a day-to-day basis include:

- Raising and submitting RFCs as needed to address Service Operation issues
- Participating in CAB or CAB/EC meetings to ensure that Service Operation risks, issues and views are taken into account
- Implementing changes as directed by Change Management where they involve Service Operation component or services
- Backing out changes as directed by Change Management where they involve Service Operation component or services
- Helping define and maintain change models relating to Service Operation components
- Receiving change schedules and ensuring that all Service Operation staff are made aware of and prepared for all relevant changes
- Using the Change Management process for standard, operational-type changes.
Aspects of Configuration Management in which Service Operation staff is involved on a day-to-day basis include:

• Informing Configuration Management of any discrepancies found between any CIs and the CMS
• Making any amendments necessary to correct any discrepancies, under the authority of Configuration Management, where they involve any Service Operation components/services
Configuration Management

Aspects of Configuration Management in which Service Operation staff is involved on a day-to-day basis include:

- Informing Configuration Management of any discrepancies found between any CIs and the CMS
- Making any amendments necessary to correct any discrepancies, under the authority of Configuration Management, where they involve any Service Operation components/services
Aspects of Release and Deployment Management in which Service Operation staff is involved on a day-to-day basis include:

• Actual implementation actions regarding the deployment of new releases, under the direction of Release and Deployment Management, where they relate to Service Operation components or services.

• Participation in the planning stages of major new releases to advise on Service Operation issues.

• The physical handling of CIs from/to the DML as required to fulfil their operational roles – while adhering to relevant Release and Deployment Management procedures.
Capacity Management

Capacity Management should operate at three levels:

- Business Capacity Management
- Service Capacity Management
- Component Capacity Management

Capacity Management activities that must be performed on a regular ongoing basis as part of Service Operation:

- Capacity and Performance Monitoring
- Handling capacity- or performance related incidents
- Capacity and performance trends
- Storage of Capacity Management data
- Demand Management
- Workload Management
- Modelling and applications sizing
- Capacity Planning
Availability Management

• During Service Design and Service Transition, IT services are designed for availability and recovery

• Service Operation is responsible for making the IT service available to the specified users at the required time and at the agreed levels

Three key opportunities for operational staff to be involved in Availability Improvement are:

• Review of maintenance activities

• Major problem reviews

• Involvement in specific initiatives
Availability Management

• During Service Design and Service Transition, IT services are designed for availability and recovery.

• Service Operation is responsible for making the IT service available to the specified users at the required time and at the agreed levels.

Three key opportunities for operational staff to be involved in Availability Improvement are:

• Review of maintenance activities
• Major problem reviews
• Involvement in specific initiatives
Knowledge Management

- Key repositories of Service Operation, which have been frequently mentioned elsewhere, are the **CMS** and the **KEDB**

- Key repositories must be widened out to include all of the Service Operation teams’ and departments’ documentation, such as operations manuals, procedures manuals, work instructions, etc
Financial Management for IT services

• Service Operation staff must participate in and support the overall IT budgeting and accounting system and may be actively involved in any charging system that may be in place.

• The Service Operation Manager must also be involved in regular, at least monthly, reviews of expenditure against budgets – as part of the ongoing IT budgeting and accounting process.

• Ensure that IT is involved in discussing all cost-saving measures and contribute to overall decisions.
IT service Continuity Management

Service Operation functions must be involved in the following areas:

• Risk assessment, using its knowledge of the infrastructure and techniques
• Execution of any Risk Management measures that are agreed
• Assistance in writing the actual recovery plans
• Participation in testing of the plans
• Ongoing maintenance of the plans
• Participation in training and awareness campaigns
• The Service Desk will play a key role in communicating with staff, customers and users during an actual disaster.
DAY 4

• Common Service Operation activities
• Organizing for Service Operation
• Technology considerations
• Implementing Service Operation
• Challenges, Critical Success Factors and risks

• Summary Day 4

• Exercises
Common Service Operation Activities
Common Service Operation Activities

Level 5: Strategic Contribution
- IT is measured in terms of its contribution to the business
- All services are measured by their ability to add value
- Technology is subordinate to the business function it enables
- Service Portfolio drives investment and performance targets
- Technology expertise is so entrenched in everyday operations it is viewed as a utility by the business

Level 4: Service Provision
- Services are quantified and initiatives aimed at delivering appropriate levels
- Service requirements and technology constraints drive procurement
- Service Design specifies performance requirements and operational norms
- Consolidated systems support multiple services
- All technology is mapped to services and is managed to service requirements
- Change Management covers both development and operations

Level 3: Technology Integration
- Critical services have been identified together with their technological dependencies
- Systems are integrated to provide required performance, availability and recovery for those services
- More focus on measuring performance across multiple devices and even platforms
- Virtual mapping of Configuration and Asset data with single Change Management for operations
- Consolidated Availability and Capacity Planning on some services
- Integrated Disaster Recovery Planning
- Systems are consolidated to save cost

