ITIL Operational Support and Analysis

Contents

1 Introduction to service management

1.1 Best practice

Organizations operating in dynamic environments need to improvetheir performance and maintain competitive advantage. Adoptingbest practices in industry-wide use can help to improve capability. Sources:

- Public frameworks and standards
- Proprietary knowledge of organizations and individuals

1.2 The ITIL frame work

- Vendor-neutral
- Non-prescriptive
- Best practice.

ITIL is successful because it describes practices that enableorganizations to deliver benefits, return on investment andsustained success.

1.3 Service management

A set of specialized organizational capabilities for providingvalue to customers in the form of services

IT service: A service provided by an IT service provider. An IT service is made up of a combination of information technology, people and processes. A customer-facing IT service directly supports the business processes of one or more customers and its service level targets should be defined in a service level agreement (SLA). Other IT services, called supporting services, are not directly used by the business but are required by the service provider to deliver customer-facing services.

The outcomes that customers want to achieve are the reason why they purchase or use a service. The value of the service to the customer is directly dependent on how well a service facilitates these outcomes.

Services can be classified as:

- Core services
- Enabling services
- Enhancing services

Service management enables service providers to:

- Understand the services they are providing
- Ensure that the services really do facilitate the outcomes their customers want to achieve

- Understand the value of the services to their customers
- Understand and manage all of the costs and risks associated with those services.

Service management is concerned with more than just delivering services. Each service, process or infrastructure component has a lifecycle, and service management considers the entire lifecycle from strategy through design and transition to operation and continual improvement.

IT service management (ITSM): The implementation and management of quality IT services that meet the needs of the business. IT service management is performed by IT service providers through an appropriate mix of people, process and information technology.

1.4 Processes and functions

Processes have the following characteristics:

- Measurability
- Specific results
- Customers
- Responsiveness to specific triggers

An organization needs to clearly define the roles and responsibilities required to undertake the processes and activities involved in each lifecycle stage. These roles are assigned to individuals within an organizational structure of teams, groups or functions

1.5 Roles

A role is a set of responsibilities, activities and authorities granted to a person or team. A role is defined in a process or function. One person or team may have multiple roles.Roles fall into two main categories

- generic roles
- specific roles

1.5.1 Process owner

The process owner role is accountable for ensuring that a process is fit for purpose, i.e. that it is capable of meeting its objectives; that it is performed according to the agreed and documented standard; and that it meets the aims of the process definition. This role may be assigned to the same person carrying out the process manager role. Key accountabilities include:

- Sponsoring, designing and change managing the process and its metrics
- Defining the process strategy, with periodic reviews to keep current, and assisting with process design
- Defining appropriate policies and standards for the process, with periodic auditing to ensure compliance
- Communicating process information or changes as appropriate to ensure awareness
- Providing process resources to support activities required throughout the service lifecycle

- Ensuring that process technicians understand their role and have the required knowledge to deliver the process
- Addressing issues with the running of the process
- Identifying enhancement and improvement opportunities and making improvements to the process.

1.5.2 Process manager

The process manager role is accountable for operational management of a process. There may, for example, be several process managers for one process in different locations. This role may be assigned to the same person carrying out the process owner role. Key accountabilities include:

- Working with the process owner to plan and coordinate all process activities
- Ensuring that all activities are carried out as required throughout the service lifecycle
- Appointing people to the required roles and managing assigned resources
- Working with service owners and other process managers to ensure the smooth running of services
- Monitoring and reporting on process performance
- Identifying opportunities for and making improvements to the process.

1.5.3 Process practitioner

A process practitioner is responsible for carrying out one or more process activities. This role may be assigned to the same person carrying the process manager role, if appropriate. Responsibilities typically include:

- Carrying out one or more activities of a process
- Understanding how his or her role contributes to the overall delivery of service and creation of value for the business
- Working with other stakeholders, such as line managers, co-workers, users and customers, to ensure that their contributions are effective
- Ensuring that the inputs, outputs and interfaces for his or her activities are correct
- Creating or updating records to show that activities have been carried out correctly.

1.5.4 Service owner

The service owner is responsible to the customer for the initiation, transition and ongoing maintenance and support of a particular service and is accountable to the IT director or service management director for the delivery of a specific IT service. The service owner's accountability for a specific service within an organization is independent of where the underpinning technology components, processes or professional capabilities reside. Service ownership is critical to service management and one person may fulfil the service owner role for more than one service. Key responsibilities include:

- Ensuring that the ongoing service delivery and support meet agreed customer requirements via effective service monitoring and performance

- Working with business relationship management to ensure that the service provider can meet customer requirements
- Ensuring consistent and appropriate communication with customers for service-related enquiries and issues
- Representing the service across the organization; for example, by attending change advisory board meetings
- Serving as the point of escalation (notification) for major incidents relating to the service
- Participating in internal and external service review meetings
- Participating in negotiating SLAs and operational level agreements (OLAs) relating to the service
- Identifying opportunities for, and making, improvements to the service.

The service owner is responsible for continual improvement and the management of change affecting the service under their care. The service owner is a primary stakeholder in all of the underlying IT processes which enable or support the service they own.

1.5.5 The RACI model

the RACI model or 'authority matrix' can be used to define the roles and responsibilities in relation to processes and activities.

- Responsible
- Accountable
- Consulted
- Informed

Only one person should be accountable for any process or individual activity, although several people may be responsible for executing parts of the activity.

1.6 Operational support and analysis within the context of the service lifecycle

1.6.1 Value to the business of operational support and analysis activities

Service operation is the stage in the lifecycle where the plans, designs and optimizations are executed and measured. Service operation is where actual value is seen by the business. The value provided to the business by service operation includes:

- Agreed levels of service are consistently delivered to the business enabling the business to gain full value from the service and to improve productivity and quality of business outcomes
- Optimization of the cost and quality of services through reduced unplanned costs and automation
- Operational results and data to support continual service improvement and its investment justification

- Confidence that the IT services are secure and only accessed by those authorized to use them.

1.6.2 OSA within the service lifecycle

ITIL Service Operation provides guidance on how to:

- Maintain stability in service operation, allowing for changes in design, scale, scope and service levels
- Achieve effectiveness and efficiency across two major control perspectives: reactive and proactive
- Enable better decision-making in areas such as managing availability, controlling demand, optimizing capacity utilization, scheduling operations, and avoiding or resolving service incidents and managing problems.

1.6.3 Optimizing service operation performance

- Long-term incremental improvement based on evaluating the performance and output of all service operation processes, functions and outputs over time. This type of improvement is typically driven by the continual service improvement stage
- Short-term ongoing improvement of working practices within the service operation processes, functions and technology. These are generally smaller improvements that can be implemented without any fundamental impact.

2 Event management

2.1 Purpose and objectives

The purpose of event management is to manage events throughout their lifecycle. This lifecycle detects events, makes sense of them and determines the appropriate control action, all of which are coordinated by the event management process. They can be used as a basis for automating many routine operations management activities.

The objectives of the event management process are to:

- Detect all changes of state that have significance for the management of a configuration item (CI) or IT service
- Determine the appropriate action for events and ensure communication to the appropriate functions
- Provide the trigger for the execution of many processes and operations management activities
- Provide comparison of actual operating performance against design standards and service level agreements (SLAs)
- Provide a basis for service assurance, reporting and service improvement.

2.2 Scope

- Configuration items (CIs): monitoring of CIs to confirm they remain in a required state or automating frequent changing of a CI state, and updating the configuration management system (CMS) accordingly
- Environmental conditions
- Software license monitoring to ensure optimum and legal license utilization and allocation
- Security
- Normal activity such as tracking usage or performance.

Event management and monitoring are closely related but different. Event management generates and detects specific notifications for monitoring, whereas monitoring detects and tracks these notifications but also actively monitors conditions that do not generate events; for example, to check that devices are operating within acceptable limits.

2.3 Value to the business and service lifecycle

- Early detection of incidents, often leading to assignment for resolution prior to any actual service outage
- Enabling automated activities to be managed by exception, reducing the need for costly real-time monitoring and downtime
- Integration into other service management processes, which can enable detection and notification of status changes or exceptions, triggering an early response and improving process performance

- Automated operations, which increase efficiency and reduce the need for expensive human resources.

2.4 Policies, principles and basic concepts

Examples of event management policies might include:

- Event notifications should go only to those responsible for the handling of their actions, with event routing information being constantly maintained
- Event management and support should be centralized as much as reasonably possible
- Changes and additions for the rule base will need to be under the control of change management
- Common messaging and logging standards and protocols should be used
- Event handling actions should be automated wherever possible
- There should be a standard classification scheme referencing common handling and escalation processes. Notification of incidents and problems should be aligned to the organization's existing categorization and prioritization policies
- All recognized events should be captured and logged, available for data manipulation, filtering and reporting to support incident and problem diagnosis activities.

2.4.1 Types of event

- Informational: this is an event not requiring action, usually logged and retained for an agreed time
- Warning: this is an unusual but not exceptional operation, usually when a device is approaching a threshold, indicating closer monitoring or checking is required
- Exception: this is when a service or device is operating abnormally and action is required

2.4.2 Filtering of events

Strategies for filtering include:

- Integrating filtering into service management processes
- Designing new services that consider event management
- Formally evaluating the effectiveness of filtering
- Planning for the deployment of event management across the entire IT infrastructure.

2.4.3 Designing for event management

Design for event management should take place during the design of a service supported by service operations functions. The designed events should then be tested and evaluated during service transition

Once event management has been deployed, day-to-day operations may identify additional events and other improvements through continual improvement.

Key design considerations include:

- What needs to be monitored?

- What type of monitoring is required?
- When should an event be generated?
- What information needs communicating?
- Who are the messages intended for?
- Who will be responsible for handling the event?

Specific design areas include:

- Instrumentation: defining and designing how to monitor and control the IT infrastructure and services. Mechanisms to be designed include event generation, classification, communication, escalation, logging and storage
- Error messaging: providing meaningful error messages and codes within software applications for inclusion in events
- Event detection and alert mechanisms: designing and populating tools with the criteria and rules to filter, correlate and escalate events.

