ITIL – Introducing service operation

This document is designed to answer many of the questions about IT service management and the ITIL framework, specifically the service operation lifecycle phase. It is a beginner's guide.

ITIL benefits within service operation

- Scalability – ITIL can be adapted for any size of organisation.
- Reduction in costs – ITIL has proven its value in reducing the overall cost of managing services.
- Improved quality – ITIL helps improve the quality of IT services through sound management practices.
- Alignment to standards – ITIL is well aligned to the ISO/IEC 20000 Standard for Service Management.
- Return on Investment (ROI) – ITIL helps IT organisations demonstrate their return on investment and measurable value to the business. This helps establish a business case for new or continuing investment in IT.
- Seamless sourcing partnerships – outsourcing, often with multiple service providers, is increasingly common today and ITIL is widely practised among industry service providers so offers a common practice base for improved service chain management.

Considering cultural change

A small part of the implementation of service operation will be about process design. Most of the challenge lies in cultural change and personal motivation of staff to use the end to end processes as the better way to do deliver service.

Any change leads to feelings of vulnerability and loss of control. These feelings generally manifest themselves through feelings of resistance. The most important thing in this stage of the ITIL implementation is to keep the focus on the reason why your organisation needs ITIL service management in the first place.

Some implementation pointers for implementing service operation

DO:

- Perform a feasibility study first
- Use what is already good in the organisation
- Take it slowly and concentrate on small steps and quick wins
- Appoint a strong project manager with end to end focus to drive the implementation programme
- Keep in mind organisation change management issues
- Keep communicating WHY your organization needs this
- Measure your successes continuously
- Enjoy the milestones and share them with the IT group

DON'T:

- Try to mature all the processes at the same time
- Start with a tool
- Start without management commitment and/or budget
- ITILISE your organisation – it's a philosophy, not an executable application
- Forget to adopt and adapt
- Rush; take your time to do it well
- Go on without a reason
- Ignore the positive activities already in place

The objectives of service operation

The main objective of service operation is to coordinate and carry out the activities and processes required to deliver and manage services at agreed levels to business users and customers.

Service operation is also responsible for ongoing management of the technology that is used to deliver and support services.

Well designed and well implemented processes will be of little value if day to day operation of those processes is not properly conducted, controlled and managed; nor will service improvements be possible if day to day activities to monitor performance, assess metrics and gather data are not systematically conducted during service operation.

Other objectives include:

- Responsive stable services
- Robust end to end operational practices
- Business as usual – day to day
- Execution of processes and services
- Responsive and operational validation
- Realising value
- Achieving service excellence

Value to the organisation of service operation

The operation of service is where these plans, designs and optimisations are executed and measured. From a customer viewpoint, service operation is where actual value is seen.

The scope of service operation

Services

All activities associated with operational services regardless of whether they are executed by the service provider, a third party supplier or by users and customers.

Service management processes

Operational aspects of all processes whatever part of the lifecycle they originate from (e.g. operational aspects of capacity and availability management).

Technology

Management of the technology delivering the services.

People

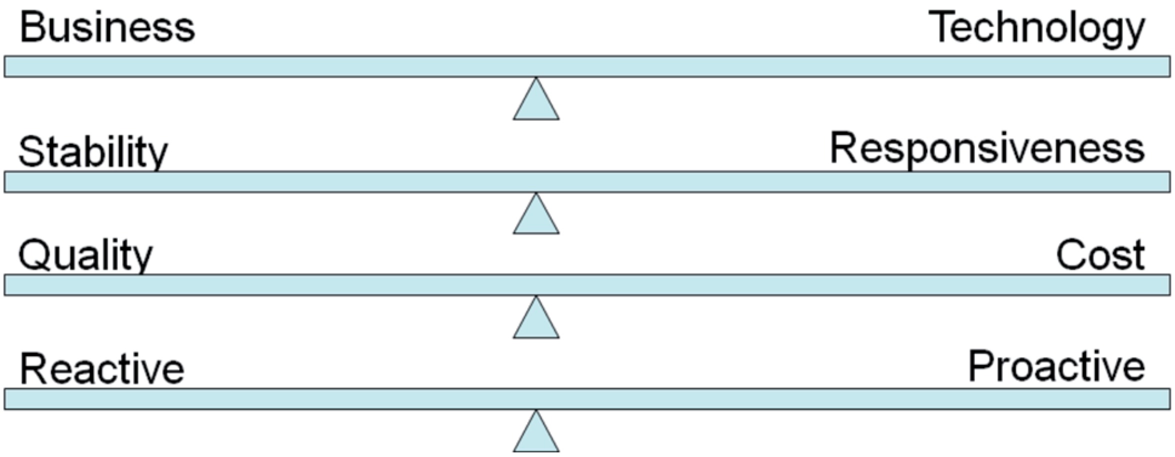
The people managing the services, processes and technology.

Achieving balance in service operation

Conflict arises because constant, agreed levels of service need to be delivered in a continually evolving technical and organisational environment. Getting the balance wrong can mean services are too expensive, unable to meet business requirements, or unable to respond in good time.

Potential areas of conflict are:

- Internal IT vs. external business views
- Stability vs. responsiveness
- Quality of service vs. cost of service
- Reactive vs. proactive



Service operation processes

There are five:

- Request fulfilment
- Incident management
- Problem management
- Access management
- Event management

Request fulfilment

Why have request fulfilment?

Request fulfilment is the process for dealing with service requests via the Service Desk, using a process similar but separate to that of incident management. Request fulfilment records/tables are linked, where necessary, to the incident or problem record(s) that initiated the need for the request.

For a service request, it is normal for some prerequisites to be defined and met (e.g. needs to be proven, repeatable, pre-approved and documented as a procedure).

These are viewed as standard changes – procurement, HR and other business units may assist/be involved.

The objectives of request fulfilment

Request fulfilment is the process of dealing with service requests from the users.