Level 2: Technology Control
- Initiatives are aimed at achieving control and increasing the stability of the infrastructure
- It has identified most technology components and understands what each is used for
- Technical management focuses on achieving high performance of each component regardless of its function
- Availability of components is measured and reported
- Reactive Problem Management and inventory control are performed
- Change control is performed on “mission critical” components
- Point solutions are used to automate those processes that are in place, usually on a platform-by-platform basis

Level 1: Technology Driven
- It is driven by technology and most initiatives are aimed at trying to understand the infrastructure and deal with exceptions
- Technology management is performed by technical experts, and only they understand how to manage each device or platform
- Most teams are driven by incidents, and most improvements are aimed at making management easier – not to improve services
- Organizations entrench technology specializations and do not encourage interaction with other groups
- Management tools are aimed at managing single technologies, resulting in duplication
- Incident Management processes start being created
**MONITORING AND CONTROL**

**Monitoring** refers to the activity of observing a situation to detect changes that happen over time.

In the context of Service Operation, this implies the following:

- Using tools to monitor the status of key CIs and key operational activities
- Ensuring that specified conditions are met (or not met) and, if not, to raise an alert to the appropriate group
- Ensuring that the performance or utilization of a component or system is within a specified range
- To detect abnormal types or levels of activity in the infrastructure
- To detect unauthorized changes
- To ensure compliance with the organization’s policies
- To track outputs to the business and ensure that they meet quality and performance req
- To track any information that is used to measure KPI

Front Metrics Technologies  
www.frontmetrics.com
**MONITORING AND CONTROL**

**Reporting** refers to the analysis, production and distribution of the output of the monitoring activity.

In the context of Service Operation, this implies the following:

- Using tools to collate the output of monitoring information that can be disseminated to various groups, functions or processes
- Using tools to collate the output of monitoring information that can be disseminated to various groups, functions or processes
**Control** refers to the process of managing the utilization or behaviour of a device, system or service.

Note: Simply manipulating a device is not the same as controlling it. Control requires three conditions:

- The action must ensure that behaviour conforms to a defined standard or norm
- The conditions prompting the action must be defined, understood and confirmed
- The action must be defined, approved and appropriate for these conditions.

In the context of Service Operation, control implies the following:

- Using tools to define what conditions represent normal or abnormal operations
- Regulate performance of devices, systems or services
- Measure availability
- Initiate corrective action, which could be automated or manual
The most common model for defining control is the Monitor Control Loop.

Typically there are two types of Monitor Control Loops:

- **Open Loop Systems** are designed to perform a specific activity regardless of environmental conditions.
- **Closed Loop Systems** monitor an environment and respond to changes in that environment.
Monitor Control Loops

Complex Monitor Control Loop
The ITSM Monitor Control Loop

Monitoring and Control can only effectively be deployed when the service is operational.

Quality of the entire set of IT Service Management processes depends on how they are monitored and controlled in Service Operation.

The implications of this are as follows:
- Service Operation staff are not the only people with an interest in what is monitored and how they are controlled.
- While Service Operation is responsible for monitoring and control of services and components, they are acting as stewards of a very important part of the set of ITSM Monitoring and Control loops.
- If Service Operation staff define and execute Monitoring and Control procedures in isolation, none of the Service Management processes or functions will be fully effective.
Monitor Control Loops

Internal and External Monitoring and Control:

• Internal Monitoring and Control
  • Monitoring and control focuses on activities that are self-contained within that team or department
  • For example, the Service Desk Manager will monitor the volume of calls

• External Monitoring and Control
  • Each team or department will also be controlling items and activities on behalf of other groups, processes or functions.
  • For example, the Server Management team will monitor the CPU performance on key servers and perform workload balancing so that a critical application is able to stay within performance thresholds set by Application Management.
Monitor Control Loops

Types of Monitoring:

Active Monitoring
• refers to the ongoing ‘interrogation’ of a device or system to determine its status. resource intensive
• reserved to proactively monitor the availability of critical devices or systems;
• used as a diagnostic step when attempting to resolve an Incident or diagnose a problem

Passive Monitoring
• is more common and refers to generating and transmitting events to a ‘listening device’ or monitoring agent.
• depends on successful definition of events and instrumentation of the system being monitored
Monitor Control Loops

Types of Monitoring:

Reactive Monitoring
- is designed to request or trigger action following a certain type of event or failure
- For example, server performance degradation may trigger a reboot, or a system failure will generate an incident.

Proactive Monitoring
- is used to detect patterns of events which indicate that a system or service may be about to fail.
- used in more mature environments where these patterns have been detected previously
Monitor Control Loops

Types of Monitoring:

Continuous Measurement

• is focused on monitoring a system in real time to ensure that it complies with a performance norm
• for example, an application server is available for 99.9% of the agreed service hours.

