IT 495
Selected Topics in Information Technology-1

IT Service Analysis, Design, and Operation

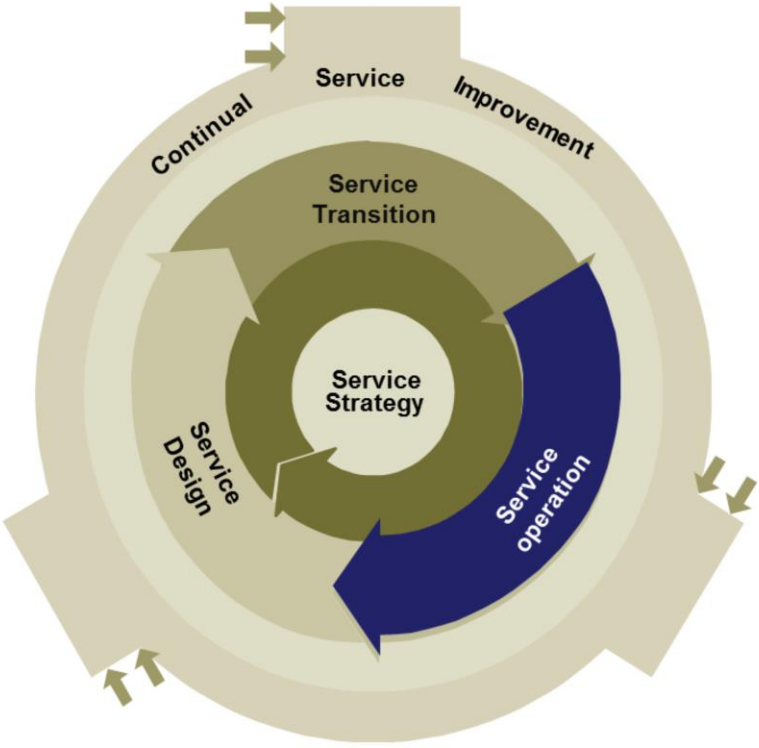
Part 5: Service Operation

Haitham S. Hamza, Ph.D.
Cairo University
Spring 2023

Acknowledgment

- Slides are based on the ITIL® Foundation Course developed by the Software Engineering Competence Center (SECC).
- All ITIL® Figures are © OGC's Official Accreditor - The APM Group Limited 2008
- I have modified them and added new slides

Service Life-Cycle



Contents

Introduction

Service Operation – Purpose

- Coordinate and carry out the activities and processes required to deliver and manage services at agreed levels to business users and customers
- Service operation is also responsible for the ongoing management of the technology that is used to deliver and support services

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

Service operation is a critical stage of the service lifecycle. Well-planned and well-implemented processes will be to no avail if the 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 operational data are not systematically conducted during service operation.

Staff involved in the service operation stage of the service lifecycle should have processes and support tools in place that allow them to have an overall view of service operation and delivery (rather than just the separate components, such as hardware, software applications and networks, that make up the end-to-end service from a business perspective). These processes and tools should also detect any threats or failures to service quality.

As services may be provided, in whole or in part, by one or more partner/supplier organizations, the service operation view of the end-to-end service should be extended to encompass external aspects of service provision. When necessary, shared or interfacing processes and tools should be deployed to manage cross-organizational workflows.

Service Operation – Objectives

- Maintain business satisfaction and confidence in IT through effective and efficient delivery and support of agreed IT services
- Minimize the impact of service outages on day-to-day business activities
- Ensure that access to agreed IT services is only provided to those authorized to receive those services

The objectives of service operation are to:

- Maintain business satisfaction and confidence in IT through effective and efficient delivery and support of agreed IT services
- Minimize the impact of service outages on day-to-day business activities
- Ensure that access to agreed IT services is only provided to those authorized to receive those services.

Service Operation – Processes

- Event Management
- Incident Management
- Request Fulfillment
- Problem Management
- Access Management

Event management

Event management manages events throughout their lifecycle. This lifecycle includes coordination activities to detect events, make sense of them and determine the appropriate control action.

Incident management

Incident management concentrates on restoring unexpectedly degraded or disrupted services to users as quickly as possible, in order to minimize business impact.