The objectives of the request fulfilment process are:

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

The scope of request fulfilment

The process needed to fulfil a request will vary depending upon exactly what is being requested but can usually be broken down into a set of activities that have to be performed.

Requests can be handled through the incident management processes (and tools) – with service requests being handled as a particular type of incident (using a high level categorisation system to identify service requests). However, there is a significant difference – an incident is an unplanned event whereas a service request is usually something that can and should be planned.

Where large numbers of service requests have to be handled, and where the actions to be taken to fulfil those requests are specialised, it may be appropriate to handle service requests as a completely separate work stream and to record and manage them as a separate record type.

The value to the organisation of request fulfilment

The value of request fulfilment is to provide quick and effective access to standard services, which business staff can use to improve their productivity or the quality of organisation services and products.

Request fulfilment effectively reduces the bureaucracy involved in requesting and receiving access to existing or new services, thereby reducing the cost of providing these services.

The activities of request fulfilment

Menu selection – request fulfilment offers great opportunities for self help practices, where users can generate a service request using technology links into service management tools. Ideally, users should be offered a menu selection via a web interface, so that they can select and input details of service requests from a predefined list.

Financial approval – one important step that is likely to be needed when dealing with a service request is that of financial approval. Most requests will have some form of financial implication, regardless of the type of commercial arrangements in place. The cost of fulfilling the request must first be established. It may be possible to agree fixed prices for standard requests – and prior approval for such requests may be given as part of the organisation's overall annual financial management. In all other cases, an estimate of the cost must be produced and submitted to the user for financial approval. If approval is given, in addition to fulfilling the request, the process must also include charging for the work done – if charging is in place.

Other approval – in some cases further approval may be needed – such as compliance related, or wider business approval. Request fulfilment must have the ability to define and check such approvals where needed.

Fulfilment – the actual fulfilment activity will depend upon the nature of the service request. Some simpler requests may be completed by the Service Desk, acting as the first line of support, while others have to be forwarded to specialist groups and/or suppliers for fulfilment. The Service Desk will monitor and chase progress and keep users informed throughout, regardless of the actual fulfilment source.

Closure – when the service request has been fulfilled it must be referred back to the Service Desk for closure – the Service Desk will check that the user is satisfied with the outcome.

Incident management

Why have incident management?

Incident management is highly visible to the organisation, and it is therefore easier to demonstrate its value than in most areas of service operation. For this reason, incident management is often one of the first processes to be implemented in service management projects. The added benefit of doing this is that incident management can be used to highlight other areas that need attention, thereby providing a justification for implementing other ITIL processes.

The objectives of incident management

To restore normal service operation as quickly as possible and minimise the adverse impact of the Incident on business operations, thus ensuring that the best possible levels of service quality and availability are maintained.

Normal service operation is defined here as service operation within Service Level Agreement limits.

The scope of incident management

Incident management includes any event which disrupts, or which could disrupt, a service. This includes events which are communicated directly by users, either through the Service Desk or through an interface from event management to incident management tools.

Incidents can also be reported and/or logged by technical staff (if, for example, they notice something untoward with a hardware or network component they may report or log an incident and refer it to the Service Desk). This does not mean, however, that all events are Incidents. Many classes of event are not related to disruptions at all, but are indicators of normal operation or are simply informational (see event management).

The value to the organisation of incident management

- The ability to detect and resolve Incidents which results in lower downtime for the organisation, which in turn means higher availability of the service.
- The ability to align IT activity to real time business priorities. This is because incident management includes the capability to identify business priorities and dynamically allocate resources as necessary.
- The ability to identify potential improvements to services. This happens as a result of understanding what constitutes an incident and also from being in contact with the activities of business operational staff.
- The Service Desk can, during its handling of incidents, identify additional service or training requirements found in IT or the business.

The activities of incident management

Incident identification and logging (Service Desk responsibility)

- Record basic details of the incident
- Alert specialist support group(s) as necessary

Categorisation, prioritisation and initial diagnosis

- Categorise incidents
- Assign impact and urgency, and thereby define priority
- Match against known errors and problems
- Inform problem management of the existence of new problems and of unmatched or multiple incidents
- Assess related configuration details (daily verification)
- Provide initial support (assess Incident details, find quick resolution)
- Close the incident or route it to a specialist support group, and inform the user(s)

Investigation and diagnosis

- Assess the incident details
- Collect and analyse all related information, and resolve, (including any work around) or route to online support
- Escalate (functionally or hierarchically) where necessary