Exception based Measurement Monitoring

• does not measure the real-time performance of a service or system, but detects and reports against exceptions
• For example, an event is generated if a transaction does not complete, or if a performance threshold is reached
Monitor Control Loops

Monitoring the Test Environment itself:

• A Test Environment consists of infrastructure, applications and processes that have to be managed and controlled just as any other environment

Monitoring items being tested:

• The results of testing have to be accurately tracked and checked
• Any monitoring tools that have been built into new or changed services have to be tested as well
Monitor Control Loops

Service Operation audits

Regular audits must be performed on the Service Operation processes and activities to ensure:

- They are being performed as intended
- There is no circumvention
- They are still fit for purpose, or to identify any required changes or improvement

Audit can be performed by:

- Service Operation Managers
- Organization’s internal IT audit team
- Third-party consultancy

Front Metrics Technologies

www.frontmetrics.com
Monitor Control Loops

Measurement, metrics and KPIs

• Measurement refers to any technique that is used to evaluate the extent, dimension or capacity of an item in relation to a standard or unit.

• Metrics refer to the quantitative, periodic assessment of a process, system or function, together with the procedures and tools that will be used to make these assessments and the procedures for interpreting them.

• A KPI refers to a specific, agreed level of performance that will be used to measure the effectiveness of an organization or process.
IT Operations

Console Management

Provide a central coordination point for:

• managing various classes of events
• detecting incidents
• managing routine operational activities
• reporting on the status or performance of technology components.

• Observation and monitoring of the IT Infrastructure can occur from a centralized console – to which all system events are routed.
Job Scheduling involves:

- defining and initiating job scheduling software packages to run batch and real-time work
- daily, weekly, monthly, annual and ad hoc schedules to meet business needs
- run-time logs have to be checked and any failures identified
- If failures do occur, then re-runs will have to be initiated

Workload Management techniques

- re-scheduling of work
- migration of workloads to alternative Platform/environment
- careful timing and ‘interleaving’ of jobs to gain maximum utilization of available resources
IT Operations

Backup

- Backup strategy
- Recovery point objectives
- Recovery time objectives

Restore may be needed in the case of:

- Corrupt data
- Lost data
- Disaster recovery/IT Service Continuity situation
- Historical data required for forensic investigation
Print and Output

Print (physical) and Output (electronic) facilities and services need to be formally managed because:

- They often represent the tangible output of a service
- Physical and electronic output often contains sensitive or confidential information.

Many organizations will have centralised bulk printing requirements which IT Operations must handle.
IT Operations

MAINFRAME MANAGEMENT

• Mainframe operating system maintenance and support
• Third-level support for any mainframe-related incidents/problems
• Writing job scripts
• System programming
• Interfacing to hardware (H/W) support
• Provision of information and assistance to Capacity Management to help achieve optimum throughput
IT Operations

SERVER MANAGEMENT AND SUPPORT

The procedures and activities which must be undertaken by the Server Team:

- Operating system support
- License management
- Third-level support
- Procurement advice
- System security
- Definition and management of virtual servers
- Capacity and Performance
- Ongoing maintenance
- Decommissioning and disposal of old server equipment.
Network Management

Their role will include the following activities:

- Initial planning and installation of new networks/network component
- Third-level support for all network related activities
- Maintenance and support of network operating system
- Monitoring of network traffic
- Reconfiguring or rerouting of traffic
- Network security
- Assigning and managing IP addresses, Domain Name Systems
- Managing Internet Service Providers
- Implementing, monitoring and maintaining Intrusion Detection Systems
- Updating Configuration Management
IT Operations

Storage and Archive

Many services require the storage of data for a specific time and also for that data to be available off-line.

A separate team or department may be needed to manage the organization’s data storage technology such as:

- Storage devices
- Network Attached Storage
- Storage Area Networks
- Direct Attached Storage
- Content Addressable Storage
Database Administration

• Database Administration must work closely with key Application Management teams
• Database administration being performed by each Application Management team for all the applications under its control
• A dedicated department, which manages all databases, regardless of type or application
• Several departments, each managing one type of database, regardless of what application they are part of.
Directory Services Management

A Directory Service is a specialized software application that manages information about the resources available on a network and which users have access to.

Its activities include:
- To ensure that new services are accessible and controlled when they are deployed
- Locating resources on a network
- Tracking the status of those resources
- Managing the rights of specific users or groups of users to access resources on a network
- Defining and maintaining naming conventions to be used for resources on a network
- Ensuring consistency of naming and access control
- Linking different Directory Services throughout the organization to form a distributed Directory Service
- Monitoring Events on the Directory Services
- Maintaining and updating the tools used to manage Directory Services
Desktop Support

Desktop support responsibilities will include:

- Desktop policies and procedures
- Designing and agreeing standard desktop images
- Desktop service maintenance including deployment of releases, upgrades, patches and hot-fixes
- Design and implementation of desktop archiving/rebuild policy
- Third-level support of desktop-related incidents
- Support for connectivity issues
- Configuration control and audit of all desktop equipment
Desktop Support

Desktop support responsibilities will include:

• Desktop policies and procedures
• Designing and agreeing standard desktop images
• Desktop service maintenance including deployment of releases, upgrades, patches and hot-fixes
• Design and implementation of desktop archiving/rebuild policy
• Third-level support of desktop-related incidents
• Support for connectivity issues
• Configuration control and audit of all desktop equipment
Middleware is software that connects or integrates software components across distributed or disparate applications and systems.