Problem management

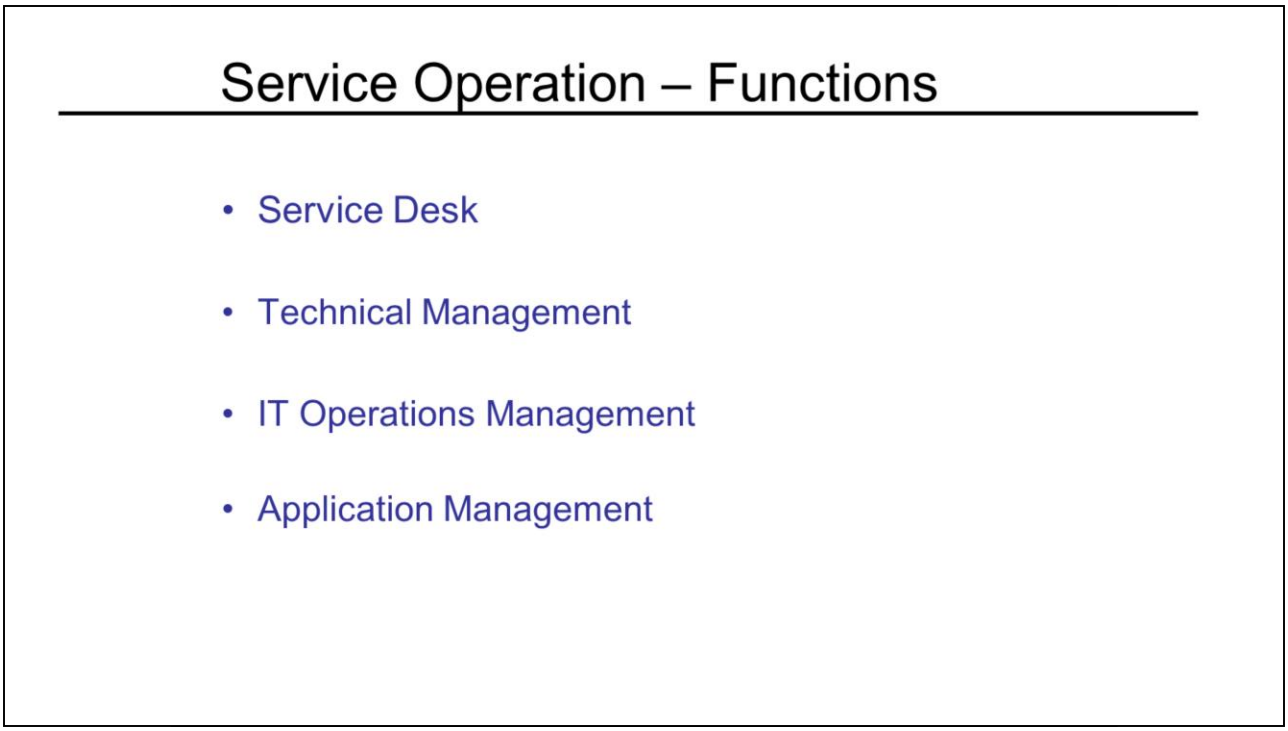
Problem management involves root cause analysis to determine and resolve the underlying causes of incidents, and proactive activities to detect and prevent future problems/incidents. This also includes the creation of known error records that document root causes and workarounds to allow quicker diagnosis and resolution should further incidents occur.

Request fulfilment

Request fulfilment is the process for managing the lifecycle of all service requests. Service requests are managed throughout their lifecycle from initial request to fulfilment using separate request fulfilment records/tables to record and track their status.

Access management

Access management is the process of granting authorized users the rights to use a service, while restricting access to non-authorized users. It is based on being able accurately to identify authorized users and then manage their ability to access services as required for their specific organizational role or job function. Access management has also been called identity or rights management in some organizations. It should fully support the policies designed in the information security management process with respect to roles, rights and segregation of duties.



Processes alone will not result in effective service operation. A stable infrastructure and appropriately skilled people are needed as well. To achieve this, service operation relies on several functions to execute operational tasks. Functions include groups of skilled people who carry out one or more service lifecycle processes and activities. Within service operation, there are four main functions:

Service desk: The service desk is the single point of contact for users when there is a service disruption, for service requests, or even for some categories of RFC. The service desk provides a point of communication to the users and a point of coordination for several IT groups and processes.

Technical management: provides detailed technical skills and resources needed to support the ongoing operation of IT services and the management of the IT infrastructure. Technical management also plays an important role in the design, testing, release and improvement of IT services. In small organizations, it is possible to manage this expertise in a single department, but larger organizations are typically split into a number of technically specialized departments.

IT operations management: IT operations management executes the daily operational activities needed to manage IT services and the supporting IT infrastructure. This is done according to the performance standards defined during service design. In some organizations this is a single, centralized department, while in others some activities and staff are centralized and some are provided by distributed or specialized departments. IT operations management has two sub-functions that are unique and are generally organizationally distinct. These are:

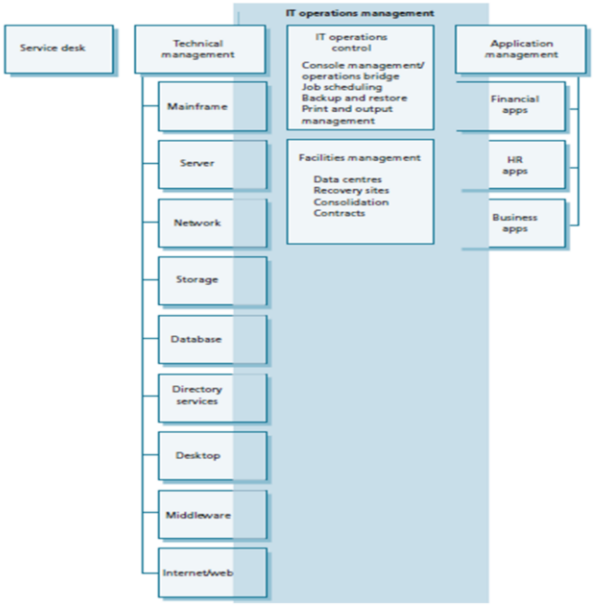
> **IT operations control**: generally staffed by shifts of operators and which ensures that routine operational tasks are carried out. IT operations control will also provide centralized monitoring and control activities, usually using an operations bridge or network operations centre.
>
> **Facilities management**: refers to the management of the physical IT environment, usually data centres or computer rooms. In many organizations technical and application management are co-located with IT operations in large data centres.

Application management: responsible for managing applications throughout their lifecycle. The application management 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. ITIL views application management differently from application development. Within IT, application development is typically focused around internal activities to design, build, test and deploy IT solutions being constructed within the IT organization. Application management takes a much broader view that recognizes the capabilities in today's marketplace to obtain applications from many sources other than the internal IT organization. In addition, it also focuses on the ongoing management and maintenance of applications that takes place once applications have been deployed.