Resolution and recovery

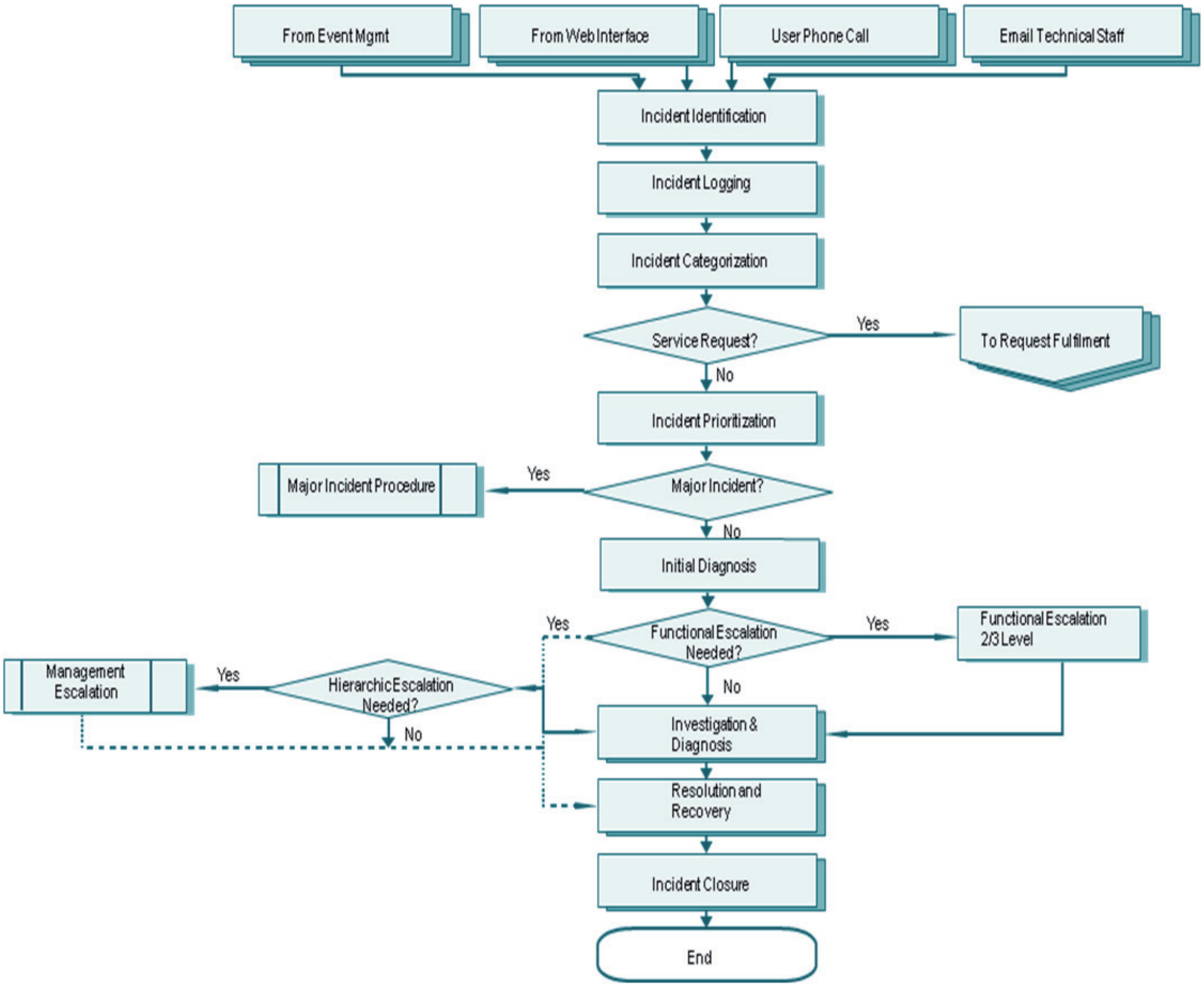
- Resolve the incident using the solution/work around or, alternatively, raise a request for change (RFC) (including a check for resolution)
- Take recovery actions

Incident closure (Service Desk responsibility)

- When the Incident has been resolved, the Service Desk should ensure that:
  - Details of the action taken to resolve the incident are concise and readable
  - Classification is complete and accurate according to root cause
  - Resolution/action is agreed with the customer – verbally or, preferably, by email or in writing
- All details applicable to the incident are recorded, such that:
  - The customer/user is satisfied
  - Cost centre project codes are allocated
  - The time spent on the incident is recorded
  - The person, date and time of closure are recorded

Note – service requests and major incidents have their own process

The incident management process diagram



The terminology of incident management

Incident – unplanned interruption to or reduction in quality of IT service

Functional escalation – escalation across IT to subject matter experts

Hierarchical escalation – involves more senior levels of management – usually for decision making

Work around – a temporary fix for the incident

A major incident – an Incident which has high impact on the organisation and for which a separate process exists

Problem management

Why have problem management?

Failure to halt the recurrence of incidents or understand the root cause of major incidents leads to lost time, loss of productivity and frustrated users.

Effective problem management halts the recurrence of incidents and has benefits to the individual and the organisation as a whole as it improves availability (up time) and user productivity.

The objectives of problem management

The objective of problem management is to minimise the adverse impact of incidents and problems on the business that are caused by errors within the IT infrastructure, and to prevent recurrence of incidents related to these errors.

The scope of problem management

Problem management includes the activities required to diagnose the root cause of incidents and to determine the resolution to the problems. It is also responsible for ensuring that the resolution is implemented through the appropriate control procedures (change management).

Problem management will also maintain information about problems and the appropriate work arounds and resolutions, so that the organisation is able to reduce the number and impact of Incidents over time. In this respect problem management has a strong interface with knowledge management, and tools such as the Known Error Database will be used for both. The Known Error Database is a hugely effective tool at the Service Desk and is used in early resolution of incidents.

Although incident and problem management are separate processes, they are closely related and will typically use the same tools, and may use similar categorisation, impact and priority coding systems. This will ensure effective communication when dealing with related incidents and problems.

The value to the organisation of problem management

Problem management works together with incident management and change management to ensure that IT service availability and quality are increased.

When incidents are resolved, information about the resolution is recorded. Over time, this information is used to speed up the resolution time and identify permanent solutions, reducing the number and resolution time of incidents. This results in less down time and less disruption to business critical systems.

Additional value from problem management is derived from the following:

- Higher availability of IT services
- Higher productivity of business and IT staff
- Reduced expenditure on work arounds or fixes that do not work
- Reduction in cost of effort in fire fighting or resolving repeat incidents

The activities of problem management

Problem Management consists of two major processes:

- **Reactive problem management** – generally executed as part of service operation
- **Proactive problem management** – initiated in service operation, but generally driven as part of continual service improvement

The reactive activities are:

Problem detection and problem logging

- Use incident guidelines for problem identification
- Other processes (e.g. availability, security) could log problems prior to incident occurring

Problem categorisation and prioritisation

- Categorise the problem by IT functional area
- Assess urgency and impact to assign priority

Problem investigation and diagnosis

- Assign to IT functional area for further investigation

Workarounds and raising a known error record

- In cases where a work around is found, it is important that the problem record remains open, and details of the work around are documented within the problem record
- As soon as the diagnosis is complete, and particularly where a work around has been found (even though it may not be a permanent resolution), a known error record must be raised and placed in the Known Error Database, so that, if further incidents or problems arise, they can be identified and the service restored more quickly

Problem resolution

- Problem record closed when known error located and work around identified

Problem closure

- Problem record closed when known error located and work around identified

The proactive activities are:

Major problem review and errors detected in the development environment

After every major problem, and while memories are still fresh, a review should be conducted to learn any lessons for the future. Specifically the review should examine:

- Those things that were done correctly
- Those things that were done wrongly
- What could be done better in the future
- How to prevent recurrence
- Whether there has been any third party responsibility and whether follow up actions are needed

Such reviews can be used as part of training and awareness activities for staff – any lessons learned should be documented in appropriate procedures, working instructions, diagnostic scripts or known error records.