Functionality provided by middleware includes:

• Providing transfer mechanisms for data from various applications
• Sending work to another application or procedure for processing
• Transmitting data or information to other systems
• Releasing updated software modules across distributed environments
• Collation and distribution of system messages and instructions
• Managing queue sizes.
IT Operations

INTERNET/WEB MANAGEMENT

Responsibilities of Web Management team:

• Defining architectures for Internet and web services
• The specification of standards for development and management of web-based applications, content, websites and web pages
• Design, testing, implementation and maintenance of websites
• Maintenance of all web development and management applications
• Liaison and advice to web-content teams within the business
• Liaison with and supplier management of ISPs, hosts, third-party monitoring
• Third-level support for Internet-/web-related incidents
Facilities Management refers to the management of the physical environment of IT Operations, usually located in Data Centre's or computer rooms.

Main components of Facilities Management are as follows:

- Building Management
- Equipment Hosting
- Power Management
- Environmental Conditioning and Alert Systems
- Safety
- Physical Access Control
- Shipping and Receiving
- Contract Management
- Maintenance
IT Operations

Data Centre strategies

Data Centre operations are governed by strategic and design decisions for management and control and are executed by operators.

This requires a number of key factors to be put in place:

• Data Centre Automation
• Policy-based management
• Real time services
• Standardization of equipment
• SOAs
• Virtualization
IT Operations

Data Centre strategies

Data Centre operations are governed by strategic and design decisions for management and control and are executed by operators.

This requires a number of key factors to be put in place:

- Data Centre Automation
- Policy-based management
- Real time services
- Standardization of equipment
- SOAs
- Virtualization
Information Security Management has overall responsibility for setting policies, standards and procedures to ensure the protection of the organization’s assets, data, information and IT services.

It includes:

- Policing and reporting
- Technical assistance
- Operational security control
- Screening and vetting
- Screening and vetting
- Training and awareness
- Screening and vetting
IT Operations

IMPROVEMENT OF OPERATIONAL ACTIVITIES

This include some of the following activities:

• Automation of manual tasks
• Reviewing makeshift activities or procedures
• Operational Audits
• Using Incident and Problem Management
• Communication
• Education and training
Service Operation functions

• Service Desk
• Technical Management
• IT Operations Management
• IT Operations Control
• Facilities Management
• Application Management
DAY 4

• Organizing for Service Operation
• Technology considerations
• Implementing Service Operation
• Challenges, Critical Success Factors and risks

• Summary Day 4

• Exercises
Organizing for Service Operation
Service Operation functions

- Service Desk
- Technical Management
- IT Operations Management
- IT Operations Control
- Facilities Management
- Application Management
Service Desk

Service Desk is the primary point of contact for:

• users when there is a service disruption,
• service requests
• some categories of Request for Change

The exact nature, type, size and location of a Service Desk will vary, depending upon the type of business, number of users, geography, complexity of calls, scope of services and many other factors.
Service Desk

Justification and role of the Service Desk

- Improved customer service, perception and satisfaction
- Increased accessibility through a single point of contact, communication and information
- Better-quality and faster turnaround of customer or user requests
- Improved teamwork and communication
- Enhanced focus and a proactive approach to service provision
- A reduced negative business impact
- Better-managed infrastructure and control
- Improved usage of IT Support resources and increased productivity of business personnel
- More meaningful management information for decision support
Service Desk

Service Desk objectives

• Logging all relevant incident/service request details, allocating categorization and prioritization codes
• Providing first-line investigation and diagnosis
• Resolving those incidents/service requests they are able
• Escalating incidents/service requests that they cannot resolve within agreed timescales
• Keeping users informed of progress
• Closing all resolved incidents, requests and other calls
• Conducting customer/user satisfaction callbacks/ surveys as agreed
• Communication with users – keeping them informed of incident progress, notifying them of impending changes or agreed outages
• Updating the CMS under the direction and approval of Configuration Management if so agreed
Service Desk organizational structure

There are many ways of structuring Service Desks and locating them – and the correct solution will vary for different organizations

- Local Service Desk
Service Operation functions

Centralized Service Desk
Service Desk

Virtual Service Desk

© Crown copyright 2007. Reproduced under license from OGC.

Front Metrics Technologies

www.frontmetrics.com
Follow the Sun
Service Desk

Follow the Sun

• Global or international organizations may wish to combine two or more of their geographically dispersed Service Desks to provide a 24-hour follow-the-sun service.
• 24-hour coverage at relatively low cost. No desk has to work more than a single shift.