2.4.4 Event rule sets and correlation engines

A rule set consists of a number of rules that define how the event messages for a specific event will be processed and evaluated. The rules are typically embedded into monitoring and event handling technologies, consisting of algorithms which correlate events that have been generated (e.g. CI state changes) to create logical additional events that need to be communicated (e.g. service or business impact events). These algorithms can be coded into event management tools referred to as correlation engines.

2.5 Process activities, methods and techniques (

2.5.1 Event occurrence

Events occur continuously but not all are detected or registered. It is therefore important that those which need to be detected are understood so they can be appropriately designed and managed

2.5.2 Event notification

- A management tool interrogates devices to collect data
- CIs generate notifications under predefined conditions that were designed and built into the CI

Service design should define which events need to be generated and, for each CI, specify how this should be done. During service transition, event generation is set up and tested

2.5.3 Event detection

Event notifications are detected by an agent running on the same system or by a management tool

2.5.4 Event logging

All events should be recorded, either as an event record or as an entry in the systems log. Where system logs are used they need to be routinely and regularly checked with instructions for any actions required. Event management procedures need to define how long events and logs are kept before being archived.

2.5.5 First-level correlation and filtering

This stage determines whether to communicate an event or ignore it. Filtering eliminates duplicates and unwanted events that cannot be disabled. Filtering undertakes the initial level of 'correlation'. Filtering is not always necessary; for some CIs every event is significant and events go straight to event correlation.

2.5.6 Event significance

Events need to be categorized: recommended categories are 'informational', 'warning' and 'exception'

2.5.7 Second-level event correlation

The meaning of the event is normally determined by the correlation engine which compares the event with a set of criteria (called business rules) in a predefined order to establish the level and type of business impact. The correlation engine is programmed in line with the performance standards defined during service design, plus any additional guidance specific to the operating environment, such as the number of similar events or a comparison of utilization information in the event of reaching minimum or maximum thresholds

2.5.8 Action and response selection

If the correlation activity recognizes an event, a response is required. The action initiates the appropriate response. It may:

- Auto-responses generated for defined events where the response will initiate the action and then evaluate whether it was completed successfully, such as when rebooting a device
- An alert raised for human intervention, containing all the information necessary for the person to determine the appropriate action
- Incident, problem and/or change records generated:
    - incident records can be generated immediately when an exception is detected or as determined by the correlation engine, including as much information about the event as possible
    - Problem records are typically updated to link an incident to an existing problem
    - Requests for change (RFCs) can be generated immediately when an exception is detected or when correlation identifies that a change is needed.

2.5.9 Event review

Because of the high volumes involved, not all events can be formally reviewed. However, significant events or exceptions do need to be reviewed and trends monitored

Event reviews also provide input into continual improvement, and the evaluation and audit of the event management process.

2.5.10 Event closure

Most events are not 'opened' or 'closed'; informational events are only logged. Auto-response events are typically closed by the generation of a second event, triggered on completion of the action initiated. Events linked to incidents, problems or changes are formally closed with a link to the relevant record from the other process.

2.6 Triggers, inputs, outputs and interfaces

Triggers include:

- Exceptions to any level of CI performance defined in the design specifications, OLAs or standard operating procedures
- Exceptions to an automated procedure or process
- An exception within a business process monitored by event management
- Completion of an automated task or job
- A status change in a server or database CI
- Access of an application or database by a user or automated procedure or job
- A predefined threshold is reached; for example, by a device, database or application.

Inputs include:

- Operational and service level requirements associated with events
- Alarms, alerts and thresholds for recognizing events
- Event correlation tables, rules, event codes and automated response solutions
- Roles and responsibilities for recognizing and communicating events
- Operational procedures for recognizing, logging, escalating and communicating events.

Outputs include:

- Events communications and escalations
- Event logs
- Events that indicate an incident has occurred
- Events that indicate the potential breach of an SLA or OLA objective
- Events and alerts that indicate completion status of deployment, operational or other support activities
- A service knowledge management system (SKMS) populated with event information and history.

Event management can interface with any process that requires monitoring and control. Examples:

- Service level management
- Information security management
- Capacity and availability management

- Service asset and configuration management
- Knowledge management
- Change management
- Incident and problem management
- Access management

2.7 Information management

The following information is used in event management:

- Simple network management protocol (SNMP) messages
- Management information bases (MIBs) of IT devices
- Vendor's monitoring software
- Correlation engines containing detailed rules to determine the significance and appropriate response to events
- Event records for all types of event

2.8 Critical success factors and key performance indicators

- CSF Detecting all changes of state that have significance for the management of CIs and IT services:
    - KPI Number and ratio of events compared with the number of incidents
    - KPI Number and percentage of each type of event per platform or application versus total number of platforms and applications underpinning live IT services (looking to identify IT services that may be at risk for lack of capability to detect their events)
- CSF Ensuring all events are communicated to the appropriate functions that need to be informed or take further control actions:
    - KPI Number and percentage of events that required human intervention and whether this was performed
    - KPI Number of incidents that occurred and percentage of these that were triggered without a corresponding event
- CSF Providing the trigger, or entry point, for the execution of many service operation processes and operations management activities:
    - KPI Number and percentage of events that required human intervention and whether this was performed
- CSF Provide the means to compare actual operating performance and behaviour against design standards and SLAs:
    - KPI Number and percentage of incidents that were resolved without impact to the business (indicates the overall effectiveness of the event management process and underpinning solutions)
    - KPI Number and percentage of events that resulted in incidents or changes
    - KPI Number and percentage of events caused by existing problems or known errors (this may result in a change to the priority of work on that problem or known error)

    - KPI Number and percentage of events indicating performance issues (for example, growth in the number of times an application exceeded its transaction thresholds over the past six months)
    - KPI Number and percentage of events indicating potential availability issues (e.g. failovers to alternative devices, or excessive workload swapping)
- CSF Providing a basis for service assurance, reporting and service improvement:
    - KPI Number and percentage of repeated or duplicated events (this will help in the tuning of the correlation engine to eliminate unnecessary event generation and can also be used to assist in the design of better event generation functionality in new services)
    - KPI Number of events/alerts generated without actual degradation of service/functionality (false positives – indication of the accuracy of the instrumentation parameters, important for continual service improvement).

2.9 Challenges and risks

Challenges include the following:

- Difficulty of obtaining funding for the necessary tools and effort needed to install them and exploit their benefits
- Setting the correct level of filtering
- Difficulty and high cost of deploying the necessary monitoring agents across the entire IT infrastructure
- The additional network traffic generated by automated monitoring activities might have negative impacts on the planned capacity levels of the network
- Time needed to acquire the necessary skills, and high cost
- Setting up the necessary processes in order to deploy the event management tools.

Risks include:

- Failure to obtain adequate funding
- Ensuring an incorrect level of filtering
- Failure to maintain momentum in deploying monitoring agents across the IT infrastructure.

2.10 Roles and responsibilities

2.10.1 Event management process owner

- Carrying out the generic process owner role for the event management process
- Planning and managing support for event management tools and processes
- Working with other process owners to ensure an integrated approach to the design and implementation of event, incident, request fulfilment, access and problem management.

2.10.2 Event management process manager

- Carrying out the generic process manager role for the event management process
- Planning and managing support for event management tools and processes

- Coordinating interfaces between event management and other service management processes.

2.10.3 Other event management roles

Events identified as incidents the service desk is responsible for:

- Investigation and resolution of events identified as incidents and then escalation to the appropriate service operation team
- Communication of information about this type of incident to the relevant technical or application management team and, where appropriate, the user.

Technical and application management staffs play several important roles:

- During service design: participation in designing the warranty aspects of the service such as classifying events, updating correlation engines, or ensuring that any autoresponses are defined
- During service transition: testing the service to ensure that events are properly generated and that the defined responses are appropriate
- During service operation: performing event management for the systems under their control; dealing with incidents and problems related to events
- If event management activities are delegated, ensuring that the staffs are adequately trained and that they have access to the appropriate tools to enable them to perform these tasks.

IT operations management staff fulfil the following roles:

- Event monitoring and first-line response may be delegated to IT operations management
- Event monitoring is commonly delegated to the operations bridge where it exists. The operations bridge can coordinate or perform the responses required or provide first-level support.

3 Incident management

3.1 Purpose and objectives

The primary goal of the incident management process is to restore normal service operation as quickly as possible and minimize the adverse impact on business operations, ensuring that agreed levels of service quality are maintained.

The objectives of the incident management process are to:

- Ensure that standardized methods and procedures are used for efficient and prompt response, analysis, documentation, ongoing management and reporting of incidents
- Increase visibility and communication of incidents to business and IT support staff
- Enhance business perception of IT through use of a professional approach in quickly resolving and communicating incidents when they occur
- Align incident management activities and priorities with those of the business
- Maintain user satisfaction with the quality of IT services.

3.2 Scope

Incident management includes any event that disrupts, or which could disrupt, a service. This includes events communicated directly by users through the service desk or detected through an interface from event management to incident management tools and/or logged by technical staff

3.3 Value to the business and service lifecycle

The value of incident management includes the ability to:

- Reduce unplanned labor and costs for both the business and IT support staff
- Detect and resolve incidents resulting in lower downtime and higher service availability
- Identify business priorities and dynamically allocate resources to incidents based on real-time business priorities
- Identify potential improvements to services by understanding what constitutes an incident and aligning with the activities of business operational staff
- Identify additional service or training requirements found in IT or the business.

3.4 Policies, principles and basic concepts

Examples of incident management policies might include:

- Incidents and statuses must be communicated in a timely and effective way
- All incident records must have a common format and set of information fields; there must be common and agreed criteria for prioritizing and escalating incidents; and a standard classification schema for incidents must be adopted
- Incidents must be resolved within timeframes acceptable to the business, be aligned with overall service levels and objectives, and maintain customer satisfaction
- All incidents must be stored and managed in a single management system, integrated with other service management technologies that use or provide incident information. Status

and detailed information on the incident must be recorded and updated on a timely basis in incident records
- Incident records must be audited on a regular basis to ensure they have been entered and categorized correctly, with feedback mechanisms to communicate audit findings and issues to incident-handling staff.

3.4.1 Timescales

Timescales must be agreed for all incident-handling stages, based on the overall incident response and resolution targets within service level agreements (SLAs) and captured as targets within operational level agreements (OLAs) and underpinning contracts (UCs). All support groups need to be made aware of these timescales. Service management tools can be used to automate timescales and escalate the incident as required, based on predefined rules.