Tracking and monitoring

The Service Desk Manager owns/is accountable for ALL incidents. Tracking and monitoring takes place throughout all of the other activities.

Trend analysis

- Review reports from other processes (e.g. incident management, availability management, change management)
- Identify recurring problems or training opportunities.

Targeting preventative action

- Perform a cost benefit analysis of all costs associated with prevention.
- Target specific areas taking up most attention.

The terminology of problem management

Problem – unknown, underlying cause of incident(s)

Known error – known, underlying cause of incident(s) and a work around identified

Work around – temporary resolution

Proactive problem management – removal of current/potential errors before they cause problems

Access management

Why have access management?

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

The objectives of access management

- Protecting Confidentiality, Integrity and Availability (CIA), sometimes know as Rights Management or Identity Management (removing access when people change roles or jobs and regularly auditing access permissions to ensure they are correct)
- Security incidents and problems related to access management will be discreetly recorded

The scope of access management

Access management is effectively the execution of both availability and information security management, in that it enables the organisation to manage the confidentiality, availability and integrity of the organisation's data and intellectual property.

Access management ensures that users are given the right to use a service, but it does not ensure that this access is available at all agreed times – this is provided by availability management.

Access management can be initiated by a service request through the Service Desk.

The value to the organisation of access management

Access management provides the following value:

- Controlled access to services ensures that the organisation is able to maintain more effectively the confidentiality of its information
- Employees have the right level of access to execute their jobs effectively
- There is less likelihood of errors being made in data entry or in the use of a critical service by an unskilled user (e.g. production control systems)
- The ability to audit use of services and to trace the abuse of services
- The ability more easily to revoke access rights when needed – an important security consideration
- May be needed for regulatory compliance

The activities of access management

Requesting access – access can be requested using one or any number of mechanisms, for example:

- A standard request
- A request for change
- A service request (submitted via the request fulfilment system)
- Executing a pre-authorised script or option
- Rules for requesting access are normally documented as part of the service catalogue

Verification – access management needs to verify every request for access to an IT service from two perspectives:

- That the user requesting access is who they say they are
- That they have a legitimate requirement for that service

Providing rights – access management does not decide who has access to which IT services. access management executes the policies and regulations defined during service strategy and service design. Access management enforces decisions to restrict or provide access, rather than making the decision. As soon as a user is verified, access management will provide that user with rights to use the requested service. In most cases this will result in a request to every team or department involved in supporting that service to take the necessary action. Ideally, these tasks should be automated.

Monitoring identity status – as users work in the organisation, their roles change as do their needs to access services, e.g. job changes, promotions/demotions, resignation or death. Access management should understand and document the typical user lifecycle for each type of user and use it to automate the process. Access management tools should provide features that enable a user to be moved from one state to another or from one group to another, easily and with an audit trail.

Logging and tracking access – access management should not only respond to requests. It is also responsible for ensuring that the rights that have been provided are being properly used. Information security management plays a vital role in detecting unauthorized access and comparing it with the rights that were provided by access management. Access management may also be required to provide a record of access for specific services during forensic investigations. If a user is suspected of breaches of policy, inappropriate use of resources, or fraudulent use of data, access management may be required to provide evidence of dates, times and even content of that user's access to specific services.

Removing or restricting rights – Just as access management provides rights to use a service, it is also responsible for revoking those rights. Again, this is not a decision that it makes on its own. Access management will execute the decisions and policies made during service strategy and design and also decisions made by managers within the organisation. Removing access is usually done in the following circumstances:

- Death
- Resignation
- Dismissal
- User has changed roles etc.

The terminology of access management

Access – refers to the level and the extent of a service's functionality or data to which a user is entitled.

Identity – refers to the information about the user that distinguishes them as an individual and which verifies their status within the organisation. By definition, the identity of a user is unique to that user.

Rights – (also called privileges) refer to the actual settings whereby a user is provided access to a service or group of services. Typical rights, or level of access, include read, write, execute, change and delete.

Service or service groups – most users do not use only one service, and users performing a similar set of activities will use a similar set of services. Instead of providing access to each service for each user separately, it is more efficient to be able to grant each user, access to the whole set of services that they are entitled to use at the same time.

Directory services – refers to a specific type of tool that is used to manage access and rights.

Event management

Why have event management?

An event can be defined as any detectable or discernable occurrence that has significance for the management of the IT infrastructure or the delivery of IT service, and evaluation of the impact a deviation might cause to the service. Events are typically notifications created by an IT service, configuration item or monitoring tool. Effective service operation is dependent on knowing the status of the infrastructure and detecting any deviation from normal or expected operation. This is provided by good monitoring and control systems, which are based on two types of tools:

- Active monitoring tools that poll key configuration items to determine their status and availability. Any expectations will generate an alert that needs to be communicated to the appropriate tool or team for action
- Passive monitoring tools that detect and correlate operational alerts or communications generated by configuration items

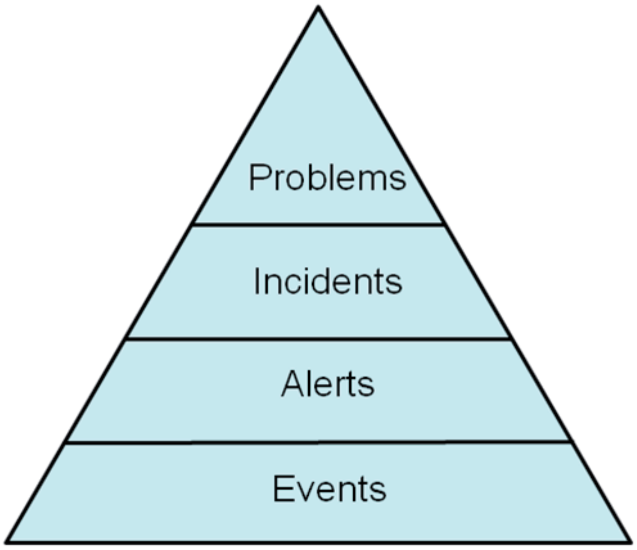
The objectives of event management

To provide the entry point for the execution of many service operation processes and activities. In addition, it provides a way of comparing actual performance and behaviour against design standards and Service Level Agreements.

