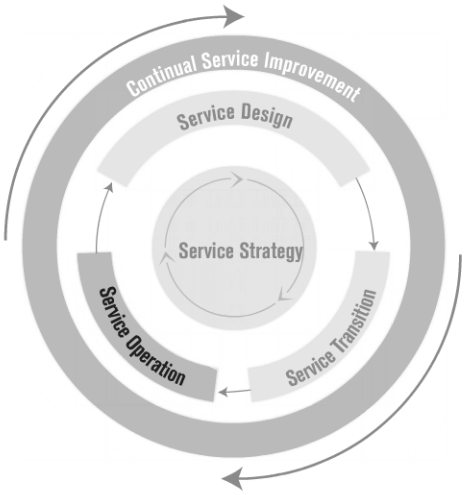
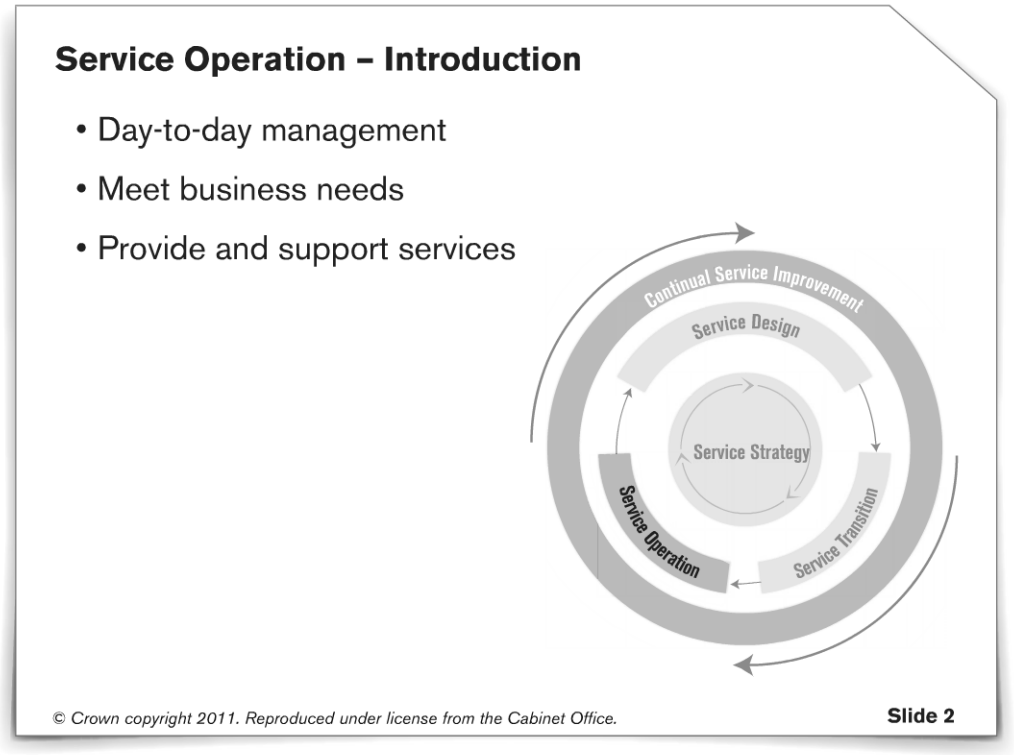
# 5
# Service Operation



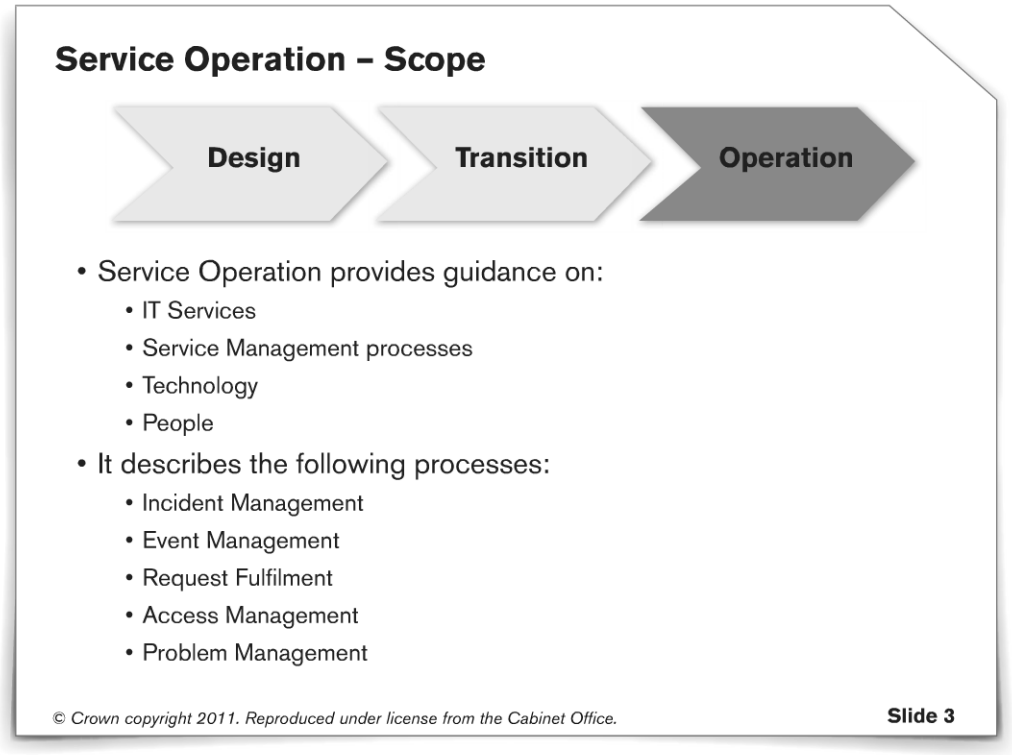



**Service Operation – Introduction**

Service Operation is the stage in the ITIL Service Lifecycle where the service providers' performance and customer requirements are tightly managed. Here, the strategy, design, transition and improvements are provided and supported on a day-to-day basis.

Service Operation provides best practice advice and guidance relating to the people, processes, infrastructure technology and relationships necessary to ensure high quality, cost-effective provision of IT service quality at agreed upon levels to business users and customers in order to meet business needs.

The overriding purpose of Service Operation is to provide (and support) services. Management of the infrastructure and the operational activities must always support this purpose. Service Operation staff should have processes and support tools in place to facilitate an overall view of Service Operation and proficiency to detect any threats or failures to service quality.




**Service Operation – Scope**

ITIL Service Operation describes the processes, functions, organization and tools used to underpin the ongoing activities required to deliver and support services. The guidance provided in this publication includes:

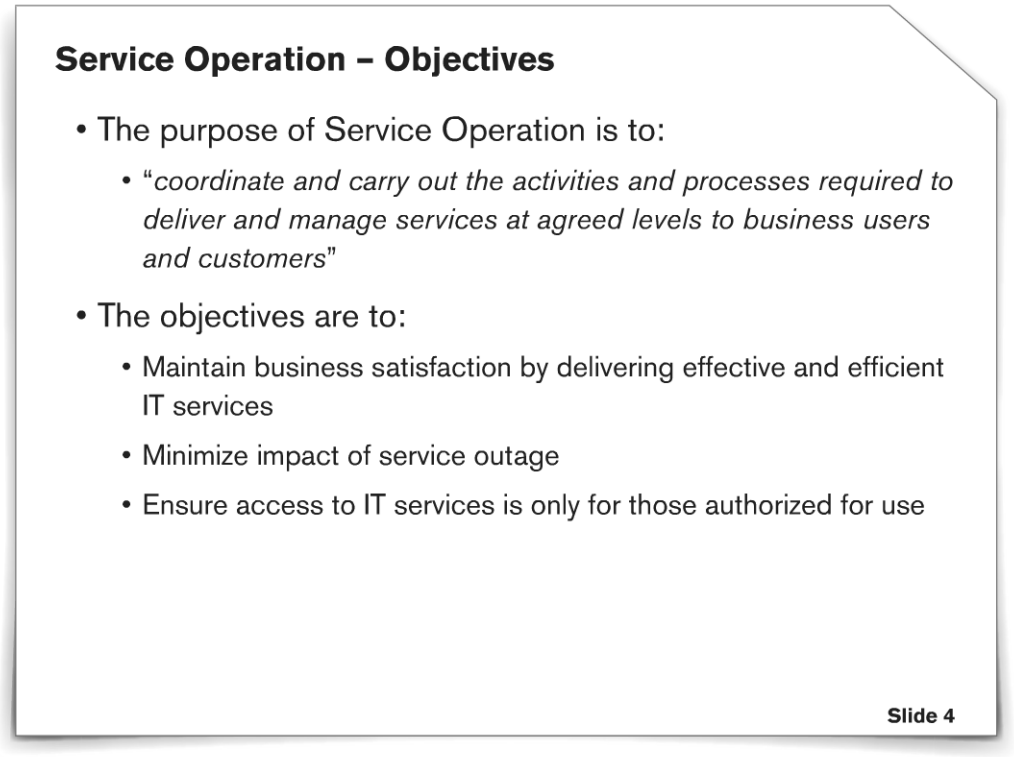
- The services themselves
- Service management processes
- Technology
- People

**Service Operation Processes:**

- Event Management
- Incident Management
- Request Fulfilment
- Access Management
- Problem Management

**Functions:**

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



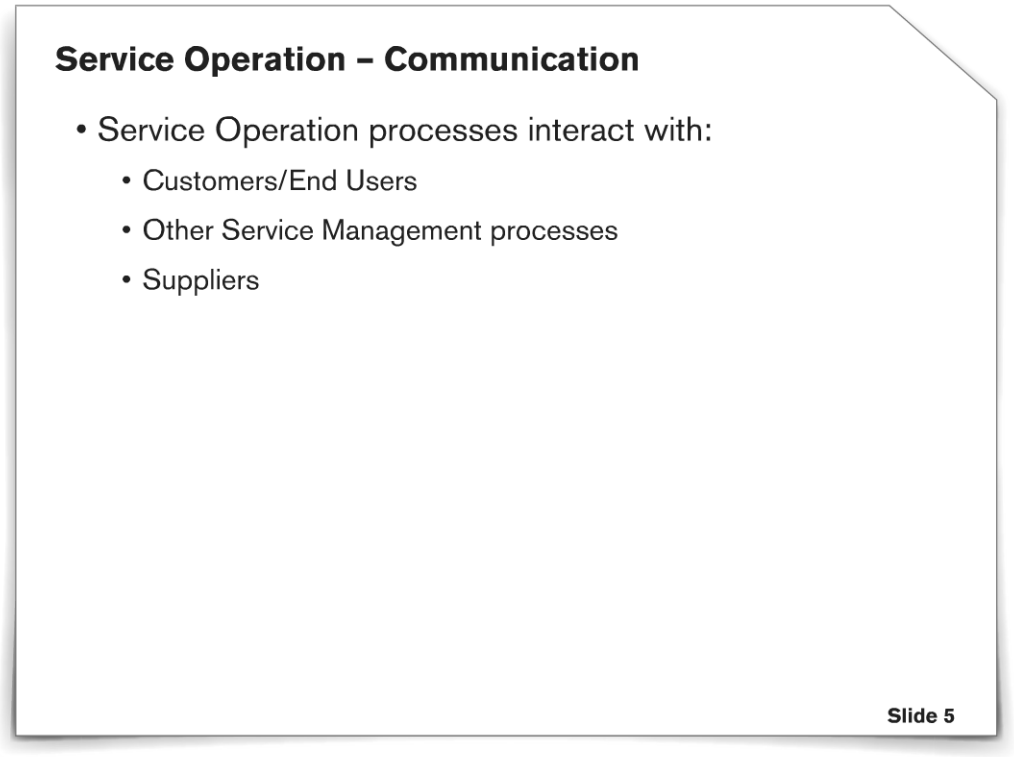

**Service Operation – Objectives**

The **purpose** 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 the ongoing management of the technology that is used to deliver and support services.

Well designed and implemented processes will be of little value 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 data are not systematically conducted during Service Operation.

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.



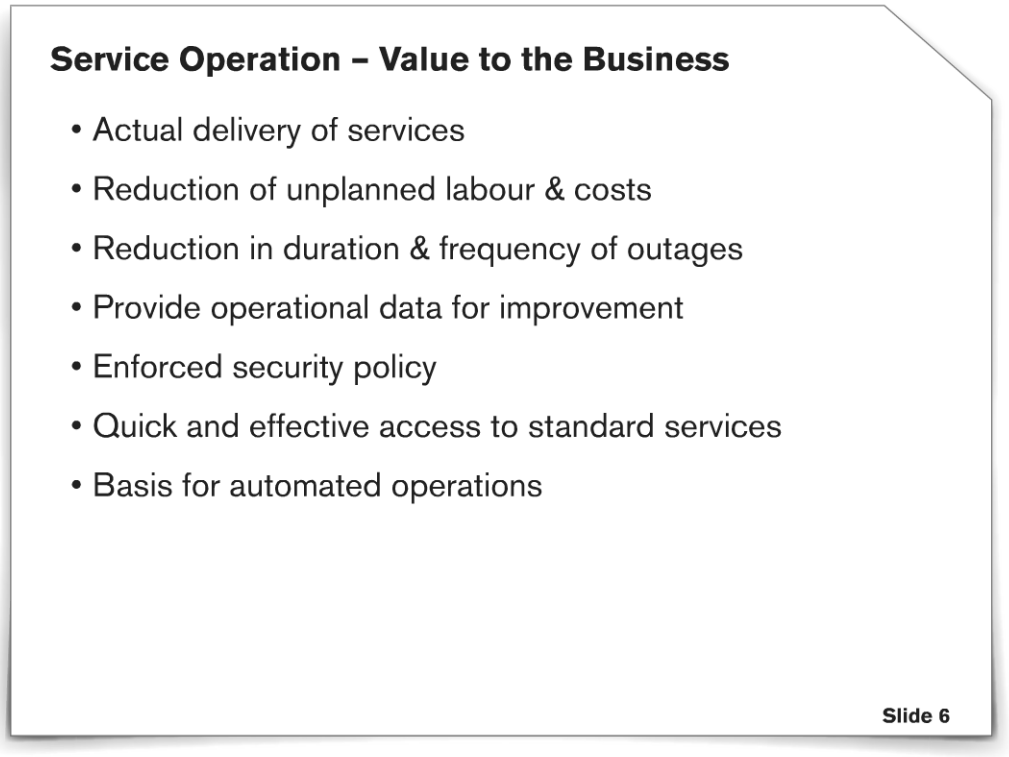

**Service Operation – Communication**

Good communication is essential between IT teams and other departments, between users and internal customers, and between the Service Operation teams and departments themselves. Issues may often be prevented or mitigated through appropriate communication with:

**Customers/end users**: From the customer's point of view, Service Operation is where actual value is seen.

**Continual Service Improvement**: Service improvements will not be possible if day-to-day activities to monitor performance, assess metrics and gather data are not systematically conducted during Service Operation.