Specialized Service Desk groups

• For some organizations it might be beneficial to create ‘specialist groups’ within the overall Service Desk structure.
• Incidents relating to a particular IT service can be routed directly.
• This can allow faster resolution of these incidents.
Service Desk

Building A Single Point Of Contact

Regardless of the combination of options chosen to fulfill an organization’s overall Service Desk structure, individual users should be in no doubt about whom to contact if they need assistance

- single telephone number
- well publicized – as well as a single e-mail address
- single web Service Desk contact page should be provided
- Prominently placing these details on Service Desk Internet/intranet sites
Service Desk staffing

Staffing levels
• correct number of staff are available at any given time to match the demand

Skill levels
• An organization must decide on the level and range of skills it requires of its Service Desk staff

Training
• It is vital that all Service Desk staff are adequately trained before they are called upon

Staff retention
• Any significant loss of staff can be disruptive and lead to inconsistency of service

Super Users
• it's useful to appoint or designate a number of ‘Super Users’ throughout the user community, to act as liaison points with IT in general and the Service Desk in particular
Service Desk metrics

It includes:

• The first-line resolution rate: the percentage of calls resolved at first line,
• Average time to resolve an incident
• Average time to escalate an incident
• Average Service Desk cost of handling an incident
• Percentage of customer or user updates conducted within target times, as defined in SLA targets
• Average time to review and close a resolved call
• The number of calls broken down by time of day and day of week, combined with the average call-time metric, is critical in determining the number of staff required
Outsourcing the Service Desk

The decision to outsource is a strategic issue for senior managers – and is addressed in detail in the Service Strategy and Service Design publications.

Some of these safeguards are set out below:

• Common tools and processes
• SLA targets
• Good communications
• Ownership of data
Technical Management refers to the groups, departments or teams that provide technical expertise and overall management of the IT Infrastructure.

Technical Management plays a dual role:
- It is the custodian of technical knowledge and expertise related to managing the IT Infrastructure.
- It provides the actual resources to support the ITSM Lifecycle.

By performing these two roles, Technical Management is able to ensure that the organization has access to the right type and level of human resources to manage technology and, thus, to meet business objectives.
Technical Management objectives

The objectives of Technical Management are to help plan, implement and maintain a stable technical infrastructure to support the organization’s business processes through:

• Well designed and highly resilient, cost-effective technical topology
• The use of adequate technical skills to maintain the technical infrastructure in optimum condition
• Swift use of technical skills to speedily diagnose and resolve any technical failures that do occur.
Generic Technical Management Activities

- Identifying the knowledge and expertise required to manage and operate the IT Infrastructure
- Documentation of the skills that exist in the organization, as well as those skills that need to be developed
- Recruiting or contracting resources with skills that cannot be developed internally
- Procuring skills for specific activities where the required skills are not available internally
- Definition of standards used in the design of new architectures
- Availability and Capacity Management are dependent on Technical Management
- Assistance in assessing risk, identifying critical service and system dependencies
- Designing and performing tests for the functionality, performance and manageability of IT services etc
TECHNICAL MANAGEMENT

Technical management organization

One or more Technical Support teams or departments will be needed to provide technical management and support for the IT

Technical Design and Technical Maintenance and Support

Technical Management consists of:

- specialist technical architects and designers (who are primarily involved during Service Design)
- specialist maintenance and support staff (who are primarily involved during Service Operation)
Technical management Metrics

Metrics for Technical Management largely depends on the technology being used.

Some generic metrics includes:

- Measurement of agreed outputs
- Process metrics
- Technology performance
- Mean Time Between Failures of specified equipment
- Measurement of maintenance activity
- Training and skills development
Technical management Metrics

Metrics for Technical Management largely depends on the technology being used.

Some generic metrics includes:

- Measurement of agreed outputs
- Process metrics
- Technology performance
- Mean Time Between Failures of specified equipment
- Measurement of maintenance activity
- Training and skills development
In business, the term ‘Operations Management’ is used to mean the department, group or team of people responsible for performing the organization’s day-to-day operational activities.

Operations Management generally has the following characteristics:

- There is work to ensure that a device, system or process is actually running or working.
- This is where plans are turned into actions.
- The focus is on daily or shorter-term activities.
- These activities are executed by specialized technical staff.
- There is a focus on building repeatable, consistent actions.
- This is where the actual value of the organization is delivered and measured.
- There is a dependency on investment in equipment.
- The value generated, must exceed the cost of the investment and all other organizational overheads (such as management and marketing costs) if the business is to succeed.
IT Operations Management role

- Operations Control
  - Console Management
  - Job Scheduling
  - Backup and Restore
  - Print and Output management
  - Maintenance activities
- Facilities Management
IT OPERATIONS MANAGEMENT

IT Operations Management objectives

- The objectives of IT Operations Management include:
- Maintenance of the status quo to achieve stability of the organization’s day-to-day processes and activities
- Regular scrutiny and improvements to achieve improved service at reduced costs, while maintaining stability
- Swift application of operational skills to diagnose and resolve any IT operations failures that occur.
IT Operations Management metrics

- Successful completion of scheduled jobs
- Number of exceptions to scheduled activities and jobs
- Number of data or system restores required
- Equipment installation statistics, including number of items installed by type, successful installations
- Process metrics.
- Maintenance performed per schedule
- Number of maintenance windows exceeded
- Maintenance objectives achieved
- Metrics related to Facilities Management
IT Operations Management documentation

This list is a summary of some of the most important and does not include reports that are produced by IT Operations Management on behalf of other processes or functions.

- Standard Operating Procedures
- Operations Logs
- Shift Schedules and Reports
- Operations Schedule
Application Management is responsible for managing applications throughout their lifecycle.

The Application Management function is performed by any department, group or team involved in managing and supporting operational applications.