Service Management Functions

Service Operation 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.



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.

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

For service operation to be successful, an organization will need to clearly define the roles and responsibilities required to undertake the processes and activities identified in Chapters 4 and 5. These roles will need to be assigned to individuals, and an appropriate organization structure of teams, groups or functions established and managed.

The Service Operation functions shown in the figure are needed to manage the 'steady state' operational IT environment. These are logical functions and do not necessarily have to be performed by an equivalent organizational structure. This means that Technical and Application Management can be organized in any combination and into any number of departments. The second-level groupings in the figure are examples of typical groups of activities performed by Technical Management and are not a suggested organization structure.

Service Desk

- The service desk represents the single point of contact for users on a day-by-day basis – and will handle all incidents and service requests.
- Goal: The primary aim of the Service Desk is to get the 'normal service' restored to the users as quickly as possible:
  - resolving incidents or fulfilling a service request or answering a query
- It is very important to assign correct caliber of staff to the Service Desk
  - poor Service Desk can give a poor impression of an otherwise very effective IT organization!

A Service Desk is a functional unit made up of a dedicated number of staff responsible for dealing with a variety of service events, often made via telephone calls, web interface, or automatically reported infrastructure events.

The Service Desk is a vitally important part of an organization's IT Department and should be the single point of contact for IT users on a day-by-day basis – and will handle all incidents and service requests, usually using specialist software tools to log and manage all such events. The value of an effective Service Desk should not be underrated – a good Service Desk can often compensate for deficiencies elsewhere in the IT organization; but a poor Service Desk (or the lack of a Service Desk) can give a poor impression of an otherwise very effective IT organization!

It is common practice that the Service Desk provides 'entry-level' positions for ITSM staff. Working on the Service Desk is an excellent 'grounding' for anyone who wishes to pursue a career in Service Management. However, this could also present challenges with people who do not understand the business or technology. Users calling the Service Desk should be able to speak to someone who is able to address their needs, and Service Desk Analysts should not be burned out in less than a year because of undue stress. Care should be taken to select appropriately skilled individuals with a good understanding of the business and to provide adequate training – thus preventing reduction in levels of support due to a lack of knowledge at the first line. It is therefore very important that the correct caliber of staff used on the Service Desk and that IT Managers do their best to make the desk an attractive place to work to improve staff retention.

In alignment to customer and business requirements, the IT organization's senior managers should decide the exact nature of its required Service Desk (and whether it should be internal or outsourced to a third party) as part of its overall ITSM strategy– and then subsequent planning must be done to prepare for and then implement the appropriate Service Desk.

Service Desk – Responsibilities

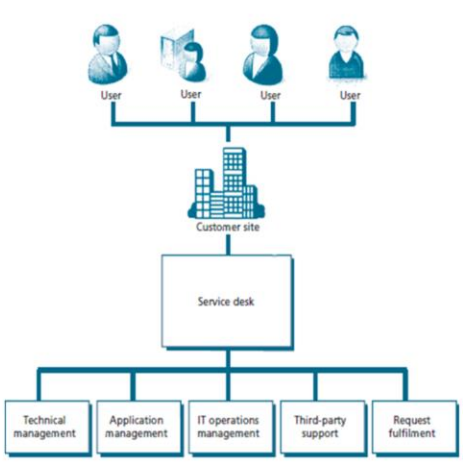
- Logging all relevant incident/service request details, allocating categorization and prioritization codes
- Providing first-line investigation and diagnosis
- Resolving those incidents/service requests
- Escalating incidents/service requests within agreed timescales
- Closing all resolved incidents, requests and other calls
- Conducting customer/user satisfaction call-backs/surveys
- Communication with users:
  - keeping them informed of incident/service requests progress,
  - notifying them of impending changes or agreed outages, etc.
- Updating the CMS under the direction and approval of Configuration Management if so agreed.

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, and also handles communication with the users. Service desk staff execute the incident management and request fulfilment processes to restore the normal-state service operation to the users as quickly as possible. In this context 'restoration of service' is meant in the widest possible sense. While this could involve fixing a technical fault, it could equally involve fulfilling a service request or answering a query – anything that is needed to allow the users to return to working satisfactorily.

Service Desk – Structures

- There are many ways of structuring Service Desks and locating them. For example:
  - Local Service Desk
  - Centralized Service Desk
  - Virtual Service Desk
  - Follow the Sun
  - Specialized Service Desk groups
- In reality, a structure that combines a number of the above options may be needed in order to fully meet the business needs