**Suppliers**: Any activity that forms part of a service is included in Service Operation, whether it is performed by the Service Provider or an external supplier. The Service Provider delivers services to the business (customer). The Service Provider may have contracts in place with third parties (external suppliers) for the delivery of components or a certain part of the service.

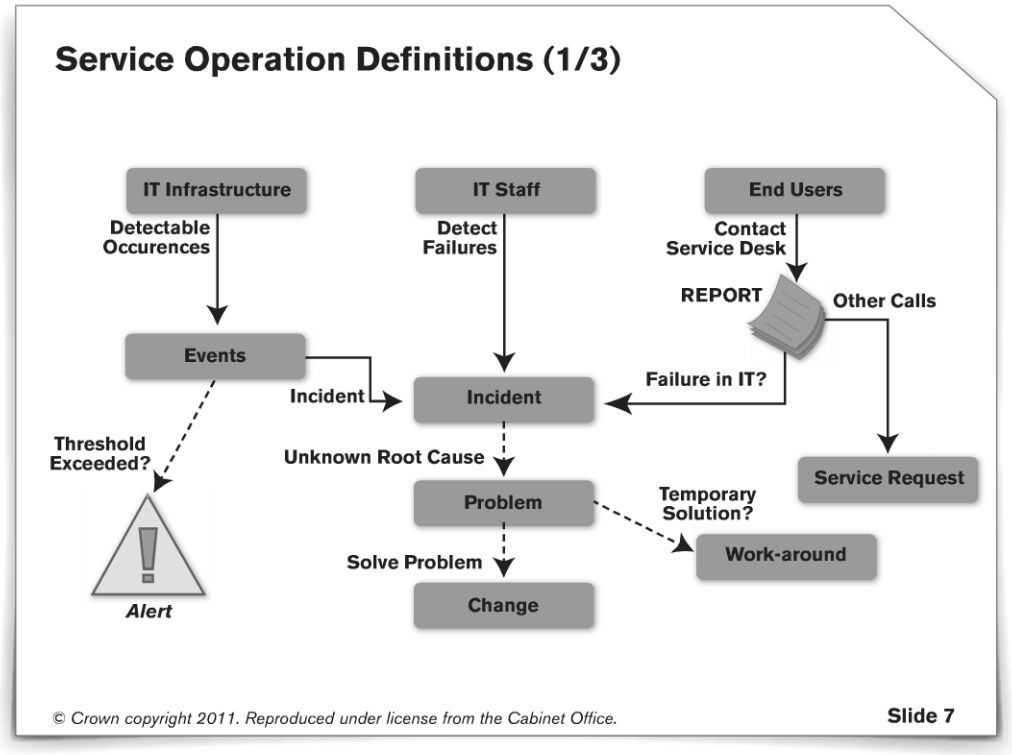



**Service Operation – Value to the Business**

**Service Operation is the fourth phase in the Service Lifecycle**. It is the phase in which a new service hits the market. Return on Investment (ROI) will begin to improve after an initial decrease in profits caused by the planning, testing and development of this new service.

Implementing and standardizing Service Operation provides value to the business and will:

- Reduce unplanned labour and costs for both the business and IT through optimized handling of service outages and identification of their root causes.
- Reduce the duration and frequency of service outages which will allow the business to take full advantage of the value created by the services they are receiving.
- Provide operational results and data that can be used by other ITIL processes to improve services continually and provide justification for investing in ongoing service improvement activities and supporting technologies.
- Meet the goals and objectives of the organization's security policy by ensuring that IT services will be accessed only by those authorized to use them.
- Provide quick and effective access to standard services which business staff can use to improve their productivity or the quality of business services and products.
- Provide 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.




**Service Operation Definitions (1/3)**

Throughout Service Operation, many concepts are defined and discussed. Many of these concepts are related to a certain extent and the graphic above shows the most common relations; however, it is not an exhaustive overview. The next page will give the exact definitions according to ITIL for these concepts.

Detectable occurrences that arise from the *IT infrastructure* are called **events** that are generally managed by the Event Management process. This process determines which events should be monitored, and how these should be handled. Details of this process are discussed later in this module.

Event Management is also responsible for defining thresholds related to these events, and when these *thresholds* are exceeded, an **alert** is raised, to draw specific attention to this/these event(s). Human intervention is often required when an alert is raised.

Some events are related to a failure, and will be reported as an **Incident**, which is handled by the Incident Management process.

End users of the IT services often have questions or need to report Incidents and their Single Point of Contact (SPOC) is the Service Desk, which handles all of these calls. A call may be submitted in several ways:

- Telephone
- Email
- Self Help tools (like a web portal)
- Other

If the call concerns a failure in the IT infrastructure, it is called an **Incident**, and it will be handled according to the procedures of Incident Management.

If the call concerns another issues, such as a complaint, or a request for documentation, it is called a **Service Request**, which is handled with the Request Fulfilment process.

IT staff may also detect failures in the IT infrastructure even before they are noticed by end users or via events. The IT staff must ensure that these failures are registered as an **Incident**.

An Incident is an unplanned interruption to an IT service and should be repaired as soon as possible. The Incident Management process provides procedures for handling Incidents effectively and efficiently.

For Incidents with a large impact, or when multiple Incidents may be related to a single root cause, a **Problem** can be defined. A Problem is the unknown root cause for one or more Incidents and the Problem Management process is established to find this root cause and a solution for the Problem. If, at any point in time, a temporary solution is found and implemented, it is called a **work-around**. This enables to user to continue using the service, while Problem Management tries to find a solution.

Many Problems may only be solved by changing a part of the service, for example, removing a software bug, adding extra hardware, etc. All modifications to the IT infrastructure or its documentation, require a **Request for Change** which is handled by the Change Management process. (This process is discussed in the Service Transition module.)

## Service Operation Definitions (2/3)

- Event
  - "Any detectable occurrence that has significance for the IT infrastructure management or IT service delivery and evaluation of the impact of possible deviations"
- Alert
  - "A warning that a threshold has been reached, something has changed, or a failure has occurred"

Slide 8

**Service Operation Definitions (2/3)**

**Event**

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 services may be considered an event.

**Note**: In most organizations there are a significant number of events that occur every day within an IT infrastructure. This will have an impact on the way in which events are correlated.

**Alert**

A warning that a threshold has been reached, something has changed, or a failure has occurred may be considered an event. The alert requires a person or team to perform a specific action, possibly on a specific device and possibly at a specific time.

## Service Operation Definitions (3/3)

- Service Request
  - "Request from a user for information, advice, a standard change or for access to an IT service"
- Incident
  - "An unplanned interruption to an IT service or reduction in the quality of an IT service"
- Work-around
  - "A temporary way of overcoming issues" (i.e., Incidents or Problems)

Slide 9

**Service Operation Definitions (3/3)**

**Service Request**

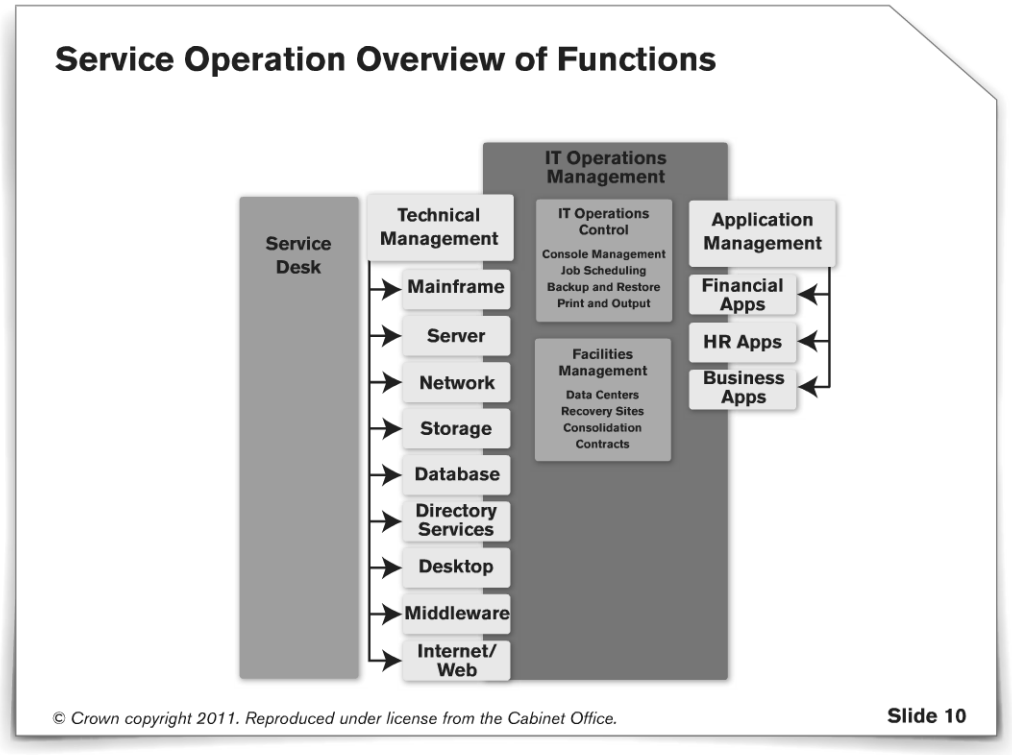
A request from a user for information, advice, a standard change or for access to an IT service such as resetting a password or providing standard IT services to a new user. Service Requests are usually handled by a Service Desk and do not require a submission of a Request for Change (RFC).

**Incident**

An Incident is any event which causes, or may cause an interruption to, or a reduction in, the quality of a service.

**Work-around**

A temporary way of overcoming issues (i.e., Incidents or Problems)




### Service Operation Overview of Functions

The different **functions** in Service Operation:

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

In order to establish clear understanding and avoid conflict of activities and ownership, it is important to understand the overlapping of functions.

Organizations face difficulty in aligning activities and responsibilities to a group of people or departments when some part of the activity is managed by another department. Overlapping helps optimize the utilization of resources and skill pools of the organization.

**Note**: It is recommended that when staff members carry out activities normally allotted to another function, that they be treated as a part of that other function temporarily, until the time activity is completed.

### Technical Management:

Technical Management provides detailed technical skills and resources needed to support the ongoing operation of the IT infrastructure. Technical Management plays an important role in the

design, testing, release and improvement of IT services. Technical Management departments may also be responsible for the daily operation of a subset of the IT infrastructure.

**IT Operations Management:**

This function is responsible for the daily operational activities needed to manage the IT infrastructure and it overlaps with the Technical and Application Management functions.

IT Operations Control ensures that routine operational tasks are carried out, provides centralized monitoring and control activities.

**Facilities Management** refers to the management of the physical IT environment, usually data centers or computer rooms.

**Application Management:**

This function is responsible for managing applications throughout their lifecycle. It supports and maintains operational applications, and plays role in the design, testing and improvement of applications. In many organizations Application Management departments have staff that perform daily operations for those applications. As with Technical Management, these staff members logically form part of the IT Operations Management function.