Other objectives:

- Provides the ability to detect, interpret and initiate appropriate action for events
- Is the basis for operational monitoring and control and the entry point for many service operation activities
- Provides operational information as well as warnings and exceptions to aid automation
- Supports continual service improvement activities of service assurance and reporting

> *“A change of state that has significance for the management of a configuration item or IT service”*



It is **unusual for an organisation to appoint an ‘Event Manager’,** as events tend to occur in multiple contexts and for many different reasons. However, it is important that Event Management procedures are coordinated to prevent duplication of effort and tools

The scope of event management

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

- Configuration Items:
  - Some configuration items will be included because they need to stay in a constant state
  - Some configuration items will be included because their status needs to change frequently and event management can be used to automate this and update the configuration management system
- Environmental conditions (e.g. fire and smoke detection)
- Software licence monitoring for usage to ensure optimum/legal licence utilisation and allocation
- Security (e.g. intrusion detection)
- Normal activity (e.g. tracking the use of an application or the performance of a server)

The value to the organisation of event management

Event management's value to the organisation is generally indirect; however, it is possible to determine the basis for its value as follows:

- Event management provides mechanisms for early detection of incidents. In many cases, it is possible for the incident to be detected and assigned to the appropriate group for action before any actual service outage occurs.
- Event management makes it possible for some types of automated activity to be monitored by exception – thus removing the need for expensive and resource – intensive, real time monitoring, while reducing down time.
- When integrated into other service management processes (such as, for example, availability or capacity management), event management can signal status changes or exceptions that allow the appropriate person or team to respond promptly, thus improving the performance of the process. This, in turn, will allow the business to benefit from more effective and more efficient service management overall.
- Event management provides a basis for automated operations, thus increasing efficiencies and allowing expensive human resources to be used for more innovative work, such as designing new or improved functionality or defining new ways in which the business can exploit technology for increased competitive advantage.

The activities of event management

Event occurs – events occur continuously, but not all of them are detected or registered. It is therefore important that everybody involved in designing, developing, managing and supporting IT services and the IT infrastructure that they run on understands what types of event need to be detected.

Event notification – most configuration items are designed to communicate certain information about themselves in one of two ways:

- A device is interrogated by a management tool, which collects certain targeted data. This is often referred to as polling.
- The configuration item generates a notification when certain conditions are met. The ability to produce these notifications has to be designed and built into the configuration item, for example, a programming hook inserted into an application.

Event detection – once an event notification has been generated, it will be detected by an agent running on the same system, or transmitted directly to a management tool specifically designed to read and interpret the meaning of the event.

Event filtering – the purpose of filtering is to decide whether to communicate the event to a management tool or to ignore it. If ignored, the event will usually be recorded in a log file on the device, but no further action will be taken.

Significance of events – every organisation will have its own categorisation of the significance of an event, but it is suggested that at least these three broad categories be represented:

- **Informational**: this refers to an event that does not require any action and does not represent an exception. They are typically stored in the system or service log files and kept for a predetermined period
- **Warning**: a warning is an event that is generated when a service or device is approaching a threshold warnings are intended to notify the appropriate person, process or tool so that the situation can be checked and appropriate action taken to avoid an exception
- **Exception**: an exception means that a service or device is currently operating abnormally. Typically this means that an Operating Level Agreement or Service Level Agreement has been breached and the business has been impacted. Exceptions could represent a total failure, impaired functionality or degraded performance.

Event correlation – if an event is significant, a decision has to be made about exactly what the significance is and what actions need to be taken to deal with it. It is here that the meaning of the event is determined.

Trigger – if the correlation activity recognises an event, a response will be required. The mechanism used to initiate that response is also called a trigger. There are many different types of triggers, each designed specifically for the task it has to initiate. Some examples:

- Incident triggers that generate a record in the incident management system
- Change triggers that generate an request for change
- A trigger resulting from an approved request for change that has been implemented but caused the event, or from an authorised change that has been detected
- Scripts that execute specific actions
- Paging systems that will notify a person or team of an event
- Database triggers that restrict access of a user to specific records or fields, or that create or delete entries in the database