Service Desk Structures – *Local Service Desk*

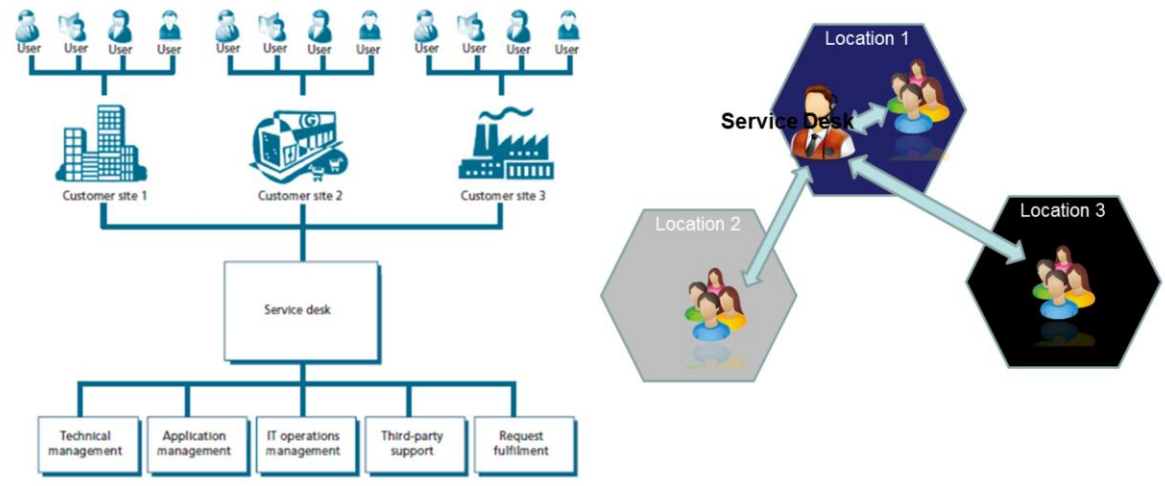


This is where a desk is co-located within or physically close to the user community it serves. This often aids communication and gives a clearly visible presence, which some users like, but can often be inefficient and expensive to resource as staff are tied up waiting to deal with incidents when the volume and arrival rate of calls may not justify this.

There may, however, be some valid reasons for maintaining a local desk, even where call volumes alone do not justify this. Reasons might include:

- Language and cultural or political differences
- Different time zones
- Specialized groups of users
- The existence of customized or specialized services that require specialist knowledge
- VIP/criticality status of users.

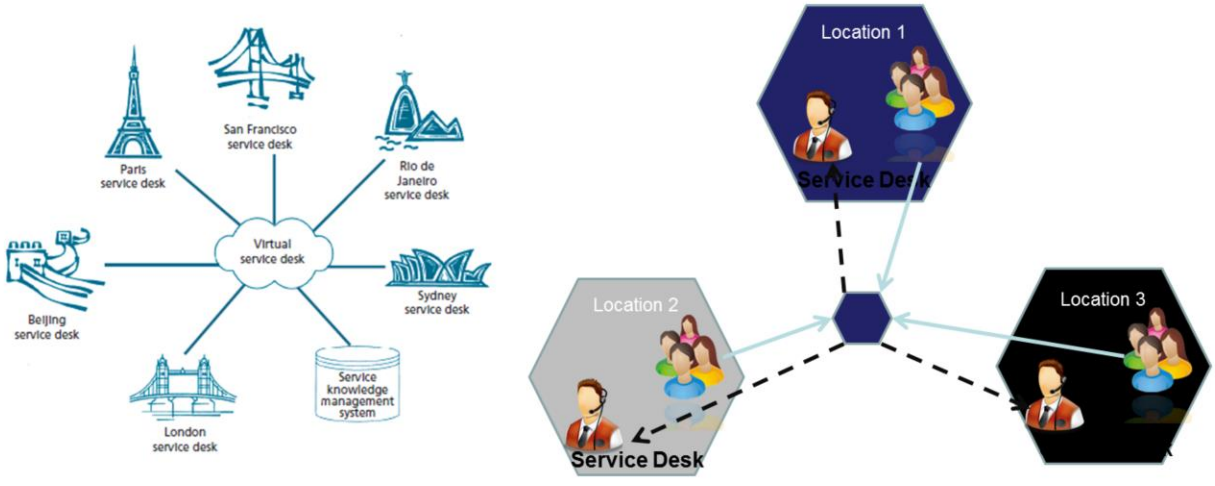
Service Desk Structures – *Centralized Service Desk*



It is possible to reduce the number of Service Desks by merging them into a single location (or into a smaller number of locations) by drawing the staff into one or more centralized Service Desk structures. This can be more efficient and cost-effective, allowing fewer overall staff to deal with a higher volume of calls, and can also lead to higher skill levels through great familiarization through more frequent occurrence of events.

It might still be necessary to maintain some form of 'local presence' to handle physical support requirements, but such staff can be controlled and deployed from the central desk.

Service Desk Structures – *Virtual Service Desk*



Through the use of technology, particularly the Internet, and the use of corporate support tools, it is possible to give the impression of a single, centralized Service Desk when in fact the personnel may be spread or located in any number or type of geographical or structural locations. This brings in the option of 'home working', secondary support group, off-shoring or outsourcing – or any combination necessary to meet user demand. It is important to note, however, that safeguards are needed in all of these circumstances to ensure consistency and uniformity in service quality and cultural terms.

Service Desk Structures – *Follow the Sun*

- Objective: provide 24-hour coverage without requiring service desk to work several or up normal shifts
- Global or international organizations may wish to combine two or more of their geographically dispersed Service Desks to provide a 24-hour follow-the-sun service.

Some global or international organizations may wish to combine two or more of their geographically dispersed service desks to provide a 24-hour follow-the-sun service. For example, a service desk in the Asia-Pacific may handle calls during its standard office hours and at the end of this period it may hand over responsibility for any open incidents to a European-based desk. That desk will handle these calls alongside its own incidents during its standard day and then hand over to a USA-based desk – which finally hands back responsibility to the Asia-Pacific desk to complete the cycle.

This can give 24-hour coverage at relatively low cost, as no desk has to work more than a single shift. However, the same safeguards of common processes, tools, shared databases of information and culture must be addressed for this approach to proceed – and well-controlled escalation and handover processes are needed.