3.4.2 Incident models

An incident model is a way of setting out the steps required to handle a particular type of incident in an agreed way. This ensures that 'standard' incidents are handled in a predefined way and within predefined timescales.

The incident model includes:

- The steps to take to handle the incident, the sequence, dependencies and responsibilities
- Timescales and thresholds for completion of the actions; escalation procedures
- Any necessary evidence-preservation activities (particularly relevant for security and capacity-related incidents).

3.4.3 Major incidents

A definition of what constitutes a major incident must be agreed and, ideally, mapped onto the overall incident prioritization system. A specific procedure, with shorter timescales and greater urgency, must be used for 'major' incidents. A separate major incident team may be formed, under the direct leadership of the incident manager, as necessary. If the service desk manager is also fulfilling the role of incident manager, then a separate person may need to lead the major incident investigation team, ultimately reporting back to the incident manager.

3.4.4 Incident status tracking

Incidents should be tracked throughout their lifecycle to support proper handling and reporting on the status of incidents. Within the incident management system, status codes may be linked to incidents to indicate where they are in relation to the lifecycle.

3.4.5 Expanded incident lifecycle

ITIL Service Design and ITIL Continual Service Improvement describe the expanded incident lifecycle which can be used to help understand all contributions to the impact of incidents and to plan for how these could be controlled or reduced.

3.5 Process activities, methods and techniques

3.5.1 Incident identification

As far as possible, all key components need to be monitored so that failures or potential failures are detected early, initiating incident management and, ideally, enabling incident resolution before they have an impact on users

3.5.2 Incident logging

All incidents must be fully logged and date- and/or time-stamped, regardless of whether they are raised through a service desk telephone call, automatically detected via an event alert or identified in any other way.

All relevant information relating to the nature of the incident must be logged so that the details are available for other support groups, if required. The incident record is updated throughout the process.

3.5.3 Incident categorization

Initial logging must allocate suitable incident categorization coding so that the exact type of call is recorded. This is important to establish trends of incident types and frequencies for use in problem management, supplier management and other ITSM activities.

Categorization of the incident must be checked, and updated if necessary, at call closure time (in a separate closure categorization field, so as not to corrupt the original categorization).

3.5.4 Incident prioritization

For every incident an appropriate prioritization code must be agreed and allocated, as this determines how the incident is handled by support tools and support staff.

Prioritization can normally be determined by taking into account the urgency of the incident (how quickly the business needs a resolution) and the level of impact it is causing

Clear guidance must be provided to enable all support staff to determine the correct urgency and impact levels, so that the correct priority can be allocated. Such guidance needs to be produced during service level negotiations.

However, there may be occasions when normal priority levels have to be overridden; for example, because of particular business expediency. The service desk should comply with such requests and correct priority levels later rather than dispute them with the user.

Organizations may also recognize ‘very important people’ (VIPs): high-ranking executives, officers, diplomats, politicians etc. whose incidents are handled on a higher priority than normal. VIPs need to be documented in the guidance provided to the service desk staff.

An incident’s priority may be dynamic; if circumstances change, or if an incident is not resolved within SLA target times, ensure the priority is updated as required to reflect the new situation.

3.5.5 Initial diagnosis

For incidents routed via the service desk, a service desk analyst carries out initial diagnosis, typically while the user is still on the telephone, to try to discover the full symptoms of the incident, determine exactly what has gone wrong and decide how to correct it. At this stage, diagnostic scripts and known error information enable early and accurate diagnosis. Where the resolution is successful, the incident is closed.

Where a service desk analyst cannot resolve an incident while talking to the user but feels that the service desk may be able to do so within the agreed time limit without assistance from other support groups, the analyst informs the user of their intentions, gives the user an incident reference number and attempts to find a resolution.

3.5.6 Incident escalation

- Functional escalation: escalation to upper support level
- Hierarchic escalation: escalation to management level

The service desk keeps the user informed of any relevant escalation that takes place and ensures the incident record is updated to keep a full history of actions.

If there are many incidents in a queue with the same priority level, the service desk and/or incident management staff initially decide the order in which the incidents are picked up and worked on, in conjunction with the managers of the relevant support groups. These managers must ensure that incidents are dealt with in true business priority order and that staff are not allowed to 'cherry-pick' the incidents.

3.5.7 Investigation and diagnosis

Support groups investigate and diagnose what has gone wrong and document all activities (including details of any actions taken to try to resolve or recreate the incident) in the incident record to maintain a complete record of all activities.

3.5.8 Resolution and recovery

When a resolution has been found, sufficient testing must be performed to ensure that the recovery action is complete and that the service has been fully restored to the users. The incident record must be updated with all relevant information and details, regardless of the actions taken or who does them, to maintain a full history.

The resolving group passes the incident back to the service desk for closure action.

3.5.9 Incident closure

The service desk checks that the incident is fully resolved and that the users are satisfied and agree the incident can be closed. The service desk also undertakes:

- Closure categorization
- User satisfaction survey
- Incident documentation

- Ongoing or recurring problem
- Formal closure

3.6 Triggers, inputs, outputs and interfaces

Triggers include the following:

- A user rings the service desk or completes a web-based incident-logging screen
- Event management tools trigger the incident automatically
- Technical staff identify potential failures and raise an incident themselves or via the service desk
- A supplier notifies the service desk of a potential or actual difficulty needing attention.

Inputs include:

- Information about CIs and their status
- Information about known errors and workarounds
- Communication about incidents and their symptoms
- Communication about requests for change (RFCs) and releases
- Communication of events
- Operational and service level objectives
- Customer feedback
- Agreed criteria for prioritizing and escalating incidents.

Outputs include:

- Resolved incidents and resolution actions
- Updated incident management records
- Problem records
- Feedback on incidents related to changes and releases
- Identification of CIs associated with or impacted by incidents
- Satisfaction feedback.

Interfaces include:

- Service level management
- Information security management
- Capacity management
- Availability management
- Service asset and configuration management
- Change management
- Problem management
- Access management

3.7 Information management

Most information used in incident management comes from the following sources:

- Incident management tools
- CMS
- Known error database

Incident management in turn generates the following information:

- Incident records
- Incident details serving as inputs to problem records.

3.8 Critical success factors and key performance indicators

- CSF Resolve incidents as quickly as possible, minimizing impacts to the business:
    - KPI Mean elapsed time to achieve incident resolution or circumvention, broken down by impact code
    - KPI Breakdown of incidents at each stage (e.g. logged, work in progress, closed)
    - KPI Percentage of incidents closed by the service desk without reference to other levels of support (often referred to as 'first point of contact')
    - KPI Number and percentage of incidents resolved remotely, without the need for a visit
    - KPI Number of incidents resolved without impact to the business (e.g. incident was raised by event management and resolved before it could impact the business)
- CSF Maintain quality of IT services:
    - KPI Total numbers of incidents (as a control measure)
    - KPI Size of current incident backlog for each IT service
    - KPI Number and percentage of major incidents for each IT service
- CSF Maintain user satisfaction with IT services
    - KPI Average user or customer survey score (total and by question category)
    - KPI Percentage of satisfaction surveys answered versus total number of satisfaction surveys sent
- CSF Increase visibility and communication of incidents to business and IT support staff:
    - KPI Average number of service desk calls or other contacts from business users for incidents already reported
    - KPI Number of business user complaints or issues about the content and quality of incident communications
- CSF Align incident management activities and priorities with those of the business:
    - KPI Percentage of incidents handled within agreed response time (incident response-time targets may be specified in SLAs, for example, by impact and urgency codes)
    - KPI Average cost per incident
- CSF Ensure that standardized methods and procedures are used for efficient and prompt response, analysis, documentation, ongoing management and reporting of incidents to maintain business confidence in IT capabilities:
    - KPI Number and percentage of incidents incorrectly assigned
    - KPI Number and percentage of incidents incorrectly categorized

    - KPI Number and percentage of incidents processed per service desk agent
    - KPI Number and percentage of incidents related to changes and releases.

A breakdown and categorization of incident metrics by category, timeframe, impact, urgency, service impacted, location and priority provides input to problem management, continual service improvement and other processes to identify issues, problem trends or other situations.

3.9 Challenges and risks

Challenges include:

- The ability to detect incidents as early as possible
- Convincing all staff that all incidents must be logged, encouraging the use of self-help facilities
- Availability of information about problems and known errors
- Integration with the CMS and use of CI relationships and CI histories
- Integration with the SLM process, to correctly assess the impact and priority of incidents and assist in the use of escalation procedures.

Risks include:

- Being inundated with incidents that cannot be handled within acceptable timescales due to a lack of available or properly trained resources
- Unintended backlog of incidents created by inadequate support tools
- Lack of adequate or timely information sources because of poor tools or lack of integration
- Mismatches in objectives or actions due to poorly aligned or absent OLAs and/or UCs.

3.10 Roles and responsibilities

3.10.1 Incident management process owner

- Carrying out the generic process owner role for the incident management process
- Designing incident models and workflows
- Ensuring there is an integrated approach to incident management, problem management, event management, access management and request fulfilment.

3.10.2 Incident management process manager

The role of incident manager may be assigned to the service desk supervisor

- Carrying out the generic process manager role for the incident management process
- Planning and managing support for incident management tools and processes, coordinating interfaces with other service management processes
- Producing management information
- Managing the work of incident support staff (first- and second-line)
- Monitoring and driving the effectiveness of incident management and making recommendations for improvement

- Developing and maintaining the incident management systems and processes
- Managing major incidents.

3.10.3 First-line analyst

- Recording, providing ownership, monitoring, tracking and communication for incidents
- Providing resolution and recovery of incidents or routing incidents to specialist support groups
- Analyzing for correct prioritization, classification and providing initial support
- Keeping users and the service desk informed about incident progress
- Escalating incidents as necessary per established escalation policies
- Closing incidents.

3.10.4 Second-line analyst

A second-line support group is typically made up of staff with greater (though still general) technical skills than the service desk.

They have additional time to devote to incident diagnosis and resolution without interference from telephone interruptions. Key responsibilities are similar to the first-line analyst role.

3.10.5 Third-line analyst

Third-line support can be provided by internal technical groups and/or third-party suppliers including network, voice, server, desktop, application management, database, hardware maintenance engineers and environmental equipment maintainers or suppliers.