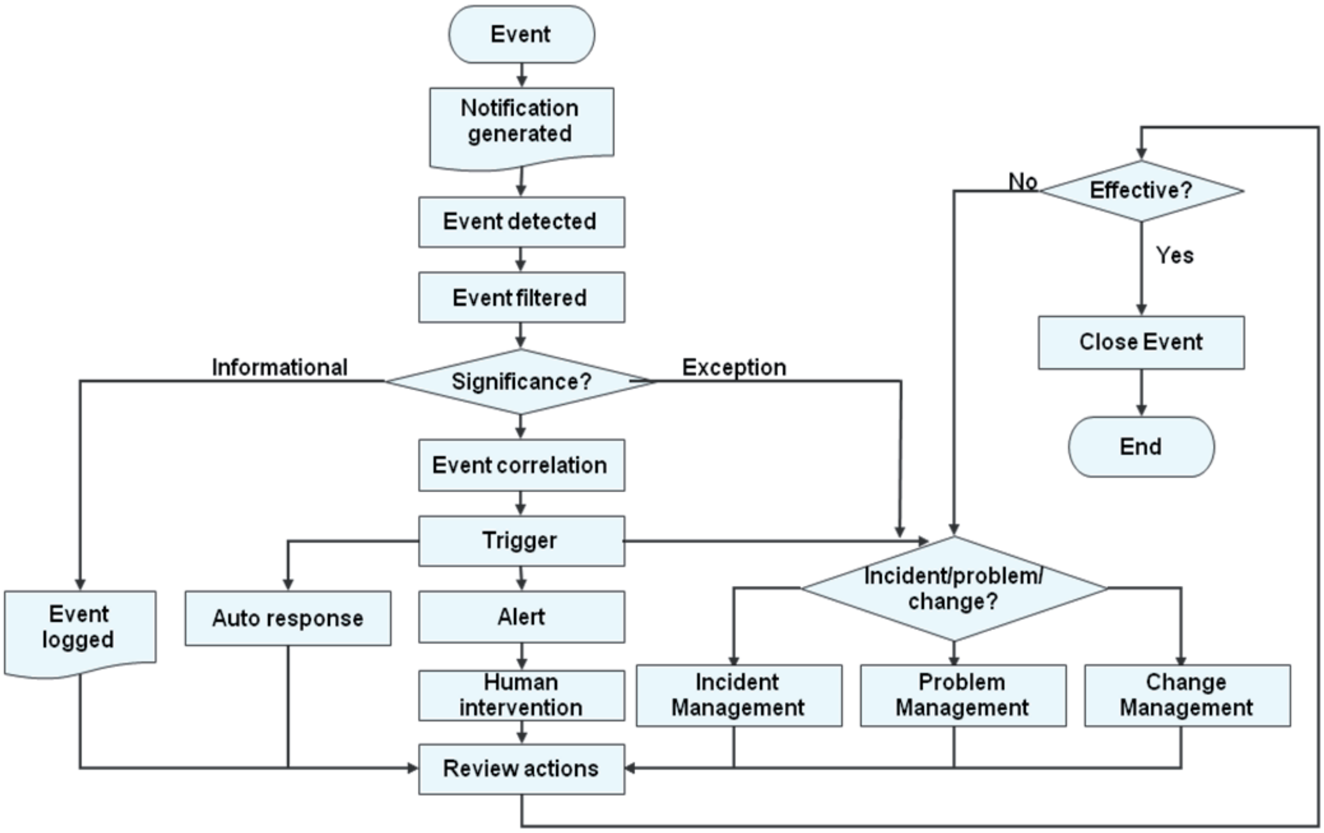
Response selection – at this point of the process, there are a number of response options available:

- Event logged – there will be a record of the event and any subsequent actions.
- Auto response – some events are understood well enough that the appropriate response has already been defined and automated. This is normally a result of good design or previous experience (within problem management). The trigger will initiate the action and then evaluate whether it was completed successfully. If not, an incident or problem record will be created. Examples of auto responses include: rebooting a device, restarting a service, locking a device or application to protect it against unauthorised access.
- Alert and human intervention – if the event requires human intervention, it will need to be escalated. The purpose of the alert is to ensure that the person with the skills appropriate to deal with the event is notified. The alert will contain all the information necessary for the person to determine the appropriate action.
- Incident, problem or change? Some events will represent a situation where the appropriate response will need to be handled through the incident, problem or change management process.
- Open a request for change.
- Open an incident record – as with a request for change an incident can be created as soon as an exception is detected, or when the correlation engine determines that a specific type or combination of events represents an incident.
- Open or link to a problem record – it is rare for a problem record to be opened without related incidents. In most cases this step refers to linking an incident to an existing problem record. This will assist the problem management teams to reassess the severity and impact of the problem, and may result in a changed priority to an outstanding problem.
- Special types of incident – in some cases an event will indicate an exception that does not directly impact any IT service, e.g. unauthorized entry to a data centre. In this case the incident will be logged using an incident model that is appropriate for this type of exception, e.g. a security incident. The incident should be escalated to the group that manages that type of incident. As there is no outage, the incident model used should reflect that this was an operational issue rather than a service issue. These incidents should not be used to calculate downtime, and can in fact be used to demonstrate how proactive IT has been in making services available.

Review actions – as thousands of events are generated on a daily basis, it is not possible to review every one. However, it is important to check that any significant events or exceptions have been handled appropriately, or to track trends or counts of event types, etc. In many cases this can be done automatically.

Close event – Some events will remain open until a certain action takes place, for example, an event that is linked to an open incident. However, most events are not opened or closed. Informational events are simply logged and then used as input to other processes, such as backup and storage management. Auto response events will typically be closed by the generation of a second event. For example, a device generates an event and is rebooted through auto response – as soon as that device is successfully back online, it generates an event that effectively closes the loop and clears the first event.