Service Desk Structures – *Specialized Service Desk Groups*

- A 'specialist groups' within the overall Service Desk structure is created.
- concept: incidents relating to a particular IT service can be routed directly to the specialist group.
- Benefit: allow faster resolution of these incidents, through greater familiarity and specialist training.

For some organizations it might be beneficial to create 'specialist groups' within the overall Service Desk structure, so that incidents relating to a particular IT service can be routed directly (normally via telephony selection or a web-based interface) to the specialist group. This can allow faster resolution of these incidents, through greater familiarity and specialist training.

The selection would be made using a script along the lines of 'If your call is about the X Service, please press 1 now, otherwise please hold for a Service Desk analyst'.

Care is needed not to over complicate the selection, so specialist groups should only be considered for a very small number of key services where these exist, and where call rates about that service justify a separate specialist group.

Technical Management– Objectives

- Technical Management: the groups, departments or teams that provide technical expertise and overall management of the IT Infrastructure.
- The objectives of Technical Management are to help plan, implement and maintain a stable technical infrastructure to support the organization's business processes:
  - Design of highly resilient, cost-effective technical topology
  - Maintain the technical infrastructure in optimum condition
  - Diagnose and resolve any technical failures that do occur

Technical management refers to the groups, departments or teams that provide technical expertise and overall management of the IT infrastructure.

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

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

Technical Management– Role

- Ensures that the organization has access to the right type and level of human resources to manage technology and thus to meet business objectives by:
  - Ensuring that the knowledge required to design, test, manage and improve IT services is identified, developed and refined
  - Ensuring that resources are effectively trained and deployed to design, build, transition, operate and improve the technology required to deliver and support IT services
  - Providing guidance to IT Operations about how best to carry out the ongoing operational management of technology

Technical Management plays a dual role:

- It is the custodian of technical knowledge and expertise related to managing the IT Infrastructure. In this role, Technical Management ensures that the knowledge required to design, test, manage and improve IT services is identified, developed and refined.
- It provides the actual resources to support the ITSM Lifecycle. In this role Technical Management ensures that resources are effectively trained and deployed to design, build, transition, operate and improve the technology required to deliver and support IT services.

By performing these two roles, Technical Management is able to ensure that the organization has access to the right type and level of human resources to manage technology and, thus, to meet business objectives. Defining the requirements for these roles starts in Service Strategy and is expanded in Service Design, validated in Service Transition and refined in Continual Service Improvement.

Part of this role is also to ensure a balance between the skill level, utilization and the cost of these resources. For example, hiring a top-level resource at the higher end of the salary scale and then only using that skill for 10% of the time is not effective. A better Technical Management strategy would be to identify the times that the skill is needed and then hire a contractor for only those tasks.

An additional, but very important role played by Technical Management is to provide guidance to IT Operations about how best to carry out the ongoing operational management of technology. This role is partly carried out during the Service Design process, but it is also a part of everyday communication with IT Operations Management as they seek to achieve stability and optimum performance.

Application Management – Objectives

- Responsible for managing applications throughout their lifecycle
- Objectives:
  - Support the organization's business processes by helping to identify functional and manageability requirements for application software
  - Assist in the design and deployment of those applications
  - Assist in 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 required functionality is available to achieve the required business outcome
  - The organization of adequate technical skills to maintain operational applications in optimum condition
  - Swift use of technical skills to speedily diagnose and resolve any technical failures that do occur.

Application management is responsible for managing applications throughout their lifecycle. This differs from application development as application management covers the entire ongoing lifecycle of an application, including requirements, design, build, deploy, operate and optimize. Application development is mainly concerned with the one-time activities for requirements, design and build of applications.

The application management function is performed by any department, group or team involved in managing and supporting operational applications. Application management also plays an important role in the design, testing and improvement of applications that form part of IT services. As such, it may be involved in development projects, but is not usually the same as the applications development teams.

Application Management is responsible for managing applications throughout their lifecycle.

The Application Management function is performed by any department, group or team involved in managing and supporting operational applications. Application Management also plays an important role in the design, testing and improvement of applications that form part of IT services. As such, it may be involved in development projects, but is not usually the same as the Applications Development teams.

The objectives of Application Management are to support the organization's business processes by helping to identify functional and manageability requirements for application software, and then to assist in the design and deployment of those 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 required functionality is available to achieve the required business outcome
- The organization of adequate technical skills to maintain operational applications in optimum condition
- Swift use of technical skills to speedily diagnose and resolve any technical failures that do occur.

Application Management – Role

- Ensures that the knowledge required to design, test, manage and improve IT services is identified, developed and refined
- Ensures that resources are effectively trained and deployed to design, build, transition, operate and improve the technology required to deliver and support IT services
- Provides guidance to IT operations about how best to carry out the ongoing operational management of applications
- Integrates the application management lifecycle into the service lifecycle

Application management is to applications what technical management is to the IT infrastructure. Application management activities are performed in all applications, whether purchased or developed in-house. One of the key decisions that they contribute to is the decision of whether to buy an application or build it. Once that decision is made, application management will have several roles:

•It is the custodian of technical knowledge and expertise related to managing applications. In this role application management, working together with technical management, ensures that the knowledge required to design, test, manage and improve IT services is identified, developed and refined.

•It provides the actual resources to support the service lifecycle. In this role, application management ensures that resources are effectively trained and deployed to design, build, transition, operate and improve the technology required to deliver and support IT services.