4 Request fulfilment

4.1 Purpose and objectives

Request fulfilment is the process responsible for managing all service requests from the users through their lifecycle.

The objectives of the request fulfilment process are to:

- Maintain user and customer satisfaction by handling all service requests in an efficient and professional manner
- Provide a channel for users to request and receive standard services for which there is a predefined authorization and qualification process
- Provide information to users and customers about the availability of services and the procedure for obtaining them
- Source and deliver the components of requested standard services
- Assist with general information, complaints or comments.

4.2 Scope

Some organizations deal with service requests through their incident management process (and tools), with service requests being handled as a particular type of 'incident'

In an organization where large numbers of service requests have to be handled, and where the actions to be taken to fulfil those requests are very varied or specialized, it may be appropriate to handle service requests as a completely separate work stream.

4.3 Value to the business and service lifecycle

- Quick and effective access to standard services; this can improve business productivity and/or quality
- A less bureaucratic system for requesting and receiving access to existing or new services, reducing the cost of providing these services
- Where fulfilment is centralized, having more control over services can reduce costs as supplier negotiation is also centralized and support costs are lower.

4.4 Policies, principles and basic concepts

Examples of request fulfilment policies include:

- The request fulfilment activities follow a predefined process flow or model which includes all stages needed to fulfil the request, the individuals or support groups involved, target timescales and escalation paths
- The ownership of service requests resides with a centralized function; for example, the service desk, which monitors, escalates, dispatches and may also fulfil the request
- Service requests that impact CIs are usually fulfilled by implementing a standard change
- All requests are logged, controlled, coordinated, promoted and managed via a single system

- All requests are authorized before activities are undertaken to fulfil them.

4.4.1 Request models

Service request models (which typically include one or more standard changes in order to complete fulfilment activities) are defined, to ensure that frequently used service requests are handled consistently and meet agreed service levels.

4.4.2 Menu selection

Request fulfilment offers great opportunities for self-help. Users are offered a self-help menu from which they can select requests and provide details.

4.4.3 Request status tracking

Track requests throughout their lifecycle to support proper handling of requests and reporting on their status. Within the request fulfilment system, status codes may be linked to requests to indicate where they are in relation to the lifecycle

4.4.4 Financial approval

The cost of providing the service should first be established and submitted to the user for approval within their management chain. In some cases there may be a need for additional compliance approval, or wider business approval.

4.4.5 Coordination of fulfilment activities

Simple requests may be completed by the service desk, while others are forwarded to specialist groups and/or suppliers for fulfilment. The service desk monitors progress and keeps users informed throughout, regardless of the actual fulfilment source.

4.5 Process activities, methods and techniques

4.5.1 Request receipt, logging and validation

Fulfilment work on service requests should not begin until a formalized request has been received, typically from the service desk. All service requests must be fully logged

4.5.2 Request categorization and prioritization

Requests can be categorized in several ways: for example, by service, activity, type, function or CI type.

Prioritization is determined by taking into account both the urgency of the request (how quickly the business needs to have it fulfilled) and the level of impact it is causing

There may also be occasions when, because of particular business expediency, normal priority levels have to be overridden. Some organizations may also recognize ‘VIPs’ whose service requests are handled as a higher priority than normal.

4.5.3 Request authorization

No work to fulfil a request should be done until it is authorized. Requests can be authorized via the service desk or by having pre-authorized requests. Alternatively, authorization may need to come from other sources

Service requests that cannot be authorized are returned to the requester with the reason for the rejection. The request record is also updated to indicate the rejection status.

4.5.4 Request review

The request is reviewed to determine the appropriate group to fulfil it. As requests are reviewed, escalated and acted upon, the request record is updated to reflect the current request status.

4.5.5 Request model execution

A request model documents a standard process flow, setting out the roles and responsibilities for fulfilling each request type to ensure that the fulfilment activities are repeatable and consistent

Request models may be described as process steps and activities that are stored as reference documents in the service knowledge management system (SKMS). Alternatively they may be stored through specialized configurations within automated workflow tools or through code elements and configurations as part of web-based self-help solutions.

Any service requests that impact CIs in the live environment are authorized through change management, typically as standard changes.

4.5.6 Request closure

Fulfilled service requests are referred back to the service desk for closure. Having checked that the user is satisfied with the outcome, the service desk also ensures that any financial requirements are complete, confirms that the request categorization was correct (or if not, corrects it), carries out a user satisfaction survey, chases any outstanding documentation, and formally closes the request.

4.6 Triggers, inputs, outputs and interfaces

The trigger for request fulfilment is the user submitting a service request, either via the service desk or using a self-help facility

Inputs include:

- Work requests
- Authorization forms
- Service requests
- RFCs
- Requests from various sources such as phone calls, web interfaces or email
- Requests for information.

Outputs include:

- Authorized or rejected service requests
- Request fulfilment status reports
- Fulfilled service requests
- Incidents (rerouted)
- RFCs and standard changes
- Asset and CI updates
- Updated request records.

The primary interfaces are concerned with requesting services and their subsequent deployment:

- Financial management for IT services
- Service catalogue management
- Release and deployment management
- Service asset and configuration management
- Change management
- Incident and problem management
- Access management

4.7 Information management

Request fulfilment is dependent on information from the following sources:

- RFCs
- Service portfolio
- Security policies
- Authorized approvers

Service requests contain information about which service is being asked for, who requested and authorized it, the process used to fulfil the request, the assignee and any actions, date and time of logging, and subsequent actions and closure details.

4.8 Critical success factors and key performance indicators

- CSF Requests must be fulfilled in an efficient and timely manner that is aligned to agreed service level targets for each type of request:
    - KPI The mean elapsed time for handling each type of service request
    - KPI The number and percentage of service requests completed within agreed target times
    - KPI Breakdown of service requests at each stage (e.g. logged, work in progress, closed)
    - KPI Percentage of service requests closed by the service desk without reference to other levels of support (often referred to as ‘first point of contact’)
    - KPI Number and percentage of service requests resolved remotely or through automation, without the need for a visit
    - KPI Total numbers of requests (as a control measure)
    - KPI The average cost per type of service request

- CSF Only authorized requests are fulfilled:
    - KPI Percentage of service requests fulfilled that were appropriately authorized
    - KPI Number of incidents related to security threats from request fulfilment activities
- CSF User satisfaction must be maintained:
    - KPI Level of user satisfaction with the handling of service requests (as measured in some form of satisfaction survey)
    - KPI Total number of incidents related to request fulfilment activities
    - KPI Size of the current backlog of outstanding service requests.

4.9 Challenges and risks

Challenges include:

- Clearly defining the type of requests to be handled by the request fulfilment process
- Establishing self-help capabilities at the front end that allow the users to interface successfully with the request fulfilment process
- Agreeing and establishing service level targets
- Agreeing the costs for fulfilling requests
- Putting in place agreements for which services are standardized and who is authorized to request them
- Making information easily accessible about which requests are available
- Making requests follow a predefined standard fulfilment procedure
- The high impact of request fulfilment on user satisfaction.

Risks include:

- Poorly defined scope, where people are unclear about what the process is expected to handle
- Poorly designed or implemented user interfaces, meaning that users have difficulty raising requests
- Badly designed or operated back-end fulfilment processes that are incapable of dealing with the volume or nature of the requests
- Inadequate monitoring capabilities, meaning that accurate metrics cannot be gathered.

4.10 Roles and responsibilities

4.10.1 Request fulfilment process owner

- Carrying out the generic process owner role for the request fulfilment process
- Designing request fulfilment models and workflows
- Working with other process owners to ensure there is an integrated approach across request fulfilment, incident management, event management, access management and problem management.

4.10.2 Request fulfilment process manager

- Carrying out the generic process manager role for the request fulfilment process
- Planning and managing support for request fulfilment tools and processes, and coordinating interfaces with other service management processes
- Assisting with identification of suitable staffing levels to deliver request fulfilment activities and services
- Ensuring all authorized service requests are being fulfilled on a timely basis, in line with service level targets
- Representing request fulfilment activities at change advisory board (CAB) meetings
- Overseeing feedback from customers and reviewing request fulfilment activities for consistency, accuracy and effectiveness in order to proactively seek improvements.

4.10.3 Request fulfilment analyst

- Providing a single point of contact and end-to-end responsibility to ensure submitted service requests have been processed
- Providing an initial triage of service requests to determine which IT resources will be engaged to fulfil them
- Communicating service requests to other IT resources that will be involved in fulfilling them
- Escalating service requests in line with established service level targets
- Ensuring service requests are appropriately logged.

5 Problem management

5.1 Purpose and objectives

The purpose of problem management is to manage problems through their lifecycle from first identification through investigation, documentation and eventual resolution and closure. Problem management seeks to minimize the adverse impact of incidents and problems on the business caused by underlying errors within the IT infrastructure, and to proactively prevent recurrence of incidents related to these errors.

The objectives of problem management are:

- To prevent problems and resulting incidents from happening
- To eliminate recurring incidents
- To minimize the impact of incidents that cannot be prevented.

5.2 Scope

Problem management includes diagnosing the root cause of incidents and determining the resolution of those problems. It is responsible for ensuring that the resolution is implemented through the appropriate control procedures, including change management and release and deployment management.

Problem management maintains information about problems and the appropriate workarounds and resolutions. This enables a reduction in the number and impact of incidents over time, with a strong interface to knowledge management and tools such as the known error database.

While incident and problem management are separate processes, they are closely related and typically use the same tools and similar categorization, impact and priority coding systems, ensuring effective communication when dealing with related incidents and problems.

A close relationship exists between proactive problem management activities and continual service improvement lifecycle activities that directly support identifying and implementing service improvements. Proactive problem management supports those activities through trending analysis and the targeting of preventive action. Identified problems from these activities become input to the continual service improvement register.

5.3 Value to the business and service lifecycle

- Higher availability of IT services by reducing the number and duration of incidents
- Higher productivity of IT staff by reducing unplanned activity caused by incidents and resolving incidents more quickly through the use of recorded known errors and workarounds
- Reduction in the cost of fire-fighting effort or resolving repeat incidents.

5.4 Policies, principles and basic concepts

- Problems are tracked separately from incidents

- All problems are stored and managed in a single management system
- The classification of problems is standard across the enterprise.