The event management process



The terminology of event management

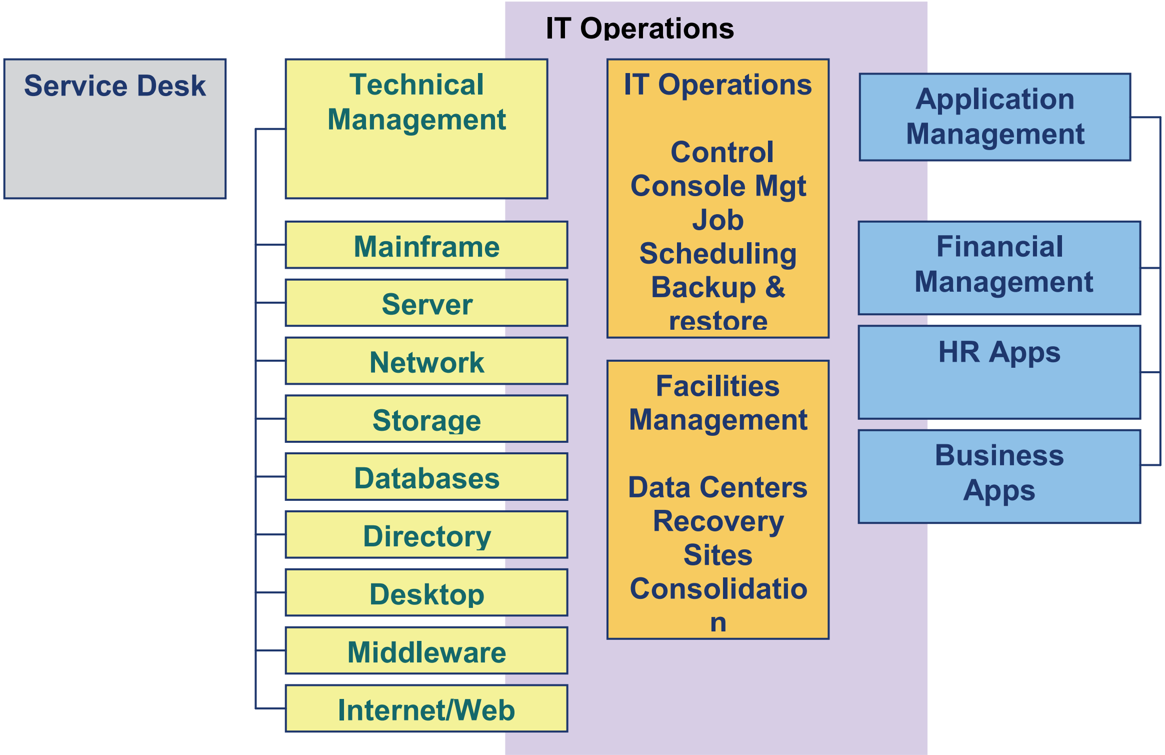
Event – a change of state that has significance for the management of a configuration item or IT service.

Trigger – an indication that some action or response to an event may be needed.

Alert – a warning that a threshold has been reached or something has been changed. (An event has occurred).

Service operation functions

- Service Desk (see separate documents)
- Technical management
- Applications management
- IT operations management



The technical management function

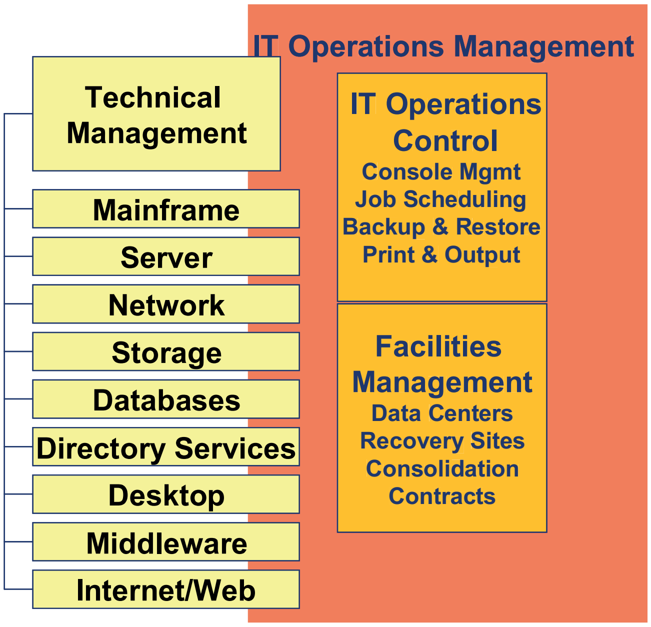
Why have a technical management function?

As the custodian of technical knowledge and expertise related to managing the IT infrastructure, the technical management function provides detailed technical skills and resources needed to support the ongoing operation of the IT infrastructure. Technical management also plays an important role in providing the actual resources to support the IT service management lifecycle, and ensures resources are effectively trained and deployed to design, build, transition, operate and improve the technology to deliver and support IT services.

The objectives of the technical management function?

Help plan, implement and maintain a stable technical infrastructure to support the organisation's business processes through:

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



Technical management groups:

- Act as guardians of technical knowledge and expertise relating to the Infrastructure
- Hold knowledge of designing, testing, building, managing and improving IT services
- Provide resources to assist in IT service management lifecycle
- Ensure these resources are trained and deployed to design, build, transition operate and improve the technology to support IT
- Design a resilient, cost effective infrastructure configuration
- Maintain the infrastructure
- Provide support during technical failures

The activities of the technical management function

In all but the smallest organisations, where a single, combined team may suffice, separate teams will be needed for each type of infrastructure being used. In many organisations the technical management teams are also responsible for the daily operation of a subset of the IT infrastructure.

Technical management will provide guidance to IT operations about how best to carry out the ongoing operational management of technology. This will partly be provided during the service design process, but there will also be everyday communication with IT operations, as they seek to achieve stability and optimum performance.

The technical management function will be made up of specialist technical architects and designers (primarily involved during the service design phase) and specialist maintenance and support staff (primarily involved in the service operation phase).

Technical teams are usually aligned to the technology they manage and can include operational activities.

Examples:

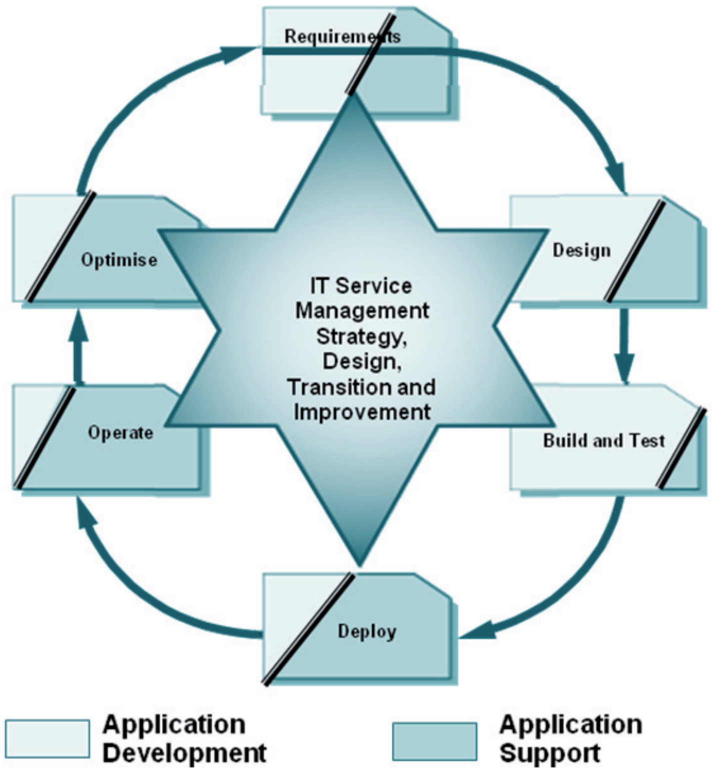
- Mainframe management
- Server management
- Internet/web management
- Network management
- Database administration
- Desktop support
- Middleware
- Storage

The application management function

Why have the application management function?