By performing these roles, application management is able to ensure that the organization has access to the right type and level of human resources to manage applications and thus to meet business objectives. This starts in service strategy and is expanded in service design, tested in service transition and refined in CSI (see other ITIL publications in this series). A key objective is to ensure a balance between the skill level and the cost of these resources.

Application management also performs other 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 it is also a part of everyday communication with IT operations management as they seek to achieve stability and optimum performance.

•The integration of the application management lifecycle into the service lifecycle.

IT Operation Management – Objectives

- IT operations: the set of activities involved in the day-to-day running of the IT infrastructure for the purpose of delivering IT services at agreed levels to meet stated business objectives
- Responsible for the ongoing management and maintenance of an organization's IT Infrastructure to ensure delivery of the agreed level of IT services to the business
- Objectives:
  - Maintenance of the status quo to achieve stability of the organization's day-to-day processes and activities
  - Identification of improvement opportunities to achieve improved service at reduced costs, while maintaining stability
  - Effective and efficient application of operational skills to diagnose and resolve any IT operations failures that occur

In business, the term 'operations management' is used to mean the department, group or team of people responsible for performing the organization's day-to-day operational activities – such as running the production line in a manufacturing environment or managing the distribution centres and fleet movements within a logistics organization. Operations management has the following characteristics:

•There is work to ensure that a device, system or process is actually running or working (as opposed to strategy or planning)

•This is where plans are turned into actions

•The focus is on daily or shorter-term activities, although it should be noted that these activities will generally be performed and repeated over a relatively long period (as opposed to one-off project-type activities)

•These activities are executed by specialized technical staff, who often have to undergo technical training to learn how to perform each activity

•There is a focus on building repeatable, consistent actions that – if repeated frequently enough at the right level of quality – will ensure the success of the operation

•This is where the actual value of the organization is delivered and measured

•There is a dependency on investment in equipment or human resources or both

•The value generated must exceed the cost of the investment and all other organizational overheads (such as management and marketing costs) if the business is to succeed.

The objectives of IT operations management include:

•Maintenance of the status quo to achieve stability of the organization's day-to-day processes and activities

•Regular scrutiny and improvements to achieve improved service at reduced costs, while maintaining stability

•Swift application of operational skills to diagnose and resolve any IT operations failures that occur.

IT Operation Management – Role

- Operations Control: oversees the execution and monitoring of the operational activities and events in the IT Infrastructure:
  - Console Management
  - Job Scheduling
  - Backup and Restore
  - Print and Output management
  - Performance of maintenance activities
- Facilities Management: manages the physical IT environment, typically a Data Centre or computer rooms and recovery sites together with all the power and cooling equipment

The role of IT operations management is to execute the ongoing activities and procedures required to manage and maintain the IT infrastructure so as to deliver and support IT services at the agreed levels.

IT operations control: IT operations control oversees the execution and monitoring of the operational activities and events in the IT infrastructure. This can be done with the help of an operations bridge or network operations centre. In addition to executing routine tasks from all technical areas, IT operations control also performs the following specific tasks:

- Console management/operations bridge, which refers to defining central observation and monitoring capability and then using those consoles to exercise event management, monitoring and control activities
- Job scheduling, or the management of routine batch jobs or scripts
- Backup and restore on behalf of all technical and application management teams and departments and often on behalf of users
- Print and output management for the collation and distribution of all centralized printing or electronic output
- Performance of maintenance activities on behalf of technical or application management teams or departments.

Facilities management: Facilities management refers to the management of the physical IT environment, typically a data centre or computer rooms and recovery sites together with all the power and cooling equipment. Facilities management also includes the coordination of large-scale consolidation projects, e.g. data centre consolidation or server consolidation projects. In some cases the management of a data centre is outsourced, in which case facilities management refers to the management of the outsourcing contract.

As with many ITSM processes and functions, IT operations management plays a dual role:

- IT operations management is responsible for executing the activities and performance standards defined during service design and tested during service transition. In this sense the role of IT operations is primarily to maintain the status quo. The stability of the IT infrastructure and consistency of IT services is a primary concern of IT operations. Even operational improvements are aimed at finding simpler and better ways of doing the same thing.
- At the same time, IT operations is part of the process of adding value to the different lines of business and to support the value network. The ability of the business to meet its objectives and to remain competitive depends on the output and reliability of the day-to-day operation of IT. As such, IT operations management must be able to continually adapt to business requirements and demand. The business does not care that IT operations complied with a standard procedure or that a server performed optimally. As business demand and requirements change, IT operations management must be able to keep pace with them, often challenging the status quo.

IT operations must achieve a balance between these roles, which will require the following:

- An understanding of how technology is used to provide IT services
- An understanding of the relative importance and impact of those services on the business
- Procedures and manuals that outline the role of IT operations in both the management of technology and the delivery of IT services
- A clearly differentiated set of metrics to report to the business on the achievement of service objectives; and to report to IT managers on the efficiency and effectiveness of IT operations
- All IT operations staff understand exactly how the performance of the technology affects the delivery of IT services
- A cost strategy aimed at balancing the requirements of different business units with the cost savings available through optimization of existing technology or investment in new technology
- A value- rather than cost-based ROI strategy.

Service Operation Processes

Service Operation Processes

Event Management

Event Management – Purpose and Objectives

- **Purpose:** Manage events throughout their lifecycle. This lifecycle of activities to detect events, make sense of them and determine the appropriate control action is coordinated by the event management process

- **Objectives:**
  - Detect all changes of state that have significance for the management of a CI or IT service
  - Provide the trigger, or entry point, for the execution of many service operation processes and operations management activities
  - Provide the ability to compare actual operating performance and behaviour against design standards and SLAs
  - Provide a basis for service assurance and reporting

The purpose of event management is to manage events throughout their lifecycle. This lifecycle of activities to detect events, make sense of them and determine the appropriate control action is coordinated by the event management process.