Application Management also plays an important role in the design, testing and improvement of applications that form part of IT services.
Application Management Role

Application Management will play a dual role:

• It is the custodian of technical knowledge and expertise related to managing applications.

• It provides the actual resources to support the ITSM Lifecycle.

• Providing guidance to IT Operations about how best to carry out the ongoing operational management of applications.

• The integration of the Application Management Lifecycle into the ITSM Lifecycle. This is discussed below.
Application Management Objective

• To support the organization’s business processes by helping to identify functional and manageability requirements for application software.

• Assist in the design and deployment of those applications and the ongoing support and improvement of those applications.
Application Management principles

• Build or buy?
  Application Management will assist in this decision during Service Design

• Operational Models
  An Operational Model is the specification of the operational environment in which the application will eventually run when it goes live
  The Operational Model should be defined and used in testing during the Service Design and Service Transition phases respectively
Application Management Lifecycle

1. Requirements
2. Design
3. Build
4. Operate
5. Optimize
6. Deploy
7. Requirements

Application Management Lifecycle
APPLICATION MANAGEMENT

Application Management generic activities

These include:

Identifying the knowledge and expertise required
Initiating training programs
Recruiting or contracting resources
Design and delivery of end-user training.
In-sourcing for specific activities when required
Definition of standards used in the design of new architectures
Research and Development of solutions
Involvement in the design and building of new services.
Designing and performing tests for the functionality etc
Application Management organization

- All Application Management departments, groups or teams perform similar activities
- Each application or set of applications has a different set of management and operational requirements

Typical examples of Application Management organizations include:

- Financial applications
- There may be several department, groups or teams managing these applications, e.g. Debtors and Creditors, Age Analysis, General Ledger, etc
- Messaging and collaboration applications
- HR applications
- Manufacturing support applications
APPLICATION MANAGEMENT

Application Management roles and responsibilities

• Applications Managers/Team-leaders
  • Take overall responsibility for leadership
  • Provide technical knowledge
  • Ensure necessary technical training
  • Report to senior management on all relevant issues
  • Perform line-management for all team

• Applications Analyst/Architect

Application Analysts and Architects are responsible for matching requirements to application specifications
Application Management metrics

• Measurement of agreed outputs
  • Ability of users to access the application and its functionality
  • Reports and files are transmitted to the users

• Process metrics
  • Response time to events and event completion rates
  • Incident resolution times for second- and third-line support
  • Problem resolution statistics

• Application performance
  • Response times
  • Application availability

• Measurement of maintenance activity
  • Maintenance performed per schedule
  • Number of maintenance windows exceeded

• Training and skills development
Application Management documentation

Documents should be controlled as CIs and related to the relevant applications or Application Management teams

- Application Portfolio
- Application Requirements
- Use and Change Cases
- Design documentation
- Manuals and Standard Operating Procedures
SERVICE OPERATION ROLES AND RESPONSIBILITIES

Service Desk roles

• Service Desk Manager
• Service Desk Supervisor
• Service Desk Analysts
• Super Users

Technical Management roles

• Technical Managers/Team-leaders
• Technical Analysts/Architects
• Technical Operator

Application Management roles:

• Applications Managers/Team-leaders
• Applications Analyst/Architect
SERVICE OPERATION ROLES AND RESPONSIBILITIES

IT Operations Management roles:

• IT Operations Manager
  • Operations Control
  • Facilities Management
• Shift Leaders
• IT Operations Analysts
• IT Operators

Event Management roles

• Role of the Service Desk
• Role of Technical and Application Management
• Role of IT Operations Management
Incident Management roles

- Incident Manager
- First line
- Second line
- Third line includes:
  - Network Support
  - Voice Support (if separate)
  - Server Support
  - Desktop Support
  - Application Management

Request Fulfillment roles

Problem Management roles

- Problem Manager
- Problem-Solving Groups

Access Management roles

- The role of the Service Desk
- The role of Technical and Application Management
- The role of IT Operations Management

Front Metrics Technologies  www.frontmetrics.com
Organization by technical specialization

In this type of organization, departments are created according to technology and the skills and activities needed to manage that technology.
Organization by activity

This type of organization structure focuses on the fact that similar activities have to be performed on all technologies in the organization.
Organization by activity

This type of organization structure focuses on the fact that similar activities have to be performed on all technologies in the organization.
Organizing to manage processes

In process-based organizations people are organized into groups or departments that perform or manage a specific process.

Organizing IT Operations by geography

IT Operations can be physically distributed and in some cases each location needs to be organized according to its own particular context.
Hybrid organization structures
The type of structure used and the exact combination of technical specialization, activity-based and process-based departments will depend on a number of organizational variables.

• Combined functions
  This structure incorporates IT Operations, Technical and Application Management departments into a single structure.

• Organizing Application and Technical Management

• Geography

• Combined Technical and Application Management structure
Technology Considerations
Generic Requirements

An integrated ITSM technology is needed that includes the following core functionality.