## Service Operation Functions

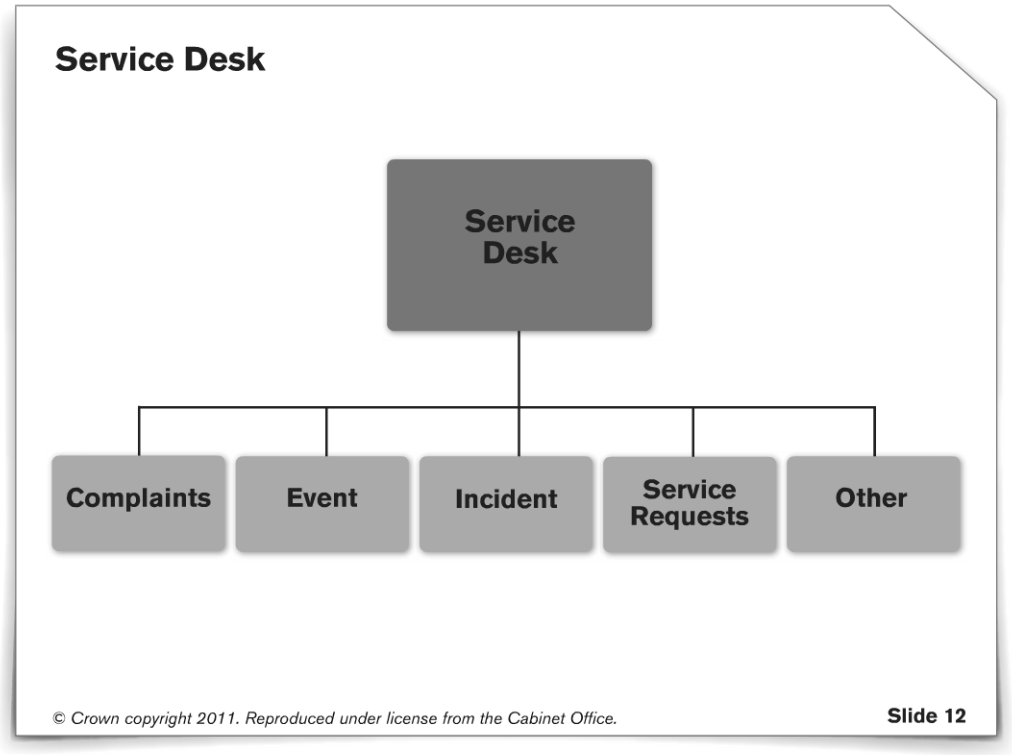
- People and automated measures that execute a defined process, an activity or combination of both
- IT functions define the different roles and responsibilities required for the overall service delivery and support of IT services

Slide 11

### Service Operation Functions

***Functions*** refer to the people and automated measures that execute a defined process, an activity or a combination of both. The functions within Service Operation are needed to manage the "steady state" operation of the IT environment. IT functions define the different roles and responsibilities required for the overall service delivery and support of IT services.

**Note**: These are logical functions and do not necessarily need to be performed by equivalent organizational structures. Technical and Application Management may be organized in any combination and into any number of departments.



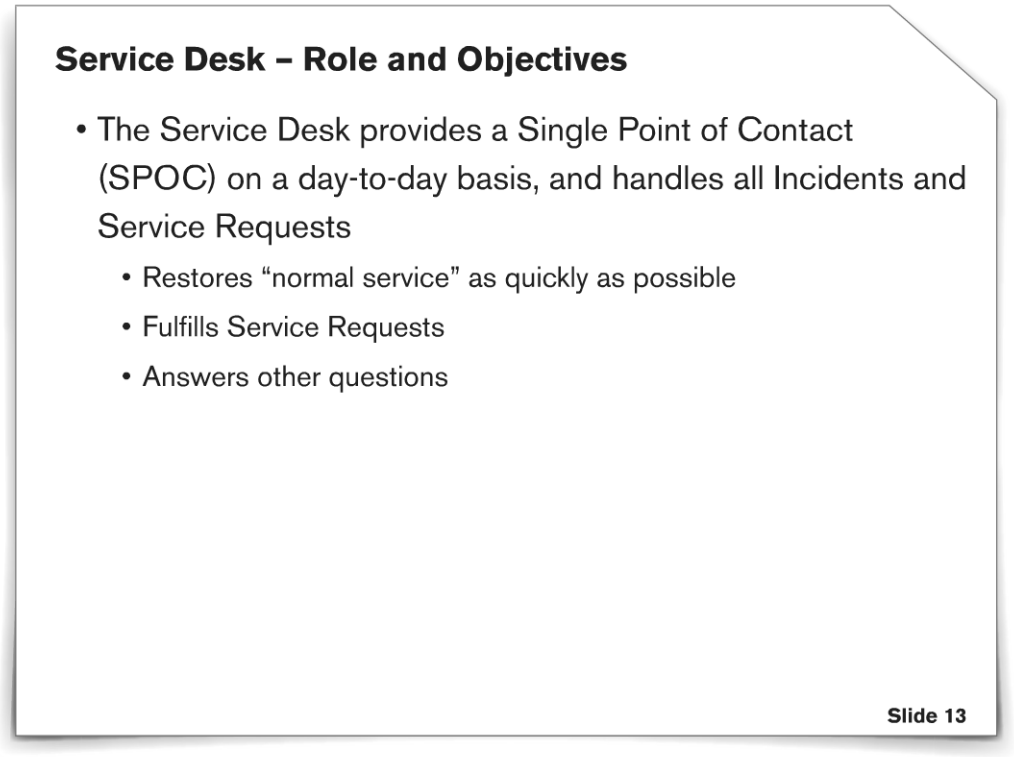

**Service Desk**

**GOAL**: To support the agreed upon IT service provision by ensuring the accessibility and availability of the IT organization and by performing various supporting activities

The Service Desk is the primary point of contact for users when there is a service disruption, for Service Requests or even for some categories of Request for Change. The Service Desk provides a point of communication to the users and a point of coordination for several IT groups and processes. To enable them to perform these actions effectively, the Service Desk is usually separate from the other Service Operation functions. In some cases (e.g., where detailed technical support is offered to users on the first call), it may be necessary for Technical or Application Management staff to be on the Service Desk. This does not mean that the Service Desk becomes part of the Technical Management function. In fact, while they are on the Service Desk, they cease to be a part of the Technical Management or Application Management functions and become part of the Service Desk, even if only temporarily.

The Service Desk is a functional unit (not a process) which is the Single Point of Contact (SPOC) for the IT organization. It handles all types of calls (events, alerts, Incidents and Service Requests), which may be either reported by a user or automatically generated by a tool. The Service Desk may handle the call itself, or refer the caller to other parties, such as External Service Support or Internal Service Support.

Service Desk staff uses the Configuration Management System (CMS) for, among other purposes, logging and keeping track of all calls. The CMS is a set of tools that supports IT Service Management and is discussed in more detail in the Service Transition book.




**Service Desk – Role and Objectives**

The Service Desk is a very important function which provides a Single Point of Contact (SPOC) for end users. It handles all Incidents and Service Requests on a day-to-day basis.

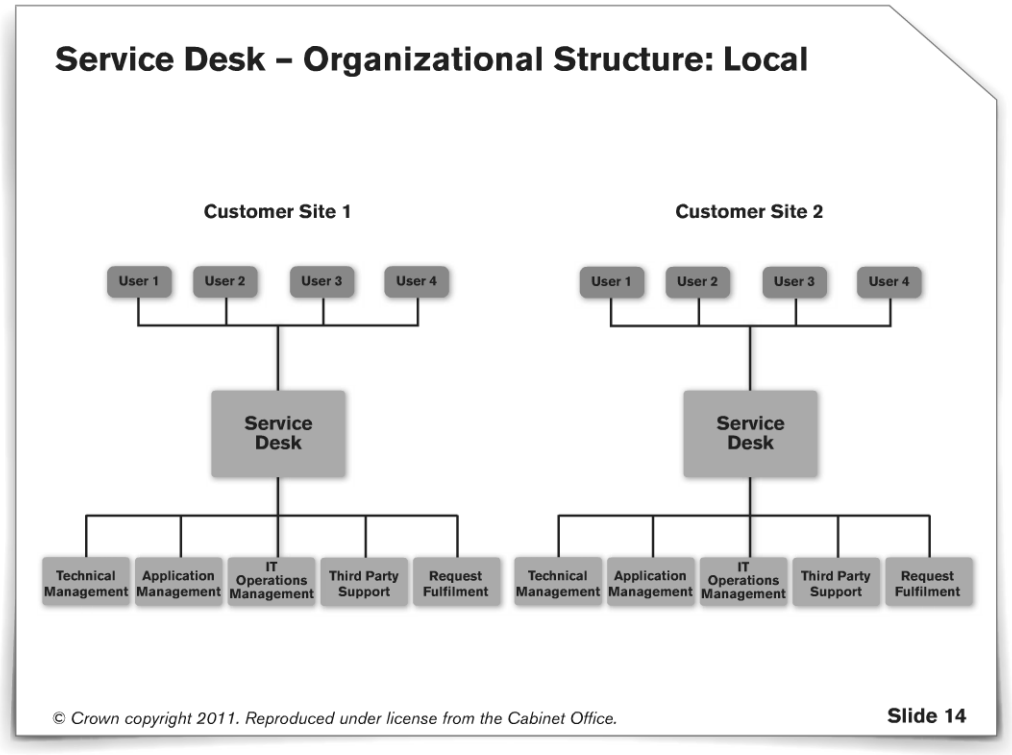
The primary **objective** is to restore the "normal service" to the users as quickly as possible.

Furthermore, the following specific **responsibilities** are important:

- Logging all relevant Incident/Service Request details, and applying categorization and prioritization codes
- Providing first-line investigation and diagnosis
- Resolving those Incidents/Service Requests within its skill set/control
- Escalating the Incident/Service Requests that they cannot resolve within agreed upon timescale
- Closing all resolved Incidents, requests or other calls
- Conducting customer/user satisfaction call-backs/surveys as agreed upon

- Communicating with users: Keeping them informed of Incident progress, and notifying them of impending changes or agreed upon outages
- Updating the CMS under the direction and approval of Configuration Management, if so agreed upon

**Note**: The Service Desk is the "owner" of any Incident.




**Service Desk – Organizational Structure: Local**

Service Desks may have different organizational structures. Many small companies begin their operation with a **Local Service Desk**.

A Local Service Desk is located within or physically close to the user community it serves.

Advantages:

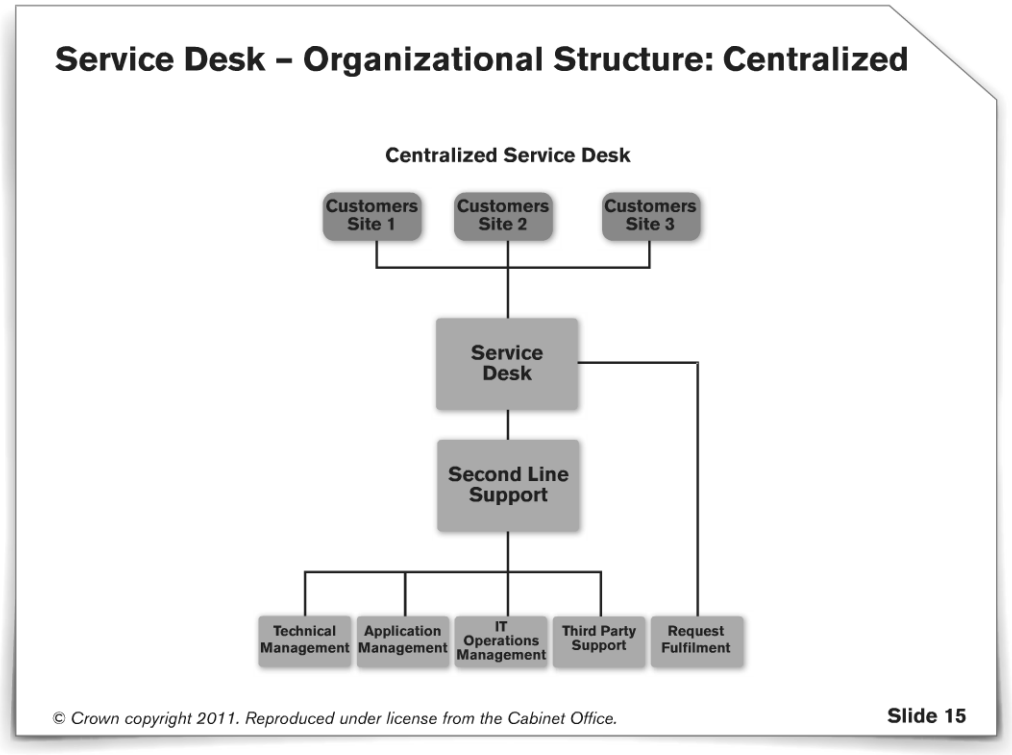
- Aids communication
- Has a clearly visible presence
- Is physically close to the user population

Disadvantages:

- Inefficient
- Expensive

(**Note**: These disadvantages are mostly applicable when the business has multiple locations. If the business has only one location, then a local Service Desk naturally makes sense).

There might be valid reasons for a Local Service Desk: language and cultural or political differences, different time zones, specialized groups of users, the existence of customized or specialized services that require specialist knowledge, or VIP/criticality status of users.




**Service Desk – Organizational Structure: Centralized**

When companies grow, they might consider a **Centralized Service Desk** (formed by one or more centralized desks).

A Centralized Service Desk constitutes the merging of Local Service Desks into a single location (or into a smaller number of locations), drawing the staff into one or more Centralized Service Desk structures. In this structure multiple user groups are served from one physical location.