5.4.1 Reactive and proactive problem management activities

Both reactive and proactive problem management activities raise problems, manage them through the problem management process, find the underlying causes of the incidents and prevent future recurrences of those incidents

5.4.2 Problem models

Many problems will be unique and require handling in an individual way. However, some incidents may recur because of dormant or underlying problems (for example, where the cost of a permanent resolution will be high and a decision has been taken not to go ahead with an expensive solution but to 'live with' the problem).

As well as creating a known error record in the known error database (KEDB) to ensure quicker diagnosis, a problem model can be created for handling such problems in the future.

5.4.3 Incidents versus problems

An incident is an unplanned interruption to an IT service or reduction in the quality of an IT service. A problem presents a different view of an incident by understanding its underlying cause. Incidents do not 'become' problems. While incident management activities are focused on restoring services to normal-state operations, problem management activities are focused on finding ways to prevent incidents from happening. It is quite common to have incidents that are also problems.

5.4.4 Problem management techniques

- Chronological analysis
- Pain value analysis
- Kepner and Tregoe (formal problem analysis to investigate deeper-rooted problems)
- Brainstorming
- Five whys (Why did this occur ? five time)
- Fault isolation
- Affinity mapping
- Hypothesis testing
- Technical observation
- Ishikawa diagrams (a method of documenting causes and effects where the main goal is represented by the trunk of the diagram)
- Pareto analysis (separating the most important potential causes of failure from more trivial issues)

5.4.5 Errors detected in the development environment

It is rare for any new applications, systems or software releases to be completely error-free. Often the more serious faults are resolved, but minor faults are not addressed. Where releases into the

live environment include known deficiencies, these are logged as known errors in the KEDB, with details of workarounds or resolution activities

5.5 Process activities, methods and techniques

5.5.1 Problem detection

Problems may be detected in a number of ways

5.5.2 Problem logging

All relevant details of the problem are recorded and date- and/or time-stamped to allow control and escalation.

The problem record needs to be cross-referenced to the related incident records.

5.5.3 Problem categorization

The same categorization system must be used for problems as for incidents, enabling meaningful correlation between the two.

5.5.4 Problem prioritization

Problems must be prioritized in the same way as incidents. However, problem prioritization also takes into account the frequency and impact of the related incidents.

Additionally, when determining the priority of a problem, the severity needs to be taken into account

5.5.5 Problem investigation and diagnosis

An investigation to diagnose the root cause is carried out. Appropriate levels of resource, skills and time need to be allocated based on the priority and category of the problem.

The configuration management system (CMS) is used to determine the extent, or potential extent, of the impact and can be useful in identifying the point of failure. It can be used to identify similar configurations against which to carry out further analysis.

It may be useful to attempt to recreate failure conditions in a test system that mirrors the live environment as far as possible.

5.5.6 Workarounds

A workaround is a temporary way of overcoming difficulties.

In some cases, before a root cause has been identified and resolved, it may be possible to put in place a workaround to resolve related incidents.

The problem record remains open while a workaround is in place.

5.5.7 Create a known error record

A known error record must be created whenever a root cause is known, and where a workaround is in place, and recorded in the KEDB

It may be useful to create a known error record before the root cause is known or a workaround has been identified. In general a known error record should be created whenever it is useful to do so.

5.5.8 Problem resolution

Once a solution has been identified, it needs to be applied as soon as possible. However, there may be constraints that delay resolution. Resolution is usually managed as part of the change management process.

The costs or the disruption associated with making the necessary change may be prohibitive, so the decision may be taken to leave the problem record open and not apply the solution. This decision is recorded as part of the problem record.

5.5.9 Problem closure

When the resolution has been successfully applied, and the change completed, the problem record is closed along with any related open incident records. If there is a related known error record it is updated to show that the resolution has been applied

5.5.10 Major problem review

- What was done correctly
- What was done incorrectly
- What could be done better
- What could be done to prevent recurrence
- Any third-party responsibilities
- Whether follow-up actions are needed.

Where appropriate, output from the major problem review is shared with the customer to demonstrate that these events are being taken seriously and handled responsibly and consistently

5.6 Triggers, inputs, outputs and interfaces

Triggers include:

- Reactive and proactive problem management, plus other problem records, and corresponding known error records
- One or more incidents via service desk staff or identified patterns and trends of incidents
- Supplier's notification of potential faults or known deficiencies
- Reviews of other sources such as operation or event logs, operation communications.

Inputs include:

- Incident records and incident reports for proactive problem trending
- Information about CIs and their status
- Communication about RFCs and releases
- Communication of events
- Operational and service level objectives

- Output from risk management and risk assessment activities.

Outputs include:

- Resolved problems and resolution actions, plus updated problem records
- RFCs
- Workarounds for incidents and known error records
- Problem management reports
- Output and improvement recommendations from majorproblem reviews.

Interfaces include the following:

- Financial management for IT services
- Availability management
- Capacity management
- IT service continuity management
- Service level management
- Change management
- Service asset and configuration management
- Release and deployment management
- Knowledge management
- Seven-step improvement process

5.7 Information management

Problem management uses the following knowledge systems:

- CMS
- KEDB

5.8 Critical success factors and key performance indicators

- CSF Minimize the impact to the business of incidents that cannot be prevented:
    - KPI The number of known errors added to the KEDB
    - KPI The percentage accuracy of the KEDB
    - KPI Percentage of incidents closed at 'first point of contact'
- CSF Maintain quality of IT services through elimination of recurring incidents:
    - KPI Total numbers of problems
    - KPI Size of current problem backlog for each IT service
    - KPI Number of repeat incidents for each IT service
- CSF Provide overall quality and professionalism of problem handling activities to maintain business confidence in IT capabilities:
    - KPI The number of major problems (opened and closed and backlog)
    - KPI The percentage of major problem reviews completed successfully and on time
    - KPI Number and percentage of problems incorrectly assigned or incorrectly categorized

    - KPI The backlog of outstanding problems and the trend
    - KPI Number and percentage of problems that exceeded their target resolution times
    - KPI Percentage of problems resolved and not resolved within SLA targets
    - KPI Average cost per problem.

Ideally, break down all metrics by category, impact, severity and urgency.

5.9 Challenges and risks

Challenges include:

- A major dependency for problem management is the establishment of an effective incident management process and tools
- The skills and capabilities of problem resolution staff to identify the true root cause of incidents
- The ability to relate incidents to problems can be a challenge if the tools used to record incidents are different from those of problems
- The ability to integrate problem management activities with the CMS to determine relationships between CIs and to refer to the history of CIs when performing problem support activities
- Ensuring that problem management is able to use all knowledge and service asset and configuration management resources available to investigate and resolve problems
- Ensuring that there is ongoing training of technical staff, both in technical aspects of their job and in the business implications of the services they support and the processes they use.

Risks include:

- Being inundated with problems that cannot be handled within acceptable timescales due to a lack of available or properly trained resources
- Becoming bogged down with problems, with the result that these problems are not solved as intended because there are inadequate support tools for investigation
- Lack of adequate and/or timely information sources because of inadequate tools or lack of integration.

5.10 Roles and responsibilities

5.10.1 Problem management process owner

- Carrying out the generic process owner role for the problem management process
- Designing incident models and workflows
- Ensuring there is an integrated approach to incident management, problem management, event management, access management and request fulfilment.

5.10.2 Problem management process manager

- Carrying out the generic process manager role for the problem management process
- Planning and managing support for problem management tools and processes, coordinating interfaces with other service management processes
- Liaising with all problem resolution groups, suppliers, contractors etc. to ensure resolution of problems within SLA targets and contractual obligations
- Ownership and maintenance of the KEDB
- Formal closure of all problem records
- Arranging, running and documenting major problem reviews and all related follow-up activities.

5.10.3 Problem analyst

- Reviewing incident data and confirming correct prioritization and classification
- Investigating assigned problems through to resolution or root cause
- Coordinating others to assist with analysis and resolution actions for problems and known errors
- Raising RFCs to resolve problems
- Monitoring progress on the resolution of known errors and advising on available workarounds for incidents
- Updating the KEDB with new or updated known errors and workarounds
- Assisting with major incidents and identifying their root causes.

6 Access management

6.1 Purpose and objectives

Access management grants authorized users the right to use a service, or group of services, while preventing access to non-authorized users.

The objectives of access management are to:

- Manage access to services based on policies in information security management
- Respond efficiently to requests for granting, changing or restricting access rights; verifying whether requests are granted appropriately
- Oversee access to services and ensure that rights provided are not improperly used.

6.2 Scope

Access management is the execution of policies and actions defined in information security management, managing the confidentiality, availability and integrity of an organization's data and intellectual property.

Access management ensures the right of access but not availability of access, which is provided by availability management.

Access management can be initiated via a service request, but is executed by technical and application management functions, coordinated by the service desk or IT operations management.

6.3 Value to the business and service lifecycle

- Controlling access to services so that the organization effectively maintains the confidentiality of its information and achieves regulatory compliance (if required)
- Giving employees the appropriate access that they need in order to be effective
- Revoking access rights when needed
- Enabling the use of services to be audited, or abuse to be traced.

6.4 Policies, principles and basic concepts

Access management enables users to access services documented in the service catalogue.

Examples of access management policies might include:

- Access management administration and activities are directed by the policies and controls in the information security policy
- Accesses to use services are logged and tracked, ensuring rights provided are appropriately used
- Access to services is maintained in alignment with changes in personnel events such as transfers and terminations
- An accurate history is maintained of who has accessed, or tried to access, services
- Procedures for handling, escalating and communicating security events are defined and aligned to the information security policy.

Key concepts include:

- Access the level and extent of a service's functionality or data that a user is entitled to use
- Identity Information that distinguishes each user and verifies his or her status in an organization; each identity is unique
- Rights (or privileges) Settings that enable a user to access a service in a particular way; for example, read, write, execute, change or delete
- Service or service groups As most users do not use just one service, and users with similar roles use a similar set of services, it is more efficient to grant each user or group of users access to a set of services in a group
- Directory services Tools used to manage access and rights.

6.5 Process activities, methods and techniques

6.5.1 Requesting access

- Standard request generated by an HR system, such as for a new starter, promotion or leaver
- Request for change (RFC) or service request
- Execution of a pre-authorized script.