- Self Help
- Workflow or process engine
- Integrated CMS
- Discovery/Deployment/Licensing technology
- Remote control
- Diagnostic utilities
- Reporting
- Dashboards
- Integration with Business Service Management

Front Metrics Technologies  www.frontmetrics.com
The following features are desirable for any Event Management technology:

- Multi-environmental, open interface to allow monitoring and alerting
- Easy to deploy, with minimal set up costs
- ‘Standard’ agents to monitor most common environments / components
- Open interfaces to accept any standard (e.g. SNMP) event input and alerting
- Centralized routing of all events to a single location
- Support for design/test phases
- Programmable assessment and handling of alerts
- Ability to allow an operator to acknowledge an alert and escalate if required
- Good reporting functionality to allow feedback into design and transition phases
- Meaningful management information and business user ‘dashboard
Integrated ITSM technology is required that has the following functionality:

- An integral CMS to allow automated relationships to be made and maintained between incidents, service requests, problems, Known Errors
- CMS that can be used to assist in determining priority and aid in investigation and diagnosis
- Automated alerting and escalation capabilities
- Open interfacing to Event Management tools
- A web interface to allow self-help and service requests
- An integrated KEDB so that diagnosed and/or resolved incident/problems
- Easy-to-use reporting facilities to allow incident metrics to be produced
- Diagnostic tools

- Workflow and automated escalation

Front Metrics Technologies    www.frontmetrics.com
PROBLEM MANAGEMENT

Integrated Service Management Technology
An integrated ITSM tool is needed that differentiates between incidents and problems

Change Management
Integration with Change Management is very important, so that Request, Event, Incident and Problem Records can be related to RFCs that have caused problems

Integrated CMS
Integrated CMS which allows Problem Records to be linked to the components affected and the services impacted – and to any other relevant CIs.

Known Error Database
An effective KEDB will be as essential requirement, which should allow easy storage and retrieval of Known Error data.
Access Management uses a variety of technologies, mainly:

**Human Resource Management technology** to validate the identity of users and to track their status

**Directory Services Technology**
Directory Services tools also enable Access Management to create roles and groups and to link these to both users and resources

**Access Management features** in Applications, Middleware, Operating Systems and Network Operating Systems

**Change Management systems**

**Request Fulfilment technology**
SERVICE DESK

Tools and technology support to enable Service Desk staff includes:

• Telephony
  • ACD
  • CTI
  • VOI
• Support tools
  • Known Error Database
  • Diagnostic scripts
  • Self-Help web Interface
  • Remote control
IT Service Continuity Planning for ITSM support tools

Organizations are likely to become quickly dependent upon their ITSM tools and will find it difficult to work without them.

A full Business Impact Analysis and Risk Analysis should be performed and plans then developed to ensure appropriate IT Service Continuity and resilience levels.
Implementing Service Operation
MANAGING CHANGE IN SERVICE OPERATION

Service Operation should strive to achieve stability – but not stagnation!

Change Triggers:

• New or upgraded hardware or network components
• New or upgraded applications software
• New or upgraded system software
• Legislative, conformance or governance changes
• Obsolescence – some components may become obsolete and require replacement or cease to be supported by the supplier/maintainer
• Business imperative – you have to be flexible to work in ITSM
• Enhancements to processes, procedures and/or underpinning tools to improve IT delivery or reduce financial costs
• Changes of management or personnel
• Change of service levels or in service provision – outsourcing, in-sourcing, partnerships, etc.
MANAGING CHANGE IN SERVICE OPERATION

Change assessment

• Service Operation staff must be involved in the assessment of all changes to ensure that operational issues are fully taken into account

• Involvement should commence as soon as possible not just at the later stages of change – i.e. CAB and ECAB membership

• The Change Manager should inform all affected parties of the change being assessed so input can be prepared and available prior to CAB meetings.

• It is important that Service Operation staff are involved at these latter stages as they may be involved in the actual implementation
Measurement of successful change

• The ultimate measure of success in respect of changes made to Service Operation is that customers and users do not experience any variation or outage of service.

• So far as possible, the effects of changes should be invisible, apart from any enhanced functionality, quality or financial savings resulting from the change.
Service Operation is generally viewed as ‘business as usual’ and there is a tendency not to use Project Management processes.

Using Project Management to manage these types of activity would have the following benefits:

- The project benefits are clearly stated and agreed.
- There is more visibility of what is being done and how it is being managed.
- It becomes easier for other IT groups and the business to quantify the contributions made by operational team.
- This in turn makes it easier to obtain funding for projects that have traditionally been difficult to cost justify.
- Greater consistency and improved quality.
- Achievement of objectives results in higher credibility for operational groups.

Front Metrics Technologies

www.frontmetrics.com
ASSESSING AND MANAGING RISK IN SERVICE OPERATION

The most obvious area is in assessing the risk of potential changes or Known Errors.