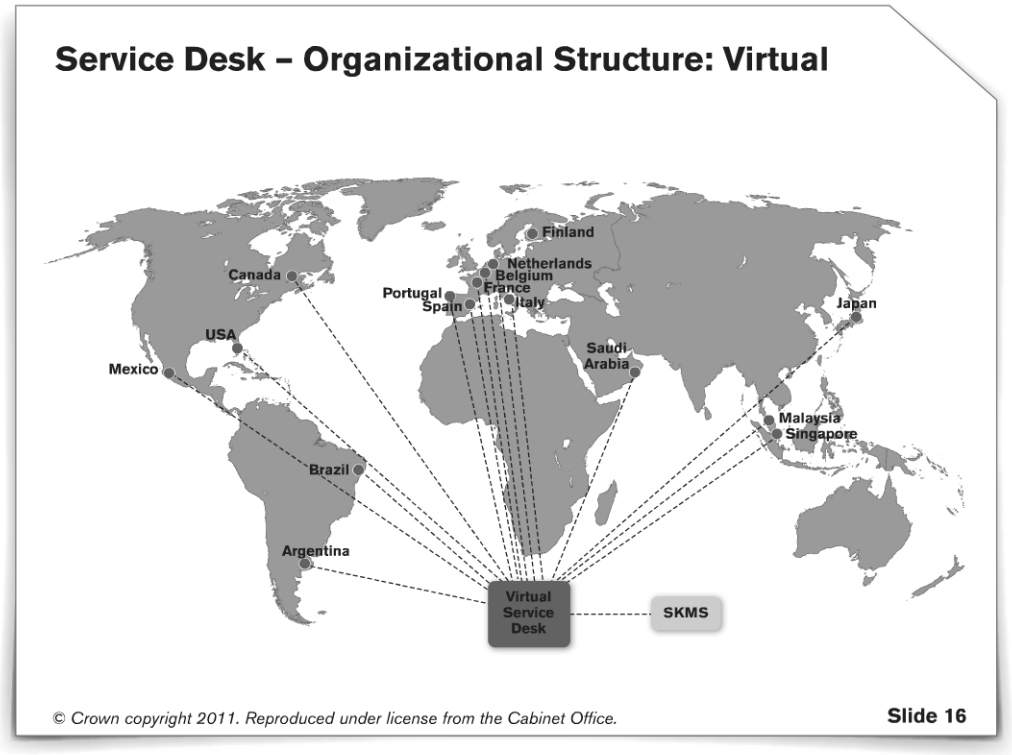
Advantages:

- More efficient
- Cost-effective

Disadvantages:

- Distance from users

To compensate for the distance a Centralized Service Desk often has a local presence to administer physical support, controlled and deployed from the Centralized Service Desk.




**Service Desk – Organizational Structure: Virtual**

Larger organizations with widespread locations or many departments might consider a Virtual **Service Desk**. This gives an impression of a single, Centralized Service Desk, located in any number or type of geographical or structural locations. For all users, there is a Single Point of Contact (e.g., phone number or email address) and their calls may be handled by any of the locations. It is important that a single Service Knowledge Management System (SKMS) is used by all locations.

Advantages:

- More efficient
- Cost-effective

Disadvantages:

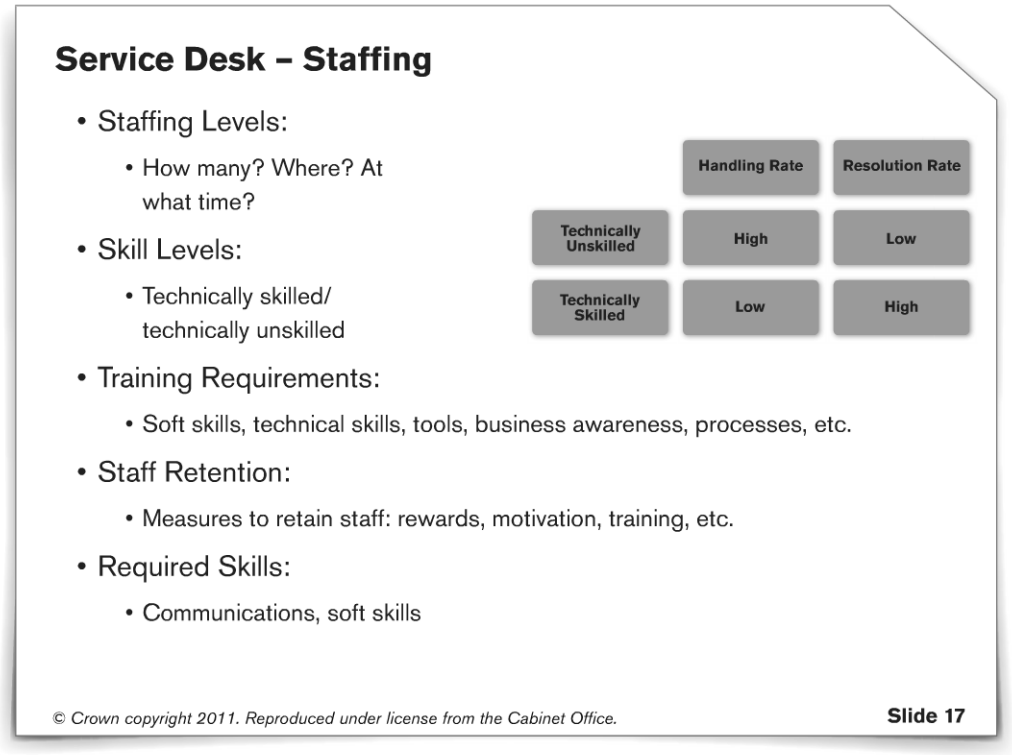
- A need to address safeguards of common processes, common tools, a single shared database of information and shared culture

**Follow-the-Sun**

Companies with a global presence may apply a "Follow-the-Sun" approach of the Virtual Service Desk. This combines two or more geographically dispersed Service Desks to provide 24-hour service. For example, a Service Desk in the Asia-Pacific region may handle calls during normal business hours and then hand over any open Incidents to the European-based desk at the end of this period. The European-based desk then handles these Incidents along with its own until its

standard hours have finished. At this point it hands over calls and Incidents to the North American-based desk who then return calls to the Asia-Pacific desk at the end of its standard hours.

This allows 24-hour coverage at a relatively low cost. However, care must be taken along the same lines as the Virtual Service Desk in terms of common processes, tools, shared knowledge base, etc.




**Service Desk – Staffing**

An important factor in the Service Desk is the staffing. 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.

**There are five areas of concern for staffing:**

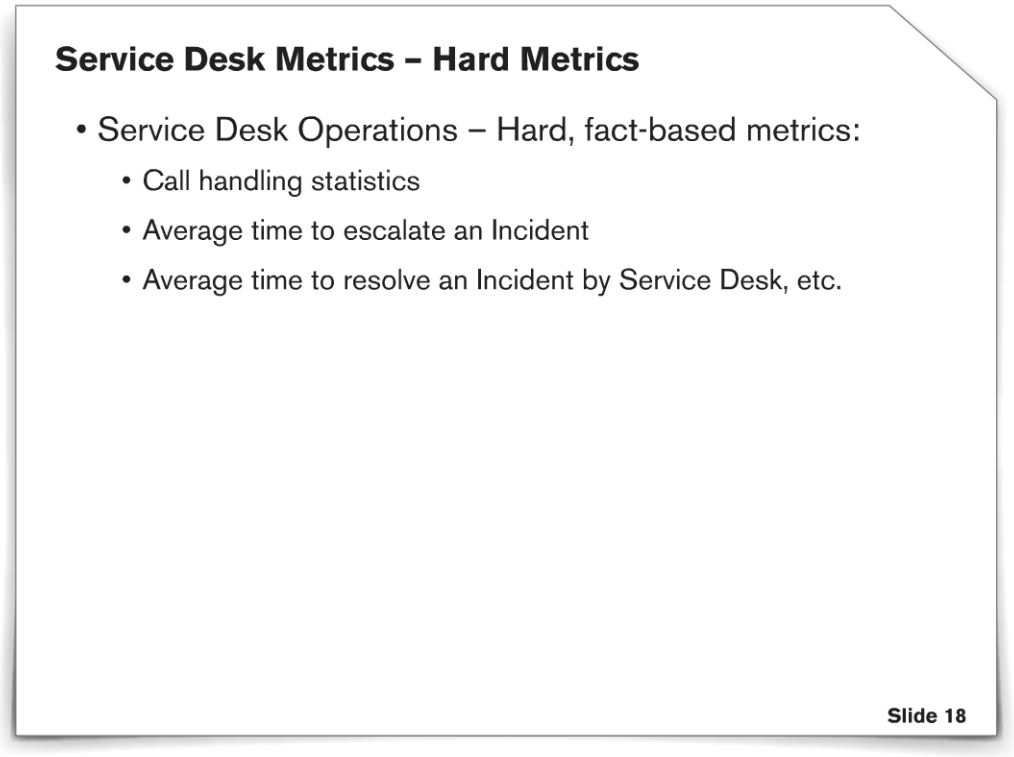
**Staffing levels**: Correct number of staff at any given moment to match the demand being placed upon the Service Desk by the business. Predict call arrival rate and call types. (Calls often peak at start of the day (password resets, for example) with another burst right after lunchtime).

**Skill levels**: An organization must decide on the level and range of skills it requires of its Service Desk staff, and ensure that all these skills are available at the appropriate times.

**Training**: Adequately train staff before it is called upon. Preferably a formal introduction program is used, followed by a business awareness program. Keep knowledge up to date, improve skills (both for current position and for future roles), helping to create clear career paths and recognizing future requirements and development.

**Staff retention**: IT managers must recognize the importance of the Service Desk, giving special attention and making the Service Desk an attractive place to work, using reward packages, team-building exercises and staff rotation.

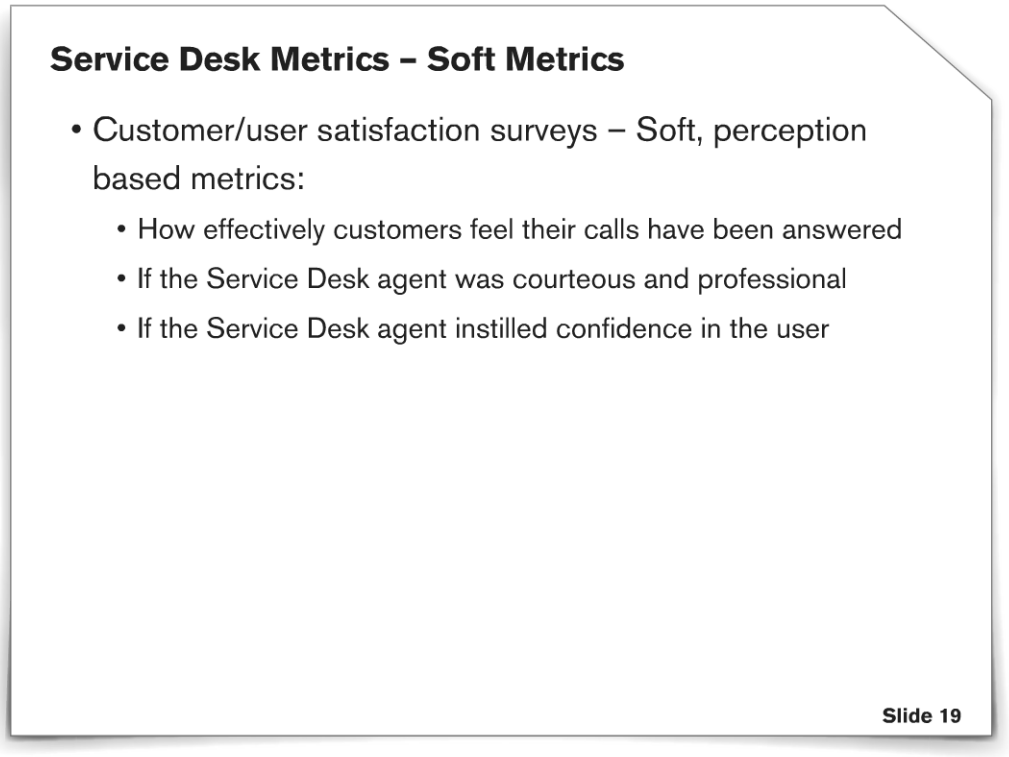
**Required skills**: Prerequisite skills are communications and soft skills. These are the primary skills that Service Desk staff must possess. Other skills may be acquired or improved when beginning work at a Service Desk.




**Service Desk Metrics – Hard Metrics**

Establish metrics in order to evaluate performance of the Service Desk at regular intervals. The performance of the Service Desk may be evaluated using hard and soft measures. Hard measures involve with numbers and statistics (fact-based). Soft measures are more focused on the personal approach (perception-based). Hard measures may be derived by assessing the health, maturity, efficiency, effectiveness and any opportunities to improve Service Desk Operations, leading to the following eight points:

1. Call handling statistics
2. The first-line resolution rate
3. Average time to resolve an Incident
4. Average time to escalate an Incident
5. Average Service Desk cost of handling an Incident (per number of calls, and cost per minute)
6. Percentage of customer or user updates
7. Average time to review and close a resolved call
8. The number of calls broken down by the time of day and day of the week (disconnected, not responded to in time)

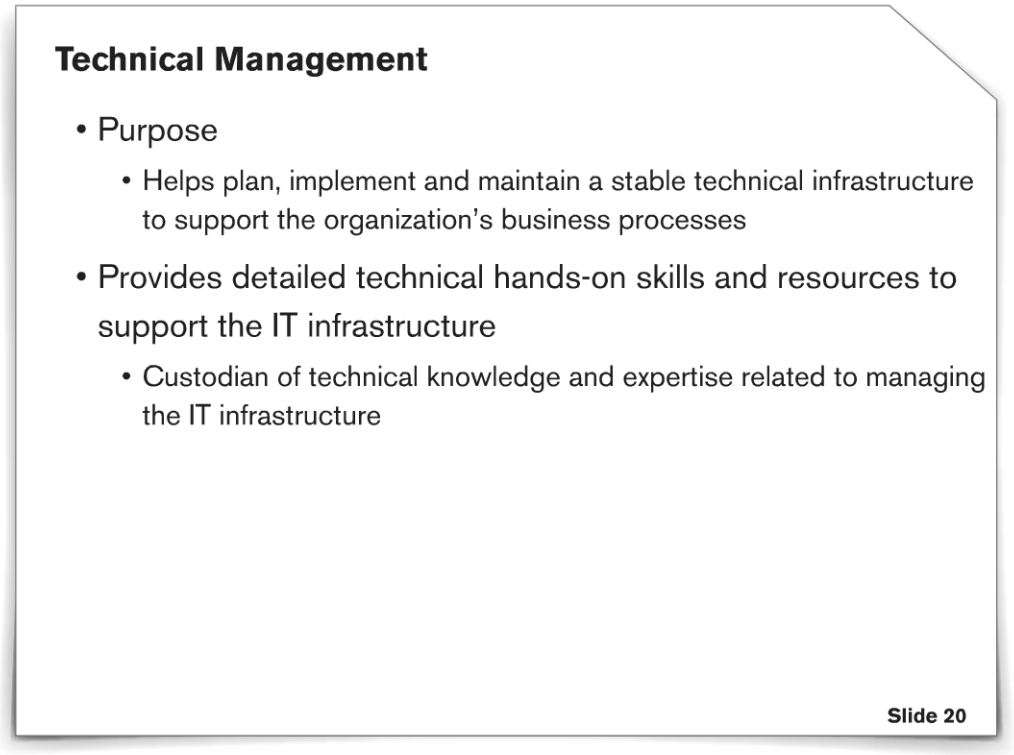



**Service Desk Metrics – Soft Metrics**

When customer or user satisfaction is of interest, we speak about soft measures. With carefully written surveys, the following three aspects may be found:

1. How effectively customers feel their calls have been answered
2. If the Service Desk agent was courteous and professional
3. If the Service Desk agent instilled confidence in the user

Types of Surveys: After-call survey, telephone, email, online, personal or group interview.