6.5.2 Verification

- The user requesting access is who they say they are. This type of verification depends on an organization's security policy; this is usually achieved by the user providing his or her username and password
- The user has a legitimate requirement for the service. This requires independent verification; for example:
    - Notification from HR or authorization from an appropriate manager
    - Submission of an RFC or service request, with supporting evidence, through change management
    - A policy stating the user is allowed access to an optional service if needed.

The RFC for new services specifies the users or user groups to be given access. Access management verifies that these users remain valid and then automatically provides access as specified in the RFC.

6.5.3 Providing rights

Access management does not decide who has which access rights; it executes the policies and regulations defined in service strategy and service design, enforcing decisions to restrict or provide access.

Following verification, the user is provided with the rights to use the requested service. Typically, this requires a request to action, which is sent to the relevant team supporting the service. Where possible, these actions should be automated.

Role conflict can occur where there are many roles and groups. Any conflict is documented and escalated for resolution.

For any role or group, there may be users who need something slightly different from the predefined role. Each exception is coordinated by access management and approved via the originating process.

Regular reviews of the roles and groups are performed to ensure that they remain appropriate, and unwanted or obsolete groups are removed.

6.5.4 Monitoring identity status

Users' roles and access needs change over time. Access management documents the user lifecycle for each type of user and automates the process based on this.

Access management tools require facilities to change user states or move users between groups and maintain an audit trail.

6.5.5 Logging and tracking access

Access monitoring and control activities need to be included in the monitoring activities undertaken by technical and application management and all service operation processes. Exceptions are handled by incident management. Specific incident models can be designed to handle abuse of access rights.

Information security management can use intrusion detection tools to detect unauthorized access and check what rights have been provided by access management.

Access management may be required to provide access records for forensic investigations. This is usually provided by operational staff, but working as part of the access management process.

6.5.6 Removing or restricting rights

Access management is responsible for revoking rights and executing the decisions and policies made during service strategy and service design.

Access is usually removed following a death, resignation, dismissal, role change or transfer.

6.6 Triggers, inputs, outputs and interfaces

Inputs include:

- Information security policies
- Operational and service level requirements for granting access to services, performing access management administrative activities and responding to access management related events
- Authorized RFCs to access rights
- Authorized requests to grant or terminate access rights.

Outputs include:

- Provision of access to IT services
- Access records and history of access granted to services
- Access records and history where access has been denied and the reasons for the denial
- Timely communications concerning inappropriate access or abuse of services.

Interfaces include:

- Demand management
- Strategy management for IT services
- Information security management
- Service catalogue management
- IT service continuity management
- Service level management
- Change management
- Service asset and configuration management
- Request fulfilment

6.7 Information management

All data held about users is subject to data protection legislation and should be protected by each organization's security procedures.

Access management generates a username and password and has the information on the access types granted to the specific resources. To be effective, access management needs the following information:

- Well-defined procedures between IT and HR that include fail-safe checks to ensure that access rights are removed as soon as they are no longer justified or required
- 'User profile', 'user template' or 'user role': used to describe the type of grouping for easier management of standard access
- The groups that users may belong to and the associated access requirements, although a user may have additional access requirements relating to their role. Some groups may have specific access requirements
- A catalogue of all the roles in the organization and which services support each role. This catalogue of roles is compiled and maintained by access management in conjunction with HR and may be automated in the directory services tools.

6.8 Critical success factors and key performance indicators

- CSF Ensure that the confidentiality, integrity and availability of services are protected in accordance with the information security policy:
    - KPI Percentage of incidents that involved inappropriate security access or attempts at access to services
    - KPI Number of audit findings that discovered incorrect access settings for users who have changed roles or left the company
    - KPI Number of incidents requiring a reset of access rights

    - KPI Number of incidents caused by incorrect access settings
- CSF Provide appropriate access to services on a timely basis to meet business needs:
    - KPI Percentage of requests for access (e.g. service request, RFC) that were provided within established service level agreements (SLAs) and operational level agreements (OLAs)
- CSF Provide timely communications about improper access or abuse of services on a timely basis:
    - KPI Average duration of access-related incidents (from time of discovery to escalation).

6.9 Challenges and risks

Challenges include:

- Monitoring and reporting on access activity as well as incidents and problems related to access
- Verifying the identity of a user, and that he or she qualifies for access to a specific service or the approving person or body
- Linking multiple access rights to an individual user
- Determining the status of users at any time
- Managing changes to a user's access requirements
- Restricting access rights to unauthorized users
- Building and maintaining a database of all users and the rights that they have been granted.

Risks include:

- Lack of appropriate supporting technologies to manage and control access to services, which can lead to a dependency on error-prone manual tasks
- Controlling access from 'back-door' sources such as application interfaces
- Managing and controlling access to services by external third-party suppliers
- Lack of management support for access management
- Access levels and management controls unnecessarily hindering the business.

6.10 Roles and responsibilities

6.10.1 Access management process owner

- Carrying out the generic process owner role for the access management process
- Designing access request workflows
- Working with other process owners to ensure there is an integrated approach to the design and implementation of access management, incident management, event management, request fulfilment and problem management.

6.10.2 Access management process manager

- Carrying out the generic process manager role for the access management process

- Planning and managing support for access management tools and processes
- Coordinating interfaces between access management and other service management processes.

6.10.3 Other access management roles

Responsibilities of service desk staff include:

- Providing a route to request access to a service via a service request. The service desk will validate the request, then pass it to the appropriate team to provide access. This team may have delegated responsibility for providing access for simple services during the call
- Communicating with the user when access has been granted and ensuring that he or she receives any other required support
- Detecting and reporting incidents related to access.

Responsibilities of technical and application management staff include:

- During service design, ensuring that mechanisms are created to simplify and control access management for each service; finding ways to detect and stop the abuse of rights
- During service transition, testing the service to ensure that access can be granted, controlled and prevented as designed
- During service operation, performing access management for the systems under their control and dealing with accessrelated incidents and problems
- Providing training to service desk or IT operations management to ensure that staff are adequately trained and that they have access to the appropriate tools to enable them to perform these tasks.

Responsibilities of IT operations management staff could include:

- Providing or revoking access to key systems or resources for each area
- Using the operations bridge to monitor events related to access management and provide first-line support and coordination in the resolution of those events where appropriate.

7 Service desk

7.1 Role

The service desk is the single point of contact for users when there is a service disruption. It can also be responsible for dealing with service requests and for some categories of request for change (RFC). The service desk commonly acts as an 'entry level' function for IT staff

The service desk plays a critical role in the delivery of services by providing:

- 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
- 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

7.2 Objectives

The primary aim of the service desk is to provide a single point of contact between the services being provided and the users.

A typical service desk:

- Manages incidents and service requests
- Handles communication with the users
- Executes the incident management and request fulfilment processes to restore the normal-state service operation to the users as quickly as possible. ('Restoration of service' is meant in the widest possible sense, such as fixing a technical fault, fulfilling a service request or answering a query; whatever is needed to allow the users to return to working satisfactorily.)

Specific responsibilities include:

- Logging all relevant incident and service request details and allocating categorization and prioritization codes
- Providing first-line investigation and diagnosis
- Resolving incidents and service requests at this level if possible
- Escalating incidents and service requests where they cannot be resolved within agreed timescales
- Keeping users informed of progress
- Closing all resolved incidents and service requests
- Conducting customer satisfaction surveys

- Maintaining communication with users:
    - Keeping users informed of incident progress
    - Notifying users of impending changes or agreed outages.

7.3 Organizational structures

7.3.1 Local service desk

A local service desk is located close to or within the user community it serves, aiding communications and providing a visible presence. However, it can be expensive and inefficient to resource.

7.3.2 Centralized service desk

The service desk function is centrally located. It may consolidate a number of local service desks into a single location or a smaller number of locations. This can be more efficient and cost-effective.

Some form of local presence might still be necessary to handle physical support requirements, although these would be controlled from the central desk.

7.3.3 Virtual service desk

A virtual service desk uses technology to give the impression of a single centralized service desk, although it may be staffed by personnel in different locations or functional areas of the organization

However, if the virtual service desk model is used, it is important to ensure consistency of service quality, terms and common processes and tools.

7.3.4 Follow the sun

An organization using the 'follow-the-sun' model combines two or more geographically dispersed service desk functions, each typically operating in 'normal working hours', to provide a 24-hour service for all users at relatively low cost. However, under this option it is important to ensure consistency of service quality, terms and common processes and tools.

7.3.5 Specialized service desk groups

In some circumstances it may be effective to create specialized service desk groups. These may be based on:

- VIP customers
- Business processes
- Culture or language.

Technology can be employed to capture the caller requirements and to route calls to the specialist group as appropriate. This can accelerate restoration of normal service for the groups served.

7.3.6 Building a single point of contact

Regardless of the model chosen for the service desk function, it is important to ensure that individual users are in no doubt as to whom they should contact if they need assistance.

The service desk needs to be seen as the single point of contact for the user, so it is advisable to ensure that there is just one telephone number, one user help portal and one email address to use in all cases.

7.4 Staffing options

7.4.1 Staffing levels

When designing and staffing the service desk, an organization must provide the correct number of appropriately trained staff to respond to the level of demand and to maintain committed levels of service.

Organizations are usually faced with a challenge when doing this. Levels of demand for the service desk vary, based on a number of factors:

- Demand levels on the business itself
- Release and deployment of new IT services

Many organizations experience increased call rates during the start of the business day and again after lunch. Consider the following factors when determining staffing levels:

- Customer service expectations
- Business requirements such as available budget and call and resolution response times
- Size, age, design and complexity of the IT infrastructure
- Number of customers and users to support, plus associated factors:
    - User skill levels
    - Language requirements
- Incident and service request types and the implications for the amount of time needed to respond, the different volumes expected and the internal expertise required to address the requests
- Period of support cover required, which can be influenced by a number of factors:
    - Hours covered
    - Out-of-hours support requirements
    - Time zones covered
    - Locations to be supported, especially if desk-side support is required
    - Workload patterns
    - Agreed service level targets
- Type of response required (email, telephone, in person)
- Level of training required (and the ongoing training requirements)
- Support technologies available
- Existing staff skill levels

- Processes and procedures in use.