Service Operation staff may need to be involved in assessing the risk and impact of:

• Failures, or potential failures – reported by Event Management, Incident/Problem Management, or warnings raised by manufacturers, suppliers contractors
• New projects that will ultimately result in delivery into the live environment
• Environmental risk (IT Service Continuity-type risks to the physical environment and locale as well as political, commercial or industrial relations)
• Suppliers, particularly where new suppliers are involved
• Security risks – both theoretical or actual arising from security related incidents
• New customers/services to be supported.
OPERATIONAL STAFF IN SERVICE DESIGN AND TRANSITION

• Service Operation staff must be involved during the early stages of Service Design and Service Transition

• To ensure that when new services reach the live environment

• They are fit for purpose, from a Service Operations perspective, and are ‘supportable’ in the future
Factors that organizations need to plan for in readiness for, and during deployment and implementation of, ITSM support tools:

- Licenses
  - Dedicated licences
  - Shared licences
  - Web licences
  - Service on demand
- Deployment
- Capacity Checks
- Timing of technology deployment
- Type of introduction
Challenges, Critical Success factors and Risks
CHALLENGES

There are a number of challenges faced within Service Operation that need to be overcome. These include those set out in this section:

Lack of engagement with development and project staff

• Traditionally, there has been a separation between Service Operation staff and those staff involved in developing new applications.
• One organization uses an ‘Operation Transition-In Policy’ to ensure that services being deployed have had the appropriate level of input from the operational teams.
• Another organization uses Operations Use Cases to get development teams to include requirements that should be fulfilled by the application to be run in production under the control of Operations personnel.
CHALLENGES

Justifying funding

• It is often difficult to justify expenditure in the area of Service Operation, as money spent in this sphere is often regarded as ‘infrastructure costs’

Examples of potential areas of savings include:

• Reduced software licences costs through the better management of licences and deployed copies
• Reduced support costs due to fewer incidents and problems and reduced resolution times
• Reduced headcount through workforce rationalization, supporting roles and accountability structures
• Less ‘lost business’ due to poor IT service quality
• Better utilization of existing infrastructure equipment and deferral of further expenditure due to better capacity management
• Better-aligned processes, leading to less duplication of activities and better usage of existing resources.
Challenges for Service Operation Managers

• Service Design may tend to focus on an individual service at a time,
• whereas Service Operation tends to focus on delivering and supporting all services at the same time
• Service Design will often be conducted in projects, while Service Operation focuses on ongoing, repeatable management processes and activities
• The two stages in the lifecycle have different metrics, which encourages Service Design to complete the project on time, to specification and in budget
• Service Transition that is not used effectively to manage the transition between the Design and Operation phases
CRITICAL SUCCESS FACTORS

Management support

• Senior and Middle Management support is needed for all ITSM activities and processes, particularly in Service Operation.

• Senior Management must provide visible support during the launch of new Service Operation initiatives (such as through appearances at seminars, signatories to memos and announcements, etc.)

Business support

• It is important that the Business Units also support Service Operation.

• This level of support can be far better achieved if the Service Operation staff involve the business in all of their activities and are open in their reporting of both successes and failures – and their efforts to improve
CRITICAL SUCCESS FACTORS

Champions
ITSM projects and the resulting ongoing practice (performed by Service Operation staff) are often more successful if one or more ‘champions’ are forthcoming who can lead others through their enthusiasm and commitment for ITSM.

Staffing and retention
Having the appropriate number of staff with the appropriate skills is critical to the success of Service Operation
Challenges that need to be overcome include the following:
• underestimation of the number of staff required and how to retain the new skills
• Scarcity of resources who have a good understanding of Service Management.
• Attempting to assign too much, too soon, to existing staff.
Service Management training

Training required for successful Service Management includes:

• Training IT staff on the processes that have been implemented
• Training on ‘soft’ or ‘people’ skills, especially for those staff in customer-facing positions
• Training about understanding the business, and the importance of achieving a service culture
• Where tools have been implemented, training on how to use and manage those tools
• Also, customers and users need appropriate training on how to work with IT – access services, request changes, submit requests, use tools, etc.

Suitable tools

Many Service Operation processes and activities cannot be performed effectively without adequate support tools
Validity of testing

• The quality of IT services that can be provided in Service Operation is dependent upon the quality of systems and components delivered into the operational environment.

• The quality level will be significantly enhanced if adequate and complete testing of new components and releases is carried out in good time.

• Documentation should also be tested for completeness and quality.

• This requires a comprehensive and realistic testing environment.
Validity of testing

• The quality of IT services that can be provided in Service Operation is dependent upon the quality of systems and components delivered into the operational environment.

• The quality level will be significantly enhanced if adequate and complete testing of new components and releases is carried out in good time.

• Documentation should also be tested for completeness and quality.

• This requires a comprehensive and realistic testing environment.

Measurement and reporting

A clear definition is needed of how things will be measured and reported.
Failure to meet the challenges or to address the Critical Success Factors outlined in previous section are obvious risks – but others are described as set out below.

**Service Loss**

- The ultimate risk to the business of weaknesses in Service Operation is the loss of critical IT services with subsequent adverse impact on its employees, customers and finances.

- In extreme cases there may be potential loss to life and limb where the IT services affected are used for critical health or safety purposes.
Risks to successful Service Operation

- Inadequate funding and resources
- Loss of momentum
- Loss of key personnel
- Resistance to change
- Lack of management support
- If the initial design is faulty
- Differing customer expectations
Questions?
THANK YOU!