**Technical Management**

**PURPOSE**: Helps plan, implement and maintain a stable technical infrastructure to support the organization's business processes

The role of **Technical Management** is to provide detailed technical skills and the resources needed to support the ongoing operation of the IT infrastructure.

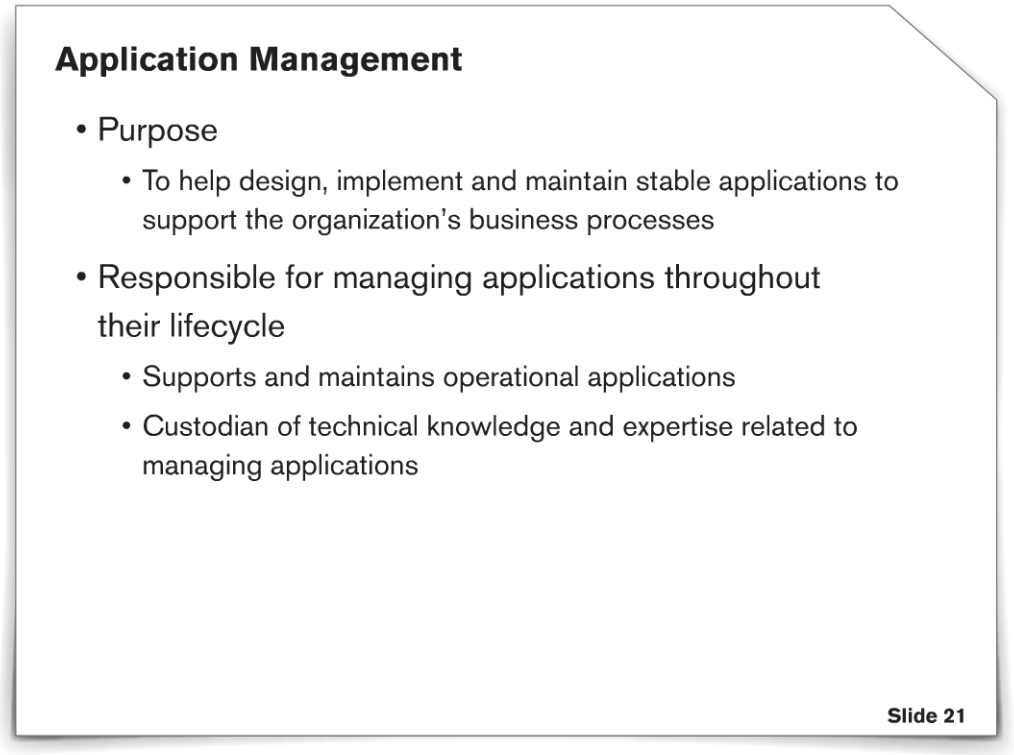
- Technical Management is the custodian of technical knowledge and expertise related to managing the IT infrastructure. The knowledge required to design, test, manage and improve IT services is identified, developed and refined
- This function provides the actual resources to support the IT Service Management Lifecycle. It is responsible for ensuring that resources are effectively trained and deployed to design, build, transition, operate and improve the technology required to deliver and support IT services.

Technical Management consists of Mainframe Management, Server Management and Support, Network Management, Storage and Archive, Database Administration, Directory Services Management, Desktop Support Middleware Management, Internet/Web Management, and Facilities and Data Center Management.

Technical Management will 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
- The swift use of technical skills to speedily diagnose and resolve any technical failures that do occur




**Application Management**

**PURPOSE**: To help design, implement and maintain stable applications to support the organization's business processes.

**Application Management** manages applications throughout their lifecycle. It supports and maintains operational applications and also plays an important role in design, testing and improvement of applications that form part of the IT services. It contributes to the question: Buy or build an application?

Application Management 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 IT Service Management Lifecycle. Furthermore, Application Management provides guidance to IT operations as to how best to implement the ongoing operational management of applications.

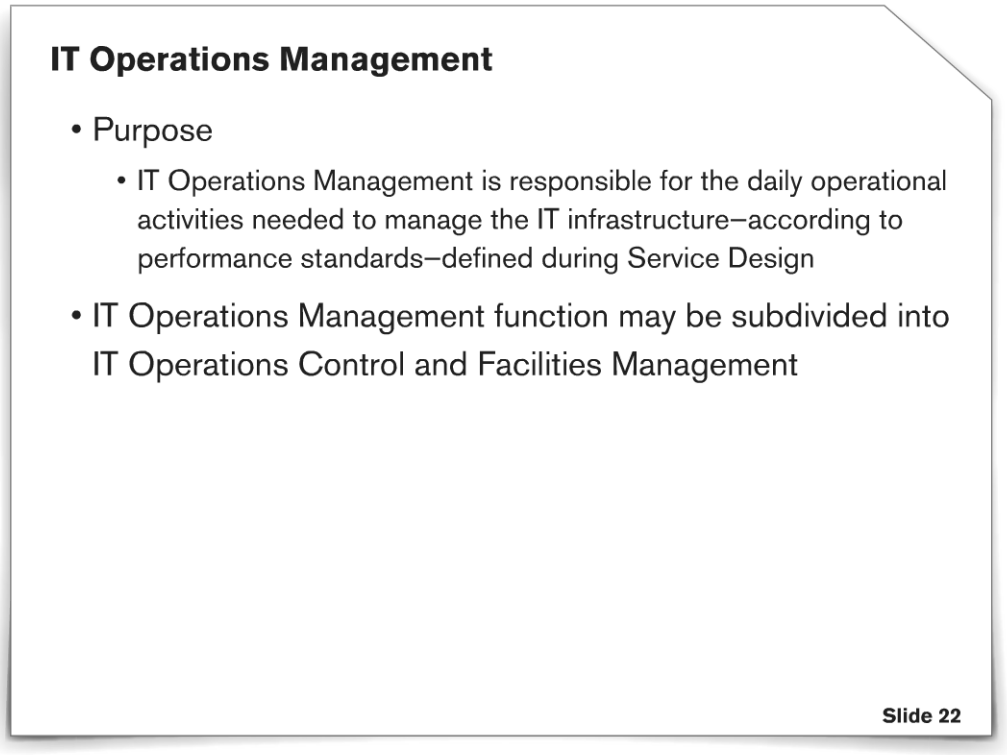
Application Management supports the organization's business processes through:

- Functional and manageable requirements
- Assisting in the design and deployment
- Providing ongoing support and improvement

As a result, the following is achieved:

- Applications that are well designed, resilient and cost-effective
- Assuring that the required functionality is available to achieve the required business outcome
- The organization has adequate technical skills to maintain operational applications in optimum condition
- The swift use of technical skills to speedily diagnose and resolve any technical failure that do occur

| | **Application development versus application management** | |
|---|---|---|
| | **Application development** | **Application management** |
| **Nature of activities** | One-time set of activities to design and construct application solutions | Ongoing set of activities to oversee and manage applications throughout their entire lifecycle |
| **Scope of activities** | Performed mostly for applications developed in house | Performed for all applications, whether purchased from third parties or developed in house |
| **Primary focus** | Utility focus<br>Building functionality for their customer<br>What the application does is more important than how it is operated | Both utility and warranty focus<br>What the functionality is as well as how to deliver it<br>Manageability aspects of the application, i.e. how to ensure stability and performance of the application |




**IT Operations Management**

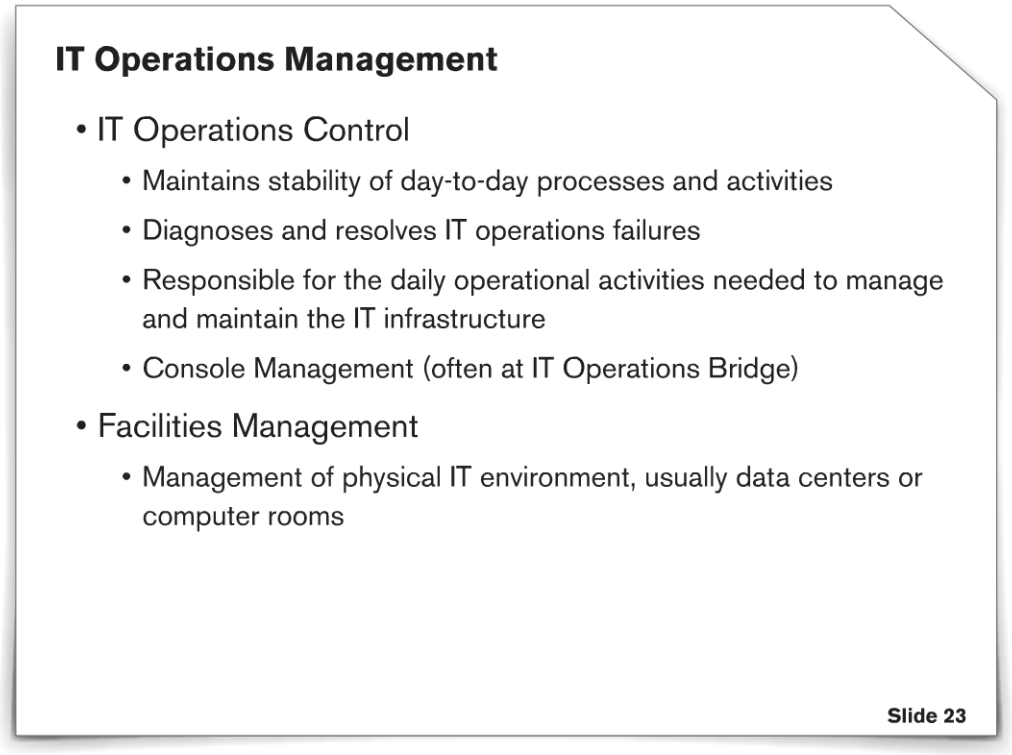
**PURPOSE**: IT Operations Management is responsible for the daily operational activities needed to manage the IT infrastructure–according to performance standards–defined during Service Design.

**IT Operations Management** may be subdivided into **IT Operations Control** and **Facilities Management**. In many organizations Technical and Application management are co-located with IT operations within large data centers. In some organizations many physical components of the IT infrastructure have been outsourced and Facilities Management may include the management of the outsourcing contracts.

As with many IT Service Management 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 IT Operations' role 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 to perform the same function.
- At the same time, IT operations is part of the process that adds value to the different lines of business and supports the value network (see the ITIL Service Strategy book). The ability of the business to meet its objectives and to remain competitive depends upon the output and reliability of the day-to-day operation of IT. As such, IT Operations Management must

continually adapt to business requirements and demand. It is inconsequential to the business if IT operations complies with a standard procedure or that a server performs optimally. As business demand and requirements change, IT Operations Management must be able to keep pace with them, often challenging the status quo.