7.4.2 Skill levels

The organization must decide on the level and range of skills it requires to fulfil the requirements of the service desk. There is a range of possible skill options, from simple call logging through to detailed technical understanding. In most cases the service desk employs a combination of skills somewhere along that scale.

Generally, higher targets result in higher costs to meet those targets.

Generally, the more standardized the solution, the less it requires specialized skills to support it.

7.4.3 Training

Once the skills requirements are understood a formal training program can be put in place and maintained. This ensures that the required skills can be provided and subsequently maintained and enhanced

To be effective, the service desk skill levels and requirements need to be reassessed periodically and accurate training records maintained

7.4.4 Staff retention

A good service desk can suffer enormously from a significant loss of staff, so efforts need to be made to ensure it remains an attractive place to work

The service desk can be a route to other functions in the organization or into supervisory or managerial roles. Take care to properly define and develop internal career paths and opportunities, and to ensure that appropriate succession planning is in place to enable career progression to take place without negatively affecting service delivery

7.4.5 Super users

Many organizations find it useful to appoint or designate a number of super users throughout the user community to act as liaison points with IT in general and with the service desk in particular

Super users do not necessarily provide support for the whole of IT. In most cases they provide support for a specific application, module or business area

Where super users form part of the service desk function they must be included in the service desk training and awareness program and take part in any additional service desk teambuilding activities. This ensures that they remain effective in their contribution and have a strong sense of being part of the service desk team.

7.5 Measuring service desk performance

Metrics need to be established so that performance of the service desk can be evaluated at regular intervals, assessing the health, maturity, efficiency and effectiveness of the function, and identifying any opportunities to improve service desk operations

Metrics need to be used in conjunction with other measures and management information to determine the reasons for any increase or decrease in calls. It is useful to be able to compare this against the customer's perception of the service, which can be gathered using a customer satisfaction survey

Some examples of useful service desk metrics, to be collected and analyzed for trends over time, include:

- First-line resolution rate showing the percentage of calls resolved by the service desk function, broken down by:
    - Percentage of calls resolved during the first contact with the user
    - Percentage resolved by the service desk staff alone compared to the percentage resolved by the first-line service desk staff and second-line support staff combined
- Average time to escalate an incident when first-line resolution is not possible
- Average service desk cost of handling an incident, which can be reported in different ways; for example:
    - Total cost of the service desk divided by the number of calls, giving basic high-level planning indications
    - Total cost of the service desk divided by the total call duration time, calculating the cost for individual calls, which can be combined with categorization data to allow more detailed and specific analysis to be carried out
- Percentage of user updates conducted within target times
- Average time to review and close a resolved call
- Number of calls broken down by time of day and day of the week, combined with the average call-time metric; this is critical to determining staff level requirements.

7.5.1 Customer satisfaction surveys

It is important that the service desk maintains data on customer perception of the service. Customer satisfaction is a critical success factor (CSF) for the service desk. A number of survey techniques and tools are available:

- After-call survey
- Outbound telephone survey
- Personal interviews
- Group interviews
- Postal or email surveys
- Online surveys

It is advisable to keep the number of questions to a minimum and, where possible, align them to the specific customer experience. To allow adequate comparison, the same percentage of calls should be selected in each period and calls rigorously carried out, despite any other time pressures.

7.6 Outsourcing the service desk

If the decision is made to outsource the service desk function, it is vital that the organization retains responsibility for the activities and the services provided. There are a number of areas to consider to safeguard the service:

- Common tools and processes should be shared by the two organizations to allow a smooth processing flow. The outsourced service desk should have access to:
    - All incident records and information
    - Problem records and information
    - Known error records
    - Change schedule
    - Sources of internal knowledge, especially second- and third-line support
    - Configuration management system (CMS)
    - Alerts from monitoring tools
- Service level agreements (SLAs) for incident handling and resolution must be agreed by all parties and reflected in operational level agreements (OLAs) and underpinning contracts (UCs)
- Good lines of communication need to be maintained between the outsourced service desk and the organization's other support teams. This can be assisted by some or all of the following steps:
    - Close physical co-location
    - Regular liaison and review meetings
    - Cross-training tutorials between the teams and departments
    - Partnership arrangements, where staff from both organizations are used jointly to staff the service desk
- Ownership of data:
    - Data collected by the outsourced service desk needs to be agreed and detailed in the underpinning contract with the outsource provider
    - Data relative to the users, customers, CIs, services, incidents, service requests, changes etc. needs to remain with the organization that is outsourcing the service desk
    - Data specifically related to the performance of the outsourcing provider's employees must remain under the ownership of that company. This may also apply to other data that is relevant only for the internal management of the outsourcing company.

8 Service operation functions

8.1 Functions

A function is a logical concept that refers to the people and automated measures that execute a defined process, an activity or a combination of processes or activities. The service operation functions are needed to manage the 'steady state' operational IT environment:

- service desk function
- Technical and application management
- IT operations management

8.2 Technical management

Technical management provides detailed technical skills and resources to support the ongoing operation of the IT infrastructure. It also plays an important role in the design, testing, release and improvement of IT services. It refers to the groups, departments and teams that provide technical expertise and overall management of the IT infrastructure

8.2.1 Role

Technical management fulfils a dual role:

- Responsible for the technical knowledge and expertise relating to the management of the IT infrastructure, ensuring the knowledge required to design, build, transition, operate and improve the technology is identified, developed and refined
- Providing the resources required to support the ITSM lifecycle, ensuring the technical resources are effectively trained and deployed to design, build, transition, operate and improve the technology.

Technical management also provides guidance to IT operations on how best to carry out the ongoing operational management of technology. This is carried out partly during the service design process, and also through day-to-day communications with IT operations management.

8.2.2 Objectives

The objectives of technical management are to help plan, implement and maintain a stable infrastructure supporting the organization's business processes through:

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

8.2.3 Activities

There are two types of activity that technical management is involved in:

- Activities that are generic to the technical management function as a whole, discussed in this section

- A set of discrete activities and processes, which are performed by all three functions of technical, application and IT operations management, plus technology management activities such as mainframe, server, middleware, network, desktop, internet, storage or archive, database and directory services management.

The key technical management activities include:

- Identifying the knowledge and expertise required, the skills that exist in the organization as well as those skills that need to be developed, and initiating training programs to develop and refine the appropriate skills
- Participating in the definition of standards and technology architectures, the design and creation of new services to meet the standards required, and taking part in enhancement and operational projects
- Assisting with risk assessment, identifying critical services and system dependencies and defining and implementing countermeasures
- Designing and performing tests for the functionality, performance and manageability of IT services
- Managing vendors and contracts
- Defining and managing event management standards and tools, and also monitoring and responding to many categories of events
- Assisting incident and problem management
- Assisting with evaluation and building of changes and the deployment of releases
- Assisting continual service improvement processes in identifying opportunities for improvement and evaluating alternative solutions
- Defining and assisting with the operational activities performed as part of IT operations management.

8.3 IT operations management

IT operations management is the function responsible for the ongoing management and maintenance of an organization's IT infrastructure to ensure delivery of the agreed level of service to the business

8.3.1 Role

IT operations management has two main areas of responsibility:

- Performing the activities and meeting the performance standards defined during service design and tested during service transition. The primary role of IT operations management is to maintain a stable infrastructure and consistency of IT service
- Supporting the ability of the business to meet its objectives; this depends on the output and reliability of the day-to-day IT operations. IT operations add value to the business as a part of the overall value network.

IT operations must maintain a balance between these activities and roles. This requires:

- An understanding among all staff of how technology and technology performance affect the delivery of IT services
- An understanding of the relative importance and impact of the services
- Processes, procedures and manuals
- A clearly defined set of achievement metrics for reporting
- A cost strategy for balancing the requirements of different business units with cost savings through the optimization of technology
- A value-based strategy for return on investment rather than a cost-based one.

8.3.2 Objectives

- Maintenance of the status quo to ensure that the organization's day-to-day processes and activities are stable
- Regular monitoring and improvement to achieve higherquality service at reduced costs, while maintaining stability
- Rapid application of operational skills to diagnose and resolve IT operation failures.

8.3.3 Activities

- Operations control: oversees the execution and management of the IT infrastructure operational events and activities
    - Console management
    - Job scheduling
    - Backup and restore
    - Print and output management
    - Maintenance activities
- Facilities management: manages the physical environments, data center, computer rooms and recovery sites, including all power and cooling equipment

8.4 Application management

Application management is responsible for managing applications throughout their lifecycle. This function supports and maintains operational applications and also plays an important role in the design, testing and improvement of applications that form part of IT services.

8.4.1 Role

Application management is to applications what technical management is to the IT infrastructure. It plays a role in all applications, whether purchased or developed in-house. It contributes to the key decision on whether to buy an application or to build it. Application management plays a dual role:

- Custodian of technical knowledge and expertise related to managing applications, ensuring that the knowledge required to design, test, manage and improve IT services is identified, developed and refined

- Provider of the resources to support the ITSM lifecycle, ensuring that resources are effectively trained and deployed to design, build, transition, operate and improve the technology required to deliver and support IT services.

Application management is also responsible for maintaining a balance between the skill level and the cost of these resources.

In addition to these two high-level roles, application management also performs the following specific roles:

- Providing guidance to IT operations about how best to carry out the ongoing operational management of applications. This role is partly carried out during the service design process, but also through day-to-day communications with IT operations management
- Integrating the application management lifecycle into the ITSM lifecycle.

8.4.2 Objectives

The objectives of application management are to:

- Support the organization's business processes by helping identify functional and manageability requirements for application software
- Assist in the design and deployment of applications and the ongoing support and improvement of those applications.

These objectives are achieved through:

- Applications that are well-designed, resilient and cost-effective
- Ensuring that the necessary functionality is available to achieve the required business outcomes
- Organization of adequate technical skills to maintain operational applications in optimum condition
- Swift use of technical skills to rapidly diagnose and resolve any technical failures that do occur.