Event management is therefore the basis for operational monitoring and control. If events are programmed to communicate operational information as well as warnings and exceptions, they can be used as a basis for automating many routine operations management activities, for example executing scripts on remote devices, or submitting jobs for processing, or even dynamically balancing the demand for a service across multiple devices to enhance performance.

The objectives of the event management process are to:

•Detect all changes of state that have significance for the management of a CI or IT service

•Determine the appropriate control action for events and ensure these are communicated to the appropriate functions

•Provide the trigger, or entry point, for the execution of many service operation processes and operations management activities

•Provide the means to compare actual operating performance and behaviour against design standards and SLAs

•Provide a basis for service assurance and reporting; and service improvement.

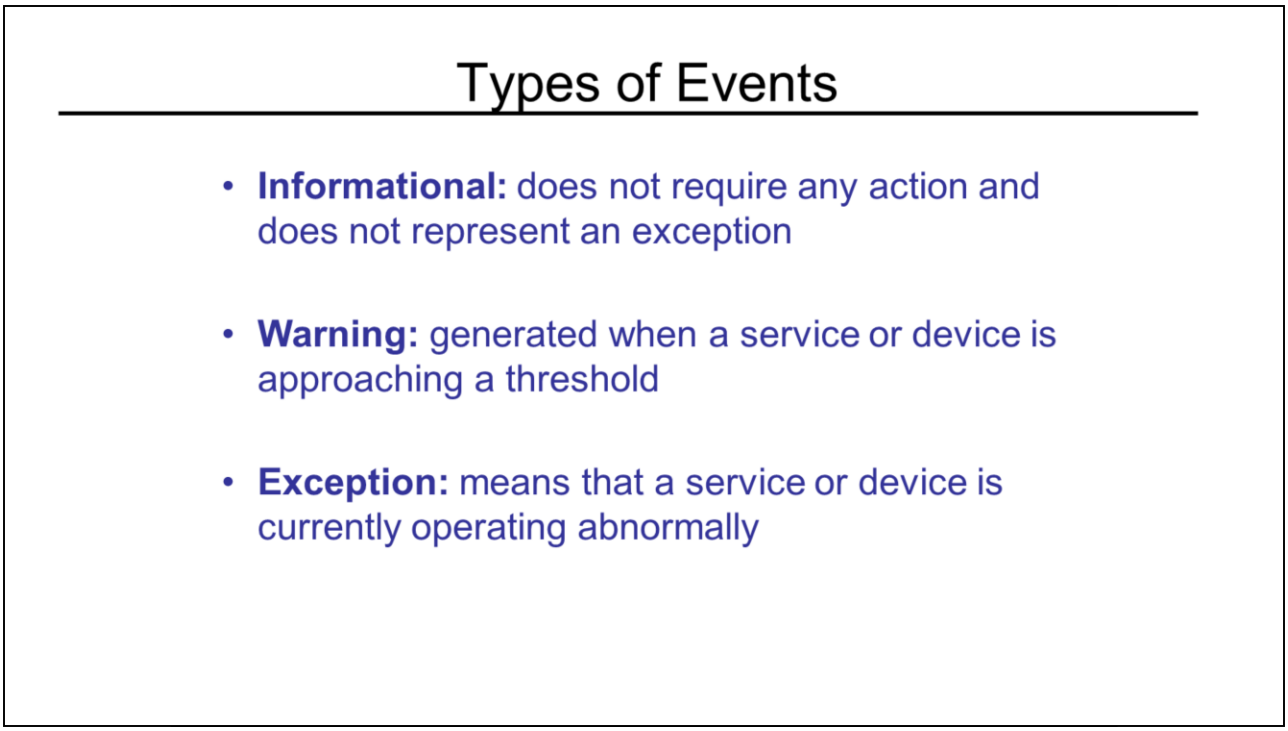
Event Management – Event and Alert

An **event** is any change of state that has significance for the management of a configuration item (CI) or IT service. Events are typically recognized through notifications created by an IT service, CI or monitoring tool

(ITIL Text)

An **alert** A notification that a threshold has been reached, something has changed, or a failure has occurred. Alerts are often crated and managed y system management tools and are managed by the event management process.

(ITIL Text)



Informational events. Examples: a scheduled workload has completed, a user has logged in to use an application, an email has reached its intended recipient.

Warning events. Warning events signify unusual, but not exceptional, operation. These are an indication that the situation may require closer monitoring. In some cases the condition will resolve itself, for example in the case of an unusual combination of workloads – as they are completed, normal operation is restored. In other cases, operator intervention may be required if the situation is repeated or if it continues for too long.

•A server's memory utilization reaches within 5% of its highest acceptable performance level

•The completion time of a transaction is 10% longer than normal.

Exception events.

•A user attempts to log on to an application with the incorrect password

•An unusual situation has occurred in a business process that may indicate an exception requiring further business investigation (e.g. a web page alert indicates that a payment authorization site is unavailable – impacting financial approval of business transactions)

•A device's CPU is above the acceptable utilization rate

•A PC scan reveals the installation of unauthorized software.