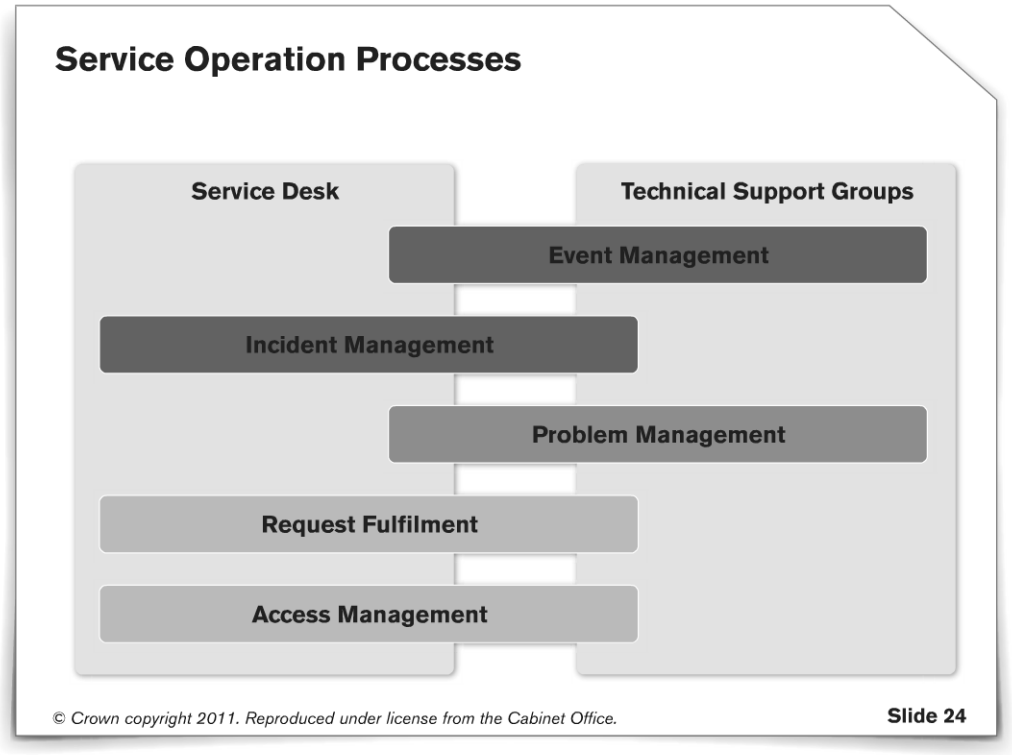

**IT Operations Management**

**IT Operations Control** is responsible for many day-to-day tasks, such as:

- Maintaining stability of day-to-day processes and activities
- Providing regular scrutiny and recommendations to achieve improved service at reduced costs, while maintaining stability
- Diagnosing and resolving IT operations failures
- Responsibility for daily operational activities required to manage and maintain the IT infrastructure
- Console Management (often at the IT Operations Bridge)

The **IT Operations Bridge** refers to the physical room in which many organizations monitor their IT. It provides a central coordination point for managing various classes of events, detecting Incidents, managing routine operational activities and reporting on the status or performance of technology components.

**Facilities Management** focuses more on the physical IT environment, such as data centers or computer rooms.




**Service Operation Processes**

The goal of Service Operation is to enable effectiveness and efficiency in delivery and support of IT services. The processes that support this goal are:

- Event Management
- Incident Management
- Problem Management
- Request Fulfilment
- Access Management

The figure above demonstrates the level of responsibility the Service Desk and the Technical Support Groups (technical, IT operations and Application Management functions) have in the Service Operation processes. Incident Management, Request Fulfilment and Access Management are primarily carried out by the Service Desk, with Event Management and Problem Management as primarily "back-of-house" processes.

## Event Management – Purpose and Objective

- Purpose
  - Monitoring all events that occur throughout the IT infrastructure to allow for "normal" Service Operation and to detect and escalate exceptions
- Objectives
  - 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. (This is covered in detail in ITIL Continual Service Improvement)

**Slide 25**

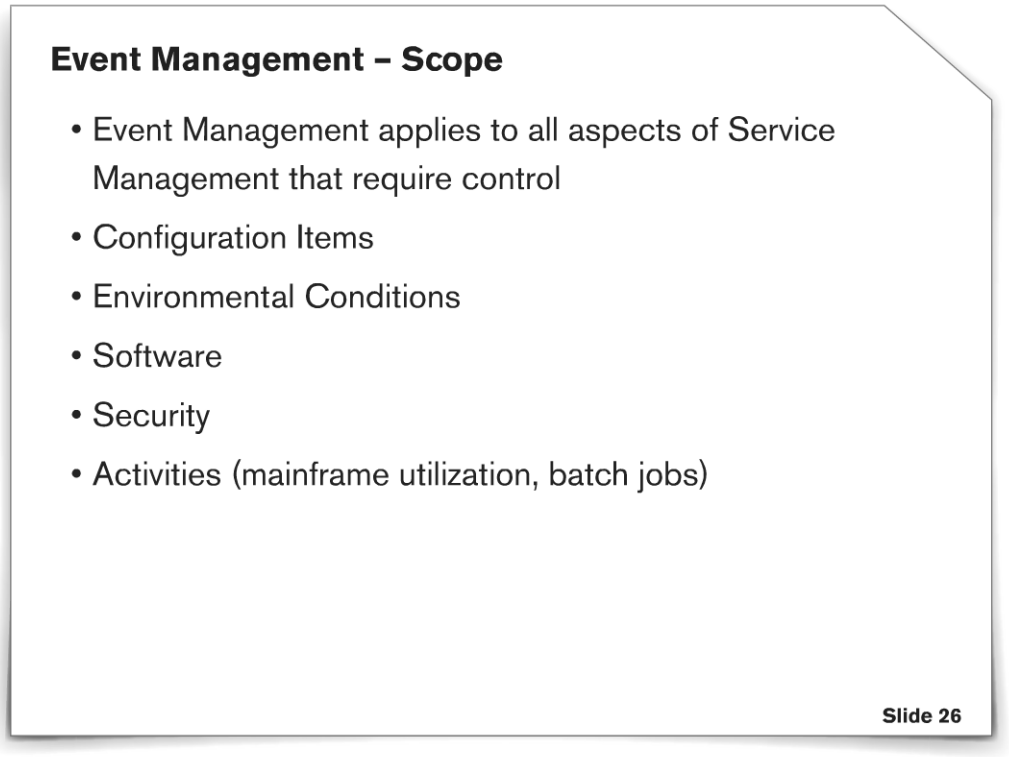
**Event Management – Purpose and Objective**

**PURPOSE**: To enable stability in IT services delivery and support by monitoring all events that occur throughout the IT infrastructure, to allow for "normal" Service Operation and to detect and escalate exceptions.

**Event Management** is a basis for Operational Monitoring and Control, due to its ability to detect events, make sense of them and determine the appropriate control action.

If events are programmed to communicate operational information as well as warnings and exceptions, they may be used as a basis for automating many routine Operations Management activities. Such activities may encompass executing scripts on remote devices, submitting jobs for processing and even dynamically balancing the demand for a service across multiple devices to enhance performance.

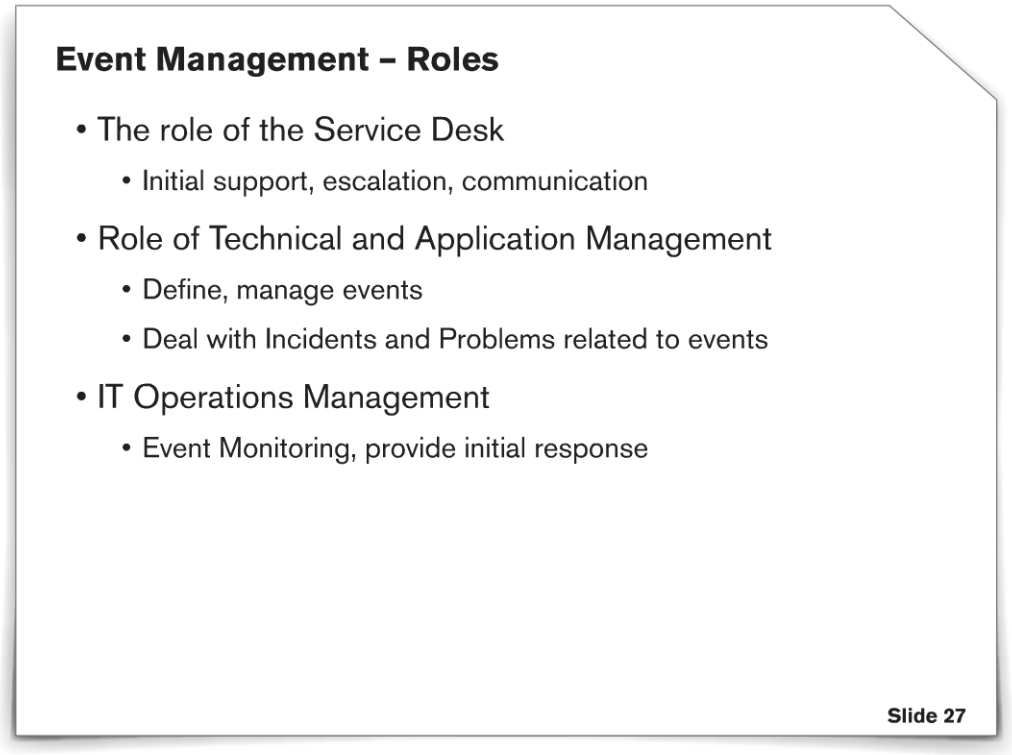
Furthermore, Event Management provides a way of comparing actual performance and behavior against design standards and Service Level Agreements. As such, Event Management also provides a basis for Service Assurance and Reporting and Service Improvement.




**Event Management – Scope**

Event Management could be used on any aspect of Service Management that requires controls and which can be automated. These include:

- Configuration Items:
  - Some CIs will be included because they need to stay in a constant state (e.g., a router on a network needs to be in an active state. Event Management tools confirm this by monitoring responses to "status requests").
  - Other CIs will be included because their status often changes and Event Management can be used to automate this and update the CMS (e.g., the updating of a file server).
- Environmental conditions (e.g., fire and smoke detection)
- Software license monitoring for usage to ensure legal license utilization
- Security (e.g., firewall breach)
- Normal activity (e.g., mainframe utilization, batch job completion)




**Event Management – Roles**

It is unusual for an organization 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 roles of the Service Operation functions within Event Management are listed below.

**The Role of the Service Desk**

The investigation and resolution of events that have been identified as being Incidents will initially be undertaken by the Service Desk and then escalated to the appropriate Service Operation team(s).

The Service Desk is also responsible for communicating information about this type of Incident to the relevant Technical or Application Management team and, where appropriate, the user.

**The Role of Technical and Application Management**

Technical and Application Management play several important roles as follows:

- During Service Design: Classify events, update correlation engines, and ensure that any autoresponses are defined
- During Service Transition: Test the service, ensure that events are properly generated and that the defined responses are appropriate

- During Service Operation: These teams will typically perform Event Management for the systems under their control
- Will also be involved in dealing with Incidents and Problems related to events

**The Role of IT Operations Management**

Event Monitoring and first-line response to be delegated to IT Operations Management.

## Incident Management – Purpose

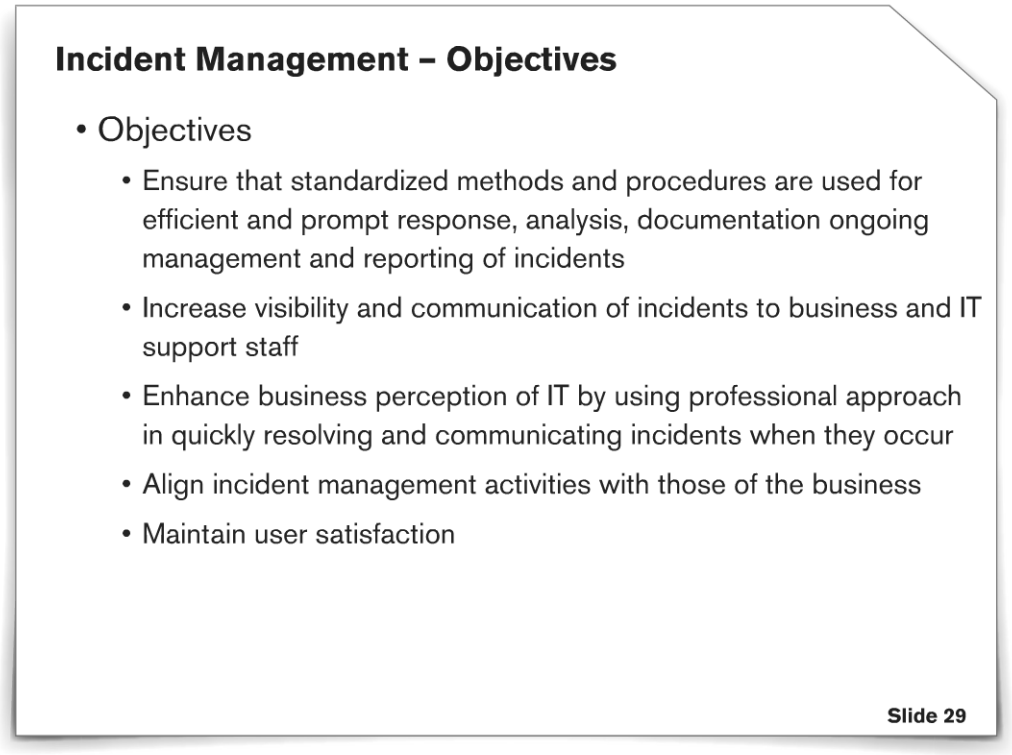
- Purpose
  - Restore normal Service Operation as quickly as possible
  - Minimize the adverse impact on business operations
  - Ensure service quality and availability are maintained

Slide 28

**Incident Management – Purpose**

**PURPOSE**: To restore normal Service Operation *as quickly as possible* and minimize the adverse impact on business operations, thus ensuring that the best possible levels of service quality and availability are maintained.

**Incident Management is the process for dealing with all Incidents**. This may include failures, questions or queries reported by the users (usually via a telephone call to the Service Desk), by technical staff, or automatically detected and reported by event monitoring tools.




**Incident Management – Objectives**

The main **objectives** of Incident Management are to:

- Resolve the service disruption as quickly as possible–at least within the targeted time as documented in the Service Level Agreement. *Normal Service Operation* is defined as "Service Operation within Service Level Agreement (SLA) limits."
- Maintain a constant stream of communication between the IT organization and its customers, concerning the status in relation to a service disruption (e.g., escalation, estimated time until solved, etc.).
- Evaluate an Incident to determine whether it is likely to reoccur and/or if it is the symptom of a chronic Problem. If so, inform Problem Management about the Incident.