8.4.3 Activities

Most application management teams or departments are dedicated to specific applications or sets of applications, but undertake some common activities including:

- Identifying the knowledge and expertise required to manage and operate applications in the delivery of IT services, and initiating training programs to develop and refine the skills
- Designing and delivering end-user training, either by application development or application management groups, or by a third party. Application management is responsible for ensuring that training is conducted as appropriate
- Defining standards for the design of new architectures, participating in the design and building of new services, contributing to the design of the technical architecture and performance standards for IT services

- Designing and performing tests for the functionality, performance and manageability of IT services, designing applications to meet the levels of service required by the business, including modelling and workload forecasting
- Assisting in risk assessment, identifying critical service and system dependencies and defining and implementing countermeasures
- Managing suppliers of specific applications within the service level management and supplier management processes
- Participating in definition of event management standards and the instrumentation of applications for the generation of meaningful events
- Supporting problem management in validating and maintaining the known error database (KEDB) with application development teams
- Evaluating changes (many changes are built by application management teams) and driving release management for their applications
- Participating in defining the operational activities performed as part of IT operations management. Application management may perform the operational activities as part of an organization's IT operations management function.

Application management teams or departments are needed for all key applications. The role varies depending on the applications being supported, but generic responsibilities include:

- Third-level support for incidents related to the application
- Involvement in operation-testing plans and deployment issues
- Application bug tracking and patch management (coding fixes for in-house code, transports and/or patches for third-party code)
- Involvement in application operability and supportability issues such as error code design, error messaging, event management hooks
- Application sizing and performance; volumetric and load testing etc. in support of capacity and availability management processes
- Involvement in developing release policies
- Identification of enhancements to existing software, for both functionality and manageability.

9 Technology and implementation

9.1 Generic requirements for IT service management technology

The same technology should be used at all stages of the service lifecycle. Generally this includes:

- Self-help
- Workflow or process engine
- Integrated configuration management system (CMS)
- Discovery, deployment and licensing technology
- Remote control
- Diagnostic utilities
- Reporting
- Dashboards
- Integration with business service management

9.2 Evaluation criteria for technology and tools

Some generic points that organizations should consider when selecting any service management tool include:

- Data handling, integration, import, export and conversion
- Data backup, control and security
- Ability to integrate multi-vendor components, existing and into the future
- Conformity with international open standards
- Usability, scalability and flexibility of implementation and usage
- Support options provided by the vendor, and credibility of the vendor and tool
- The platform the tool will run on and how this fits the IT strategy
- Training and other requirements for customizing, deploying and using the tool
- Costs: initial and ongoing.

It is generally best to select a fully integrated tool, but this must support the processes used by the organization, and extensive tool customization should be avoided.

Tool requirements should be categorized using MoSCoW analysis:

- M: MUST have this
- S: SHOULD have this if at all possible
- C: COULD have this if it does not affect anything else
- W: WON'T have this, but WOULD like in the future.

9.3 Evaluation criteria for technology and tools for process implementation

9.3.1 Event management

Event management technology should have the following features:

- A multi-environmental, open interface to:
    - Allow monitoring and alerting across heterogeneous services and the entire IT infrastructure
    - Accept any standard (e.g. simple network management protocol) event input and generation of multiple alerting
- 'Standard' agents to monitor the most common environments, components and systems
- Configurable and programmable functionality to support correlation, assessment and handling of alerts, manipulation and routing of events (centralized or local)
- Capability to suppress or flag events during periods of scheduled outages
- Capability to allow an operator to acknowledge an alert, and if no response is entered within a defined timeframe, to escalate the alert
- Good reporting functionality.

Technology should allow a direct interface into the organization's incident management and escalation processes to support staff, third-party suppliers and engineers.

9.3.2 Incident management

Integrated ITSM technology should have the following features:

- Incident-logging capabilities that allow for efficient entry of incident data, categorization, prioritization, tracking and reporting of incidents
- An integral CMS to allow automated relationships to be made and maintained and used to assist in prioritization, investigation and diagnosis
- A process flow engine to allow processes to be predefined and automatically controlled
- Automated alerting and escalation capabilities
- A web interface to allow self-help and service requests to be input via internet or intranet screens
- An integrated known error database (KEDB)
- Easy-to-use reporting facilities
- Diagnostic tools.

Note that target times should be included in the support tools that are used to automate the workflow control and escalation paths.

9.3.3 Request fulfilment

Integrated ITSM technology is needed so that service requests can be linked to related incidents or events.

Some organizations may use the incident management element of ITSM tools and treat service requests as a subset and defined category of incidents. Request fulfilment technology should have the following capabilities:

- Front-end self-help capabilities
- Workflow engine capabilities

Otherwise the facilities required are very similar to those for managing incidents and changes: for example, predefined workflow control of models, priority levels, automated escalation and effective reporting.

9.3.4 Problem management

Problem management should have the following features:

- An integrated ITSM tool that differentiates between incidents and problems
- Integration with change management. This is very important, so that request, event, incident and problem records can be related to the requests for change (RFCs) that have caused problems
- Integration with the CMS. This is needed to allow problem records to be linked to the components affected and the services. Service asset and configuration management forms part of a larger service knowledge management system (SKMS) which includes linkages to many of the data repositories used in service operation
- An effective KEDB. This is an essential requirement to allow easy storage and retrieval of known error data
- Good reporting facilities.

Note that in some cases the components or systems that are being investigated by problem management may have been provided by third-party vendors or manufacturers. Therefore, vendors' support tools and/or KEDBs may also need to be used.

9.3.5 Access management

- Human resource management technology, to authenticate the identity of users, authorize their access, and track their status
- Directory services technology to enable technology managers to assign names to resources on a network and then provide access to those resources based on the profile of the user. 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.

9.3.6 Service desk

Telephony systems used by the service desk should include:

- An automatic call distribution system to allow group pick-up capabilities from a single telephone number
- Computer telephony integration software to allow caller recognition and the incident record from the CMS to be automatically updated with the user's details
- Voice-over internet protocol, which can reduce telephony costs
- Statistical software to allow telephony statistics to be gathered and analyzed:

    - Number of calls received, in total and broken down by any 'splits'
    - Call arrival profiles and answer times
    - Call abandon rates
    - Call handling rates by individual service desk call handlers
    - Average call durations
- Hands-free headsets, with dual-user access capabilities for use, for example, during training of new staff.

The following support tools will be particularly beneficial for use by the service desk:

- An integrated KEDB to store details of previous incidents, problems, workarounds, root causes and their resolutions
- Functionality to categorize and quickly retrieve previous known errors, using pattern matching and keyword searching against symptoms
- Multi-level diagnostic scripts to allow service desk staff to pinpoint the cause of failures. These context-sensitive scripts appear on screens, dependent upon the multi-level categorization of the incident, and are driven by the user's answers to diagnostic questions
- Automated 'self-help' functionality so users can seek and obtain help to resolve their own difficulties. Ideally this should be a 24/7 web interface driven by menu selection: for example, frequently asked questions; 'how to do' search capabilities; password change or software repairs and fixes. Self-help may also include allowing users to log incidents themselves
- Remote control of the user's desktop to allow service desk analysts to conduct investigations or correct settings
- Appropriate IT service continuity and resilience levels.

9.4 Practices for process implementation

9.4.1 Service operation and project management

It is important that all projects make use of project management processes. Using project management processes can bring the following benefits:

- Project benefits are agreed and documented
- It is easier to see what is being done and how it is being managed
- Funding can be easier to obtain
- There is greater consistency and improved quality
- Objectives are more likely to be achieved, leading to higher credibility for operational groups.

9.4.2 Assessing and managing risk in service operation

Risk assessment and management is required throughout the service lifecycle

- Risks from potential changes or known errors

- Failures or potential failures: these may be identified by event management, incident management or problem management, but also by warnings from manufacturers, suppliers or contractors
- Environmental risks: risks to the physical environment as well as political, commercial or industrial relations risks, which could lead to invoking IT service continuity
- Suppliers, particularly if they control key service components
- Security risks
- Support of new customers or services.

9.4.3 Operational staff in service design and transition

Activities during service design and service transition should involve staff from all IT groups to ensure that new components and services are designed, tested and implemented in a way that will provide the service utility and service warranty required.

Service operation staff must be involved during the early stages of design and transition to ensure that new services are fit for purpose from an operational perspective and supportable in the future. This will mean that:

- Services are capable of being supported from a technical and operational viewpoint with existing (or agreed additional) resources and skills
- There is no adverse impact on other practices, processes or schedules
- There are no unexpected operational costs
- There are no unexpected contractual or legal complications
- There are no complex support paths with multiple support departments or third parties.

9.5 Challenges, critical success factors and risks relating to implementing practices and processes

9.5.1 Challenges

- Lack of engagement with development and project staff. While it is good to have segregation of duties, involving service operations staff at the outset of development projects is good for both teams
- Justifying funding: while it is often difficult to justify expenditure in the area of service operation, in reality, such an investment can show a positive return on investment and improvement in service quality; for example, reduced software license costs and reduced support costs due to fewer incidents
- Challenges for service operation managers, such as differing perspectives of projects and operations, ineffective transitions and managing virtual teams
- Unreasonable targets and timescales, as previously agreed in the SLAs and OLAs
- Normal daily operation or business as usual not having been considered as part of the design
- Poor supplier management and/or poor supplier performance

- Achieving a balance between maintaining a stable production environment and being responsive to the business needs for changing the services
- Insufficient knowledge transfer and training during service transition.

9.5.2 Critical success factors

- Management support
- Business support
- Champions
- Staffing and retention
- Service management training
- Suitable tools
- Validity of testing
- Measurement and reporting

Other CSFs include defining clear accountabilities, roles and responsibilities, establishing a culture that enables knowledge to be shared freely and willingly, demonstrating continual improvements and improved customer and user satisfaction ratings

9.5.3 Risks

- 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 employees, customers and finances
- Resistance to change and circumvention of the processes due to perceived bureaucracy
- Lack of maturity and integration of systems and tools, resulting in people 'blaming' technology for other shortcomings
- Poor integration between the processes, causing process isolation and a silo approach to delivering ITSM.

Additional risks to successful service operation include inadequate funding and resources, loss of key personnel, faulty initial design and differing customer expectations.

9.6 Planning and implementing service management technologies

There are a number of factors to consider when deploying and implementing ITSM support tools:

- Licenses
    - Dedicated licenses
    - Shared licenses
    - Web licenses
    - Service on demand
- Deployment
- Capacity checks
- Timing of technology deployment
- Type of introduction (big bang or phased approach)