Application management is responsible for managing applications throughout their lifecycle.

By supporting and maintaining operational applications, applications management plays an important role in the design, testing and improvement of applications that form part of IT services.



Applications management supports the business processes by:

- Identifying functional and manageability requirements
- Assisting in design and deployment
- Providing ongoing support and improvement

Objectives are achieved by:

- Good design of resilient and cost effective applications
- Functionality to meet the business requirements
- Technical skills being available to ensure applications perform optimally and any incidents are resolved in good time

The objectives of the application management function

Application management ensures that resources are effectively trained and deployed to design, build, and transition, operate and improve the technology required to deliver and support IT services.

By performing this role, application management is able to ensure that the organisation has access to the right type and level of human resources to manage applications, and therefore meets business objectives. This starts in service strategy and is expanded in service design, tested in service transition and refined in continual service improvement.

Application management:

- Is responsible for applications throughout their lifecycle
- Ensures appropriate roles – Applications Managers/Team Leaders, Applications Analysts/Architects
- Ensures availability of functionality
- Maintains operational applications
- Provides support during application failures

The activities of the application management function

While most application management teams are dedicated to specific applications or sets of applications, there are a number of activities which they have in common, for example:

- Identifying the knowledge and expertise required to manage and operate applications in the delivery of IT services
- Initiating training programs to develop and refine the skills in the appropriate application management resources and maintaining records for these resources
- Recruiting or contracting resources with skills that cannot be developed internally, or where there are insufficient numbers of staff to perform the required activities
- Designing and delivering end user training
- Researching and developing solutions that can help expand the service portfolio
- Ensuring all system documentation is up to date and complete and that relevant staff are familiar with the contents etc.

The IT operations management function

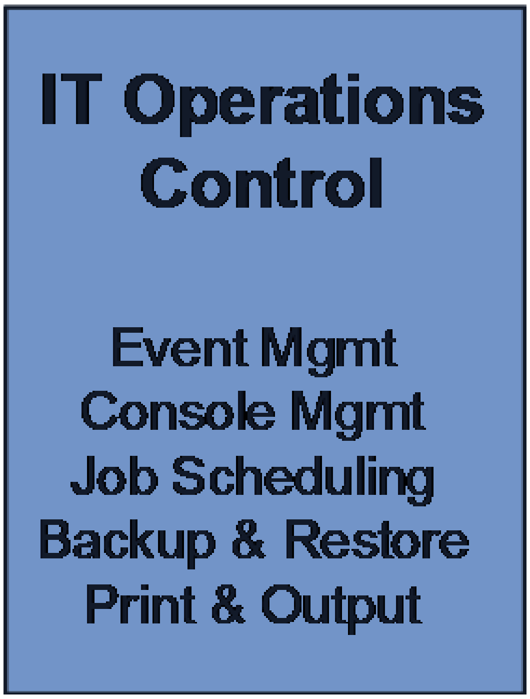
Why have the IT operations management function

IT operations is the function responsible for the daily operational activities needed to manage the IT infrastructure. This is done according to the performance standards defined during service design.

In some organisations this is a single, centralised team, while in others some activities and staff are centralised and some are provided by distributed and specialized departments.

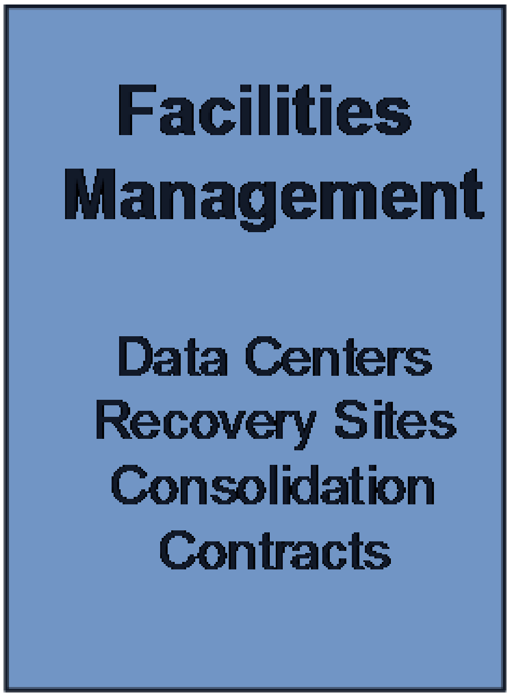
The objectives of IT operations management

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



IT Operations Control

Event Mgmt
Console Mgmt
Job Scheduling
Backup & Restore
Print & Output



Facilities Management

Data Centers
Recovery Sites
Consolidation
Contracts

The activities of the IT operations management function

IT operations management has two unique functions, which are usually organised in the following structure:

IT operations control: generally staffed by shifts of operators, ensures that routine operational tasks are carried out. Also provides centralised monitoring and control activities, usually using an Operations Bridge or Network Operations Centre, e.g. console management, job scheduling, backup and restore etc.

Facilities management: management of the physical IT environment, usually data centres or computer rooms. In some organisations, many physical components have been outsourced and facilities management may include the management of the outsourcing contracts, e.g. data centres, recovery sites, contracts etc.