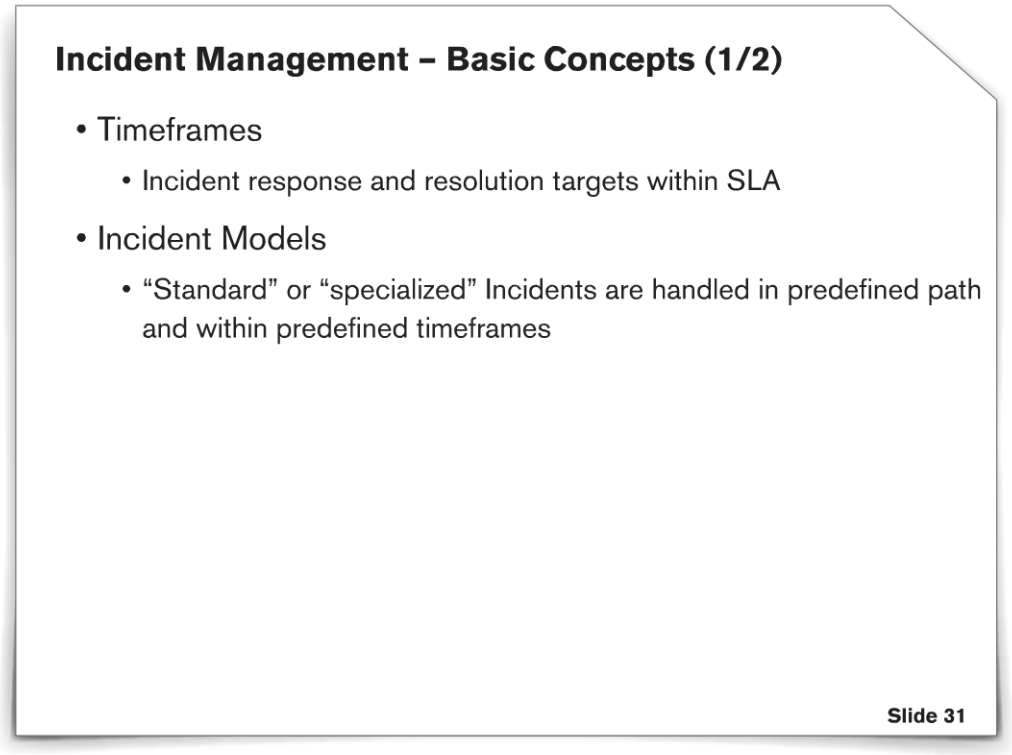
## Incident Management – Scope

- Scope
  - Incident Management includes any event which disrupts, or which could disrupt, a service.
  - Incidents reported (or logged) by technical staff, tools, user(s), etc.

Slide 30

**Incident Management – Scope**

The scope of Incident Management includes all Incidents and any event which disrupts, or which could disrupt, a service. This does not imply that all events are Incidents, since many classes of events are indicators of normal operation or simply provide information.




**Incident Management – Basic Concepts (1/2)**

**Timeframes**

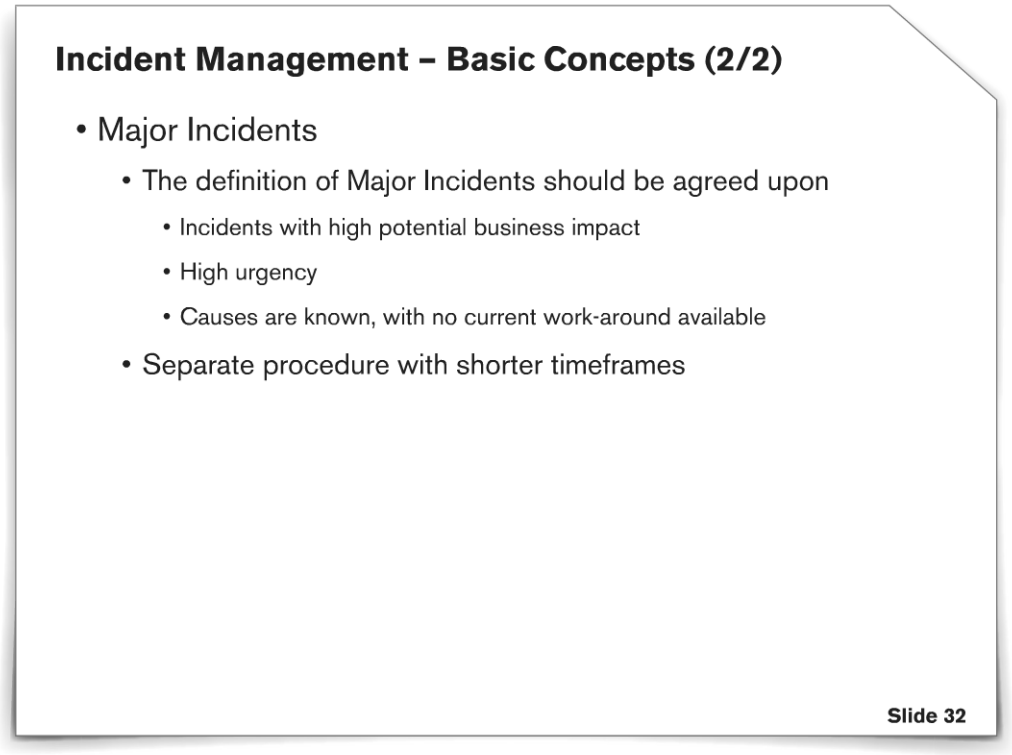
Timeframes must be agreed upon for all Incident handling stages (these will differ depending upon the priority level of the Incident)—based upon the overall Incident response and resolution targets within Service Level Agreements—and captured as targets within Operational Level Agreements and Underpinning Contracts. All support groups must know these timeframes and Service Management tools should be automated accordingly.

**Incident Models**

An Incident Model is a way of predefining the steps required to handle a process (in this case a process for dealing with a particular type of Incident) in an agreed upon way. Support tools may then be used to manage the required process. This will ensure that "Standard" Incidents are handled in predefined path and within predefined timeframes. "Specialized" (e.g., security related) Incidents will be routed to Information Security Management.

An Incident Model includes the following:

- Steps taken to handle the Incident
- Chronological order
- Responsibilities timeframes
- Escalation procedures



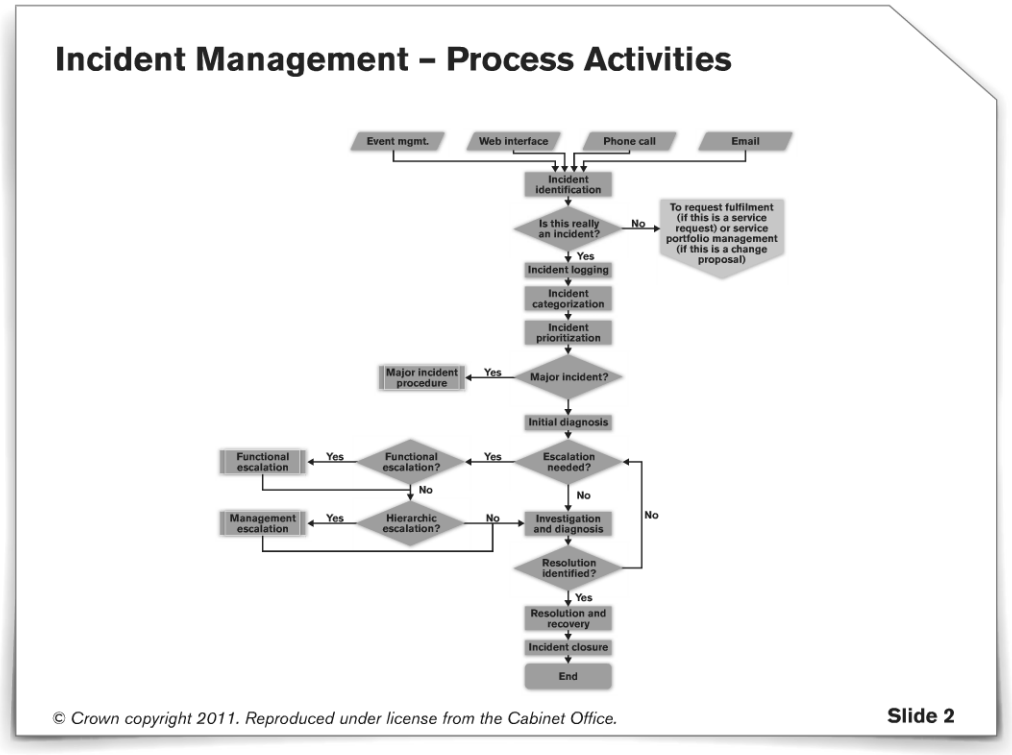

**Incident Management – Basic Concepts (2/2)**

**Major Incidents**

It is very important for organizations to agree upon the definition of major Incidents. *Possible* characteristics may include:

- Incidents with high potential business impact
- High urgency
- Causes are known, with no current work-around available

For Major Incidents, a separate procedure with shorter timeframes and greater urgency must be used. In addition, some lower priority Incidents with high potential business impact may be handled in this way.




**Incident Management – Process Activities**

**Identification**: Used for tracking, assisting in finding solutions and compiling historical information for future use and reporting.

**Logging**: The Incidents must be fully logged and date/time stamped, regardless of whether they are raised through a Service Desk telephone call or automatically detected via an event alert.

**Categorization**: Grouping of Incidents according to the necessity, for example, by origin or associated support group. If the Incident is a Service Request, the appropriate Service Request procedure would be followed.

**Prioritization**: Will determine how the Incident is handled. In consultation with the customer, the Service Desk will determine the priority based upon impact and urgency. If it is a Major Incident, the appropriate Major Incident procedure would be followed.

**Initial Diagnosis**: The Service Desk Operator (SDO) must carry out initial diagnosis. Use of diagnostic scripts and Known Error information may be valuable for this. If possible, the SDO will resolve the Incident and close the Incident if the resolution is successful.

If the Service Desk Operator cannot resolve the Incident, the user should be given the Incident reference number, and attempt to find a resolution.

If an escalation is needed, the appropriate escalation procedure is followed.

**Investigation and Diagnosis**: Each of the support groups involved with the Incident handling will investigate and diagnose, while maintaining a historical record of activities.

**Resolution and Recovery**: When a resolution has been identified and sufficiently tested, and the recovery action is completed assuring that the service has been fully restored to the user(s), the Incident Record must be updated with detailed information.

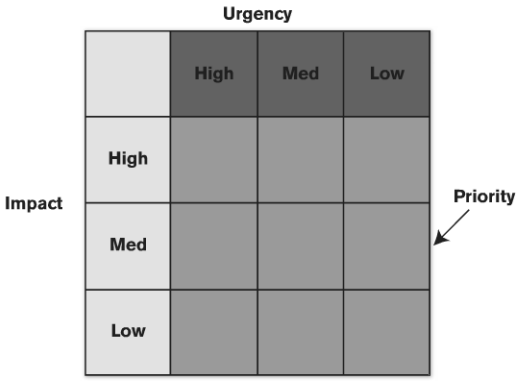
**Closure**: The Service Desk should check that the Incident is fully resolved and that the users are satisfied and willing to agree the Incident may be closed.

## Incident Management – Prioritization

Priority = Urgency x Impact

Impact = Effect upon the business

Urgency = Extent to which the resolution can bear delay






Slide 33

### Incident Management – Prioritization

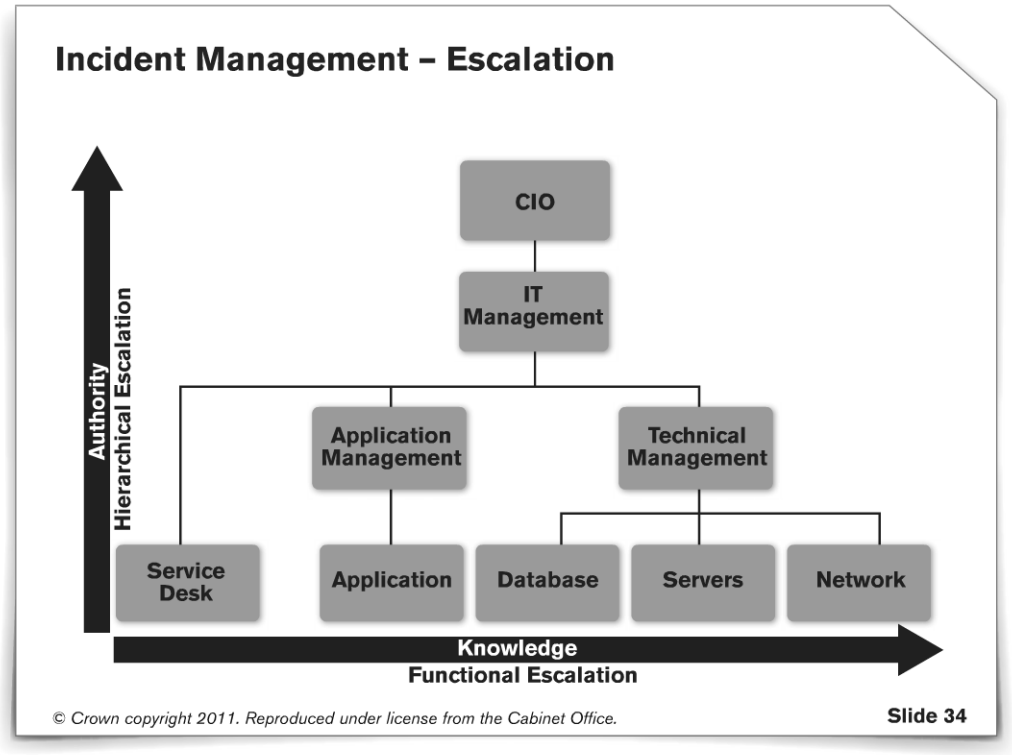
It is important to be able to establish the priority of Incidents and determine which Incidents should be handled first.