Two things are significant about the above examples:

•Exactly what constitutes informational versus a warning, versus an exception? There is no definitive rule about this. Informational events convey data for use in decision making, warning events tend to convey predictive information that some exception might occur and exception events indicate an abnormal situation that requires action to address. For example, a manufacturer may provide that a benchmark of 75% memory utilization is optimal for application X. However, it is discovered that, under specific conditions, response times begin to degrade above 70% utilization. Thresholds are then set that trigger warning events if utilization is between 70 and 75%. At 75% or higher, an exception event is triggered that will require immediate action, such as adding more memory.

•Each relies on the sending and receipt of a message of some sort. These are generally referred to as event notifications and they don’t just happen without planning. The following sections will explore exactly how events are defined, generated and captured.

Service Operation Processes

Incident Management

Incident Management – Purpose and Objectives

- **Purpose:** Restore normal service operation as quickly as possible and minimize the adverse impact on business operations, thus ensuring that agreed levels of service quality are maintained
  - 'Normal service operation' is defined as an operational state where services and CIs are performing within their agreed service and operational levels
- **Objectives:**
  - Ensure 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
  - Align incident management activities/priorities with those of the business
  - Maintain user satisfaction

Incident management is the process responsible for managing the lifecycle of all incidents. Incidents may be recognized by technical staff, detected and reported by event monitoring tools, communications from users (usually via a telephone call to the service desk), or reported by third-party suppliers and partners.

The purpose of incident management is to restore normal service operation as quickly as possible and minimize the adverse impact on business operations, thus ensuring that agreed levels of service quality are maintained. 'Normal service operation' is defined as an operational state where services and CIs are performing within their agreed service and operational levels.

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.

Incident Management – Scope

- Incident management includes any event which disrupts, or which could disrupt, a service:
  - Reported by users
    - service desk
    - interface from event management to incident management tools
  - Reported and/or logged by technical staff

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 events are not related to disruptions at all, but are indicators of normal operation or are simply informational.

Although both incidents and service requests are reported to the service desk, this does not mean that they are the same. Service requests do not represent a disruption to agreed service, but are a way of meeting the customer's needs and may be addressing an agreed target in an SLA. Service requests are dealt with by the request fulfilment process.

Service Operation Processes

Problem Management

Problem Management – Purpose and Objectives

- **Purpose:** manage the lifecycle of all problems from first identification through further investigation, documentation and eventual removal
- **Objectives:**
  - Prevent problems and resulting incidents from happening
  - Eliminate recurring incidents
  - Minimize the impact of incidents that cannot be prevented

Problem management is the process responsible for managing the lifecycle of all problems. ITIL defines a 'problem' as the underlying cause of one or more incidents.

The purpose of problem management is to manage the lifecycle of all problems from first identification through further investigation, documentation and eventual removal. Problem management seeks to minimize the adverse impact of incidents and problems on the business that are caused by underlying errors within the IT Infrastructure, and to proactively prevent recurrence of incidents related to these errors. In order to achieve this, problem management seeks to get to the root cause of incidents, document and communicate known errors and initiate actions to improve or correct the situation.

The objectives of the problem management process are to:

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

Problem Management – Scope

- Diagnose the root cause of incidents and determine the resolution to those problems
- Maintain information about problems and the appropriate workarounds and resolutions
- Perform reactive problem management: solving problems in response to one or more incidents
- Perform proactive problem management: identifying and solving problems and known errors before further incidents related to them can occur again
  - Supports CSI lifecycle activities in identifying and implementing service improvements

Problem management includes the activities required to diagnose the root cause of incidents and to determine the resolution to those problems. It is also responsible for ensuring that the resolution is implemented through the appropriate control procedures, especially change management and release and deployment management. Problem management will also maintain information about problems and the appropriate workarounds and resolutions, so that the organization 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 KEDB will be used for both. Incident and problem management are closely related and will typically use the same tools, and may use similar categorization, impact and priority coding systems.

The problem management process has both reactive and proactive aspects:

- Reactive problem management is concerned with solving problems in response to one or more incidents.
- Proactive problem management is concerned with identifying and solving problems and known errors before further incidents related to them can occur again.
- Examples of proactive problem management activities might include:
  - Conducting periodic scheduled reviews of incident records, operational logs and maintenance records, event logs, to find patterns and trends that may indicate the presence of underlying problems.
  - Conducting major incident reviews where review of 'How can we prevent the recurrence?' can provide identification of an underlying cause or error.
  - Conducting brainstorming sessions to identify trends that could indicate the existence of underlying problems.
  - Using check sheets to proactively collect data on service or operational quality issues that may help to detect underlying problems.

Reactive and proactive problem management activities are generally conducted within the scope of service operation. A close relationship exists between proactive problem management activities and CSI 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 will become input to the CSI register used to record and manage improvement opportunities.

Problems versus Incidents

- **Incidents do not 'become' 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, which may also be the cause of other incidents.
- 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 in the first place

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, which may also be the cause of other incidents. 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 in the first place. It is quite common to have incidents that are also problems.

The rules for invoking problem management during an incident can vary and are at the discretion of individual organizations. Some general situations where it may be desired to invoke problem management during an incident might include situations where:

•Incident management cannot match an incident to existing problems and known errors

•Trend analysis of logged incidents reveals an underlying problem might exist

•A major incident has occurred where problem management activities need to be undertaken to identify the root cause

•Other IT functions identify that a problem condition exists

•The service desk may have resolved an incident but has not determined a definitive cause and suspects that it is likely to recur

•Analysis of an incident by a support group which reveals that an underlying problem exists, or is likely to exist

•A notification from a supplier that a problem exists that has to be resolved.