**Priority**: Order in which calls are processed, based on impact, urgency and dependent upon resource availability (time, money, people).

**Impact** is determined by the effect upon the activities of the business, and **urgency** is determined by how quickly the Incident must be resolved. The Service Desk determines the priority of Incidents as they receive them. In consultation with the customer, the Service Desk will derive the priority from the impact and urgency of the Incident, considered against the criteria described in the Service Level Agreement. When determining impact, Service Desk staff should take into consideration:

- Risk to life or limb
- The number of services affected–there may be multiple services
- The level of financial losses
- Effect upon business reputation
- Regulatory or legislative breaches
- *Impact is not about the technical complexity of resolution*

By prioritizing calls, second-line support will know which calls require more urgent attention than others and in what order they should be addressed. Priority is not simply about queuing Incidents for resolution; it is also about the resources (time, staff, expertise, research and third party support) that will be allocated to resolution. In practical terms, sometimes a low priority Incident may be allowed to miss its resolution target time, so that a higher priority Incident may meet its target.




**Incident Management – Escalation**

Incident routing is known as horizontal or functional escalation and occurs primarily due to a lack of knowledge or expertise. As soon as it becomes clear that the Service Desk is unable to resolve the Incident itself, the Incident must be immediately escalated for further support. If the organization has a second-level support group and the Service Desk believes that the Incident may be resolved by that group, it should refer the Incident to them. If the second-level support group cannot solve the Incident it must be escalated to the third-level support group. (This could be internal or an external third party.) The rules for escalation and handling of Incidents must be agreed upon in OLAs and UCs with internal and external groups respectively.

When referring Incidents, care should be taken by the Service Desk to ensure that SLA resolution times are not exceeded.

*Vertical* or *hierarchical escalation* may occur at any moment during the Incident Lifecycle. It usually occurs when major Incidents are reported or when it becomes apparent that an Incident will not be resolved in time resulting in breached SLAs. This allows the relevant authority to take corrective action.

Escalation *never* turns an Incident into a Problem, although it may result in ownership of an Incident passing to the Problem manager for administrative reasons and/or the identification of an associated Problem.

*The Service Desk owns the Incident throughout its lifecycle, regardless of where it has been escalated*. The Service Desk is responsible for tracking progress, keeping users informed and ultimately for Incident closure.

## Incident Management – Metrics

- The KPIs (Key Performance Indicators) for Incident Management are:
  - Percentage of Incidents handled within agreed upon resolution time
  - Percentage of Incidents assigned incorrectly
  - Percentage of Incidents resolved by the Service Desk (and by the networking team, etc.)
  - Number of Incidents processed per agent

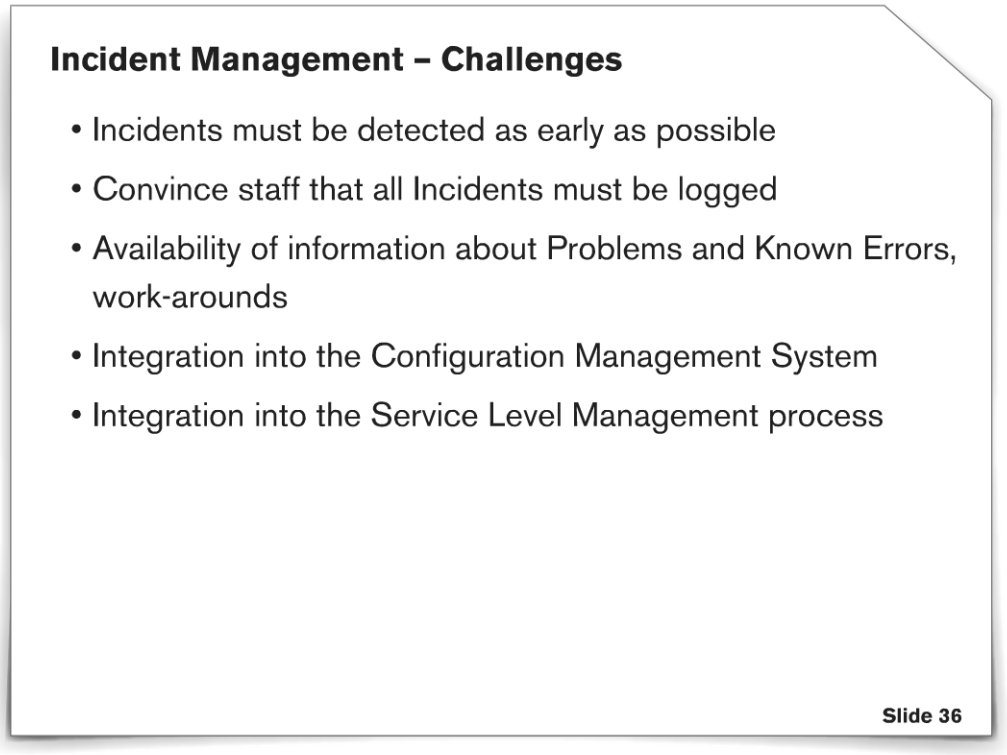
Slide 35

**Incident Management – Metrics**

Under the authority of the Incident Manager and in collaboration with the Service Desk and support groups handling Incidents, reports should be made to judge the efficiency and effectiveness of the Incident Management process and its operation. The report should be distributed to IT Services Management and specialist support groups. It may also be made available to users and customers, for instance as SLA reports.

Incident Management reports may include:

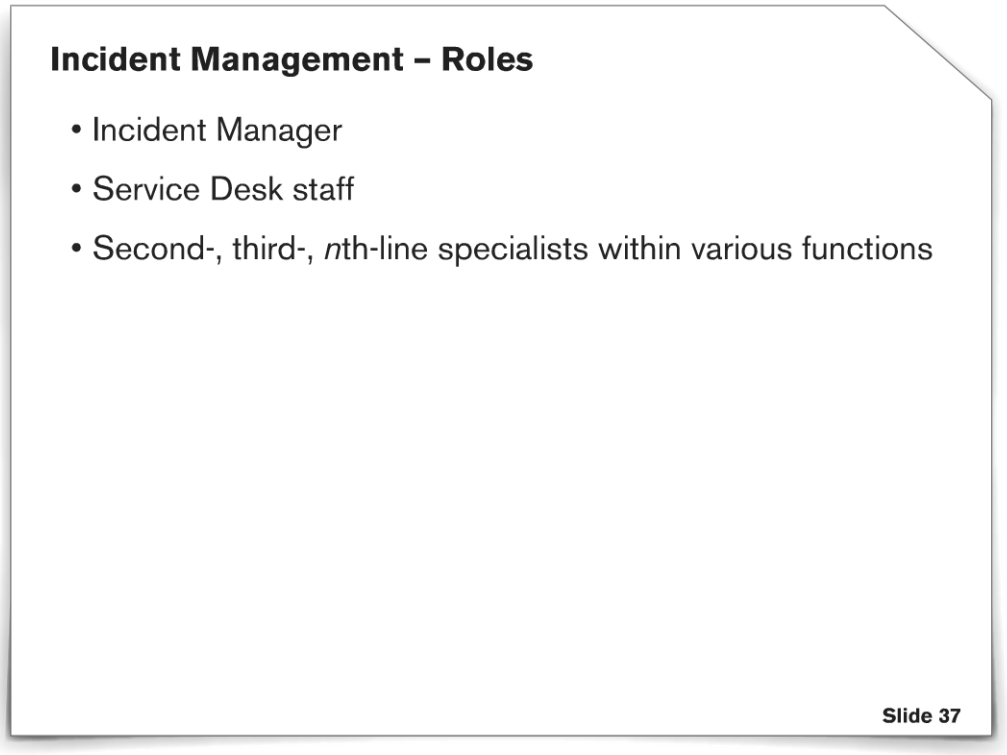
- Size of current Incident backlog
- Number and percentage of major Incidents
- Mean elapsed time to achieve Incident resolution or circumvention, broken down by impact code
- Percentage of Incidents handled within the agreed upon resolution time
- Number and percentage of Incidents incorrectly assigned
- Number and percentage of Incidents incorrectly categorized
- Percentage of Incidents closed by the Service Desk without being referred to other levels of support (often referred to as “first-call resolution rate”)




**Incident Management – Challenges**

The following **challenges** must be addressed to ensure the success of Incident Management:

- Earliest possible detection of Incidents is a challenge, as most of the Incidents are detected or reported late, which results in higher unavailability of the service. This requires user education, the use of super-users, or Event Management tools.
- Convince staff that all Incidents must be logged. Offer users various ways of logging calls: phone, email, web form, etc. Educate the users as to the benefits of logging an Incident and encourage the use of self-help tools.
- Poor quality of Problem and/or Known Error Records will cause delays in resolution of Incidents, as they will have to be reinvestigated.
- Access to the Configuration Management System lets support staff determine the relationships of CIs, and helps them understand the history of CIs when performing first-line support
- A good understanding of Service Level Agreements will assist Incident Management to correctly assess the impact and priority of Incidents. It will also help to define and execute escalation procedures, resulting in an increased customer satisfaction and more efficient use of resources.




**Incident Management – Roles**

The following roles are needed for the Incident Management process:

**Incident Manager**

An Incident Manager has the responsibility for:

- Driving the efficiency and effectiveness of the Incident Management process
- Producing management information
- Managing the work of Incident support staff (first- and second-line)
- Monitoring the effectiveness of Incident Management and making recommendations for improvement
- Developing and maintaining the Incident Management systems
- Managing major Incidents
- Developing and maintaining the Incident Management process and procedures

**Service Desk**

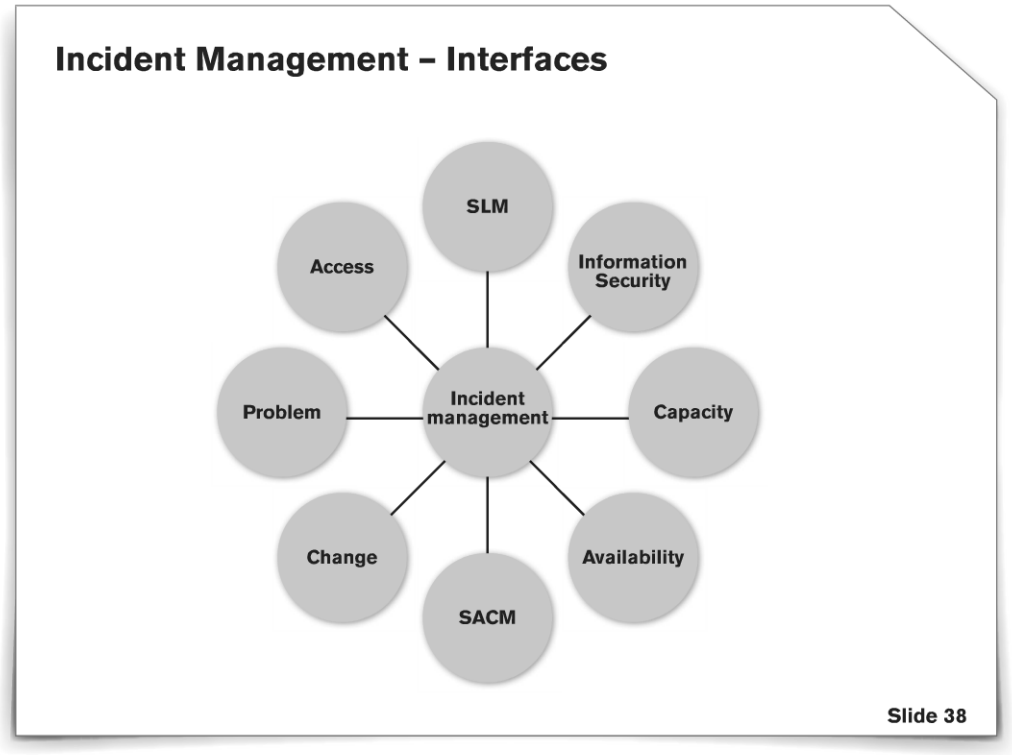
The Service Desk will handle first-line Incidents.

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-to-day basis. They give initial response and support for the detected Incidents. It is the responsibility of the Service Desk to log and record ALL Incidents, perform Incident classification and categorization and match Incidents to existing Incidents or Problem Records. **The Service Desk must also manage communications with end-users**.

Finally, it is the responsibility of the Service Desk to handle the Incident closure action, which includes checking that the Incident is fully resolved and that the users are satisfied and willing to agree the Incident can be closed.

Second-, third- and *n*th-line specialists within various functions:

- Handle escalated Incidents
- Involve third parties, suppliers as required




**Incident Management - Interfaces**

**Service Design**

- Service Level Management. Management. The ability to resolve incidents in a specified time is a key part of delivering an agreed level of service. Incident management enables SLM to define measurable responses to service disruptions. It also provides reports that enable SLM to review SLAs objectively and regularly. In particular, incident management is able to assist in defining where services are at their weakest, so that SLM can define actions as part of the service improvement plan (SIP) (see *ITIL Continual Service Improvement* for more details). SLM defines the acceptable levels of service within which incident management works, including:
  - Incident response times
  - Impact definitions
  - Target fix times
  - Service definitions, which are mapped to users
  - Rules for requesting services
  - Expectations for providing feedback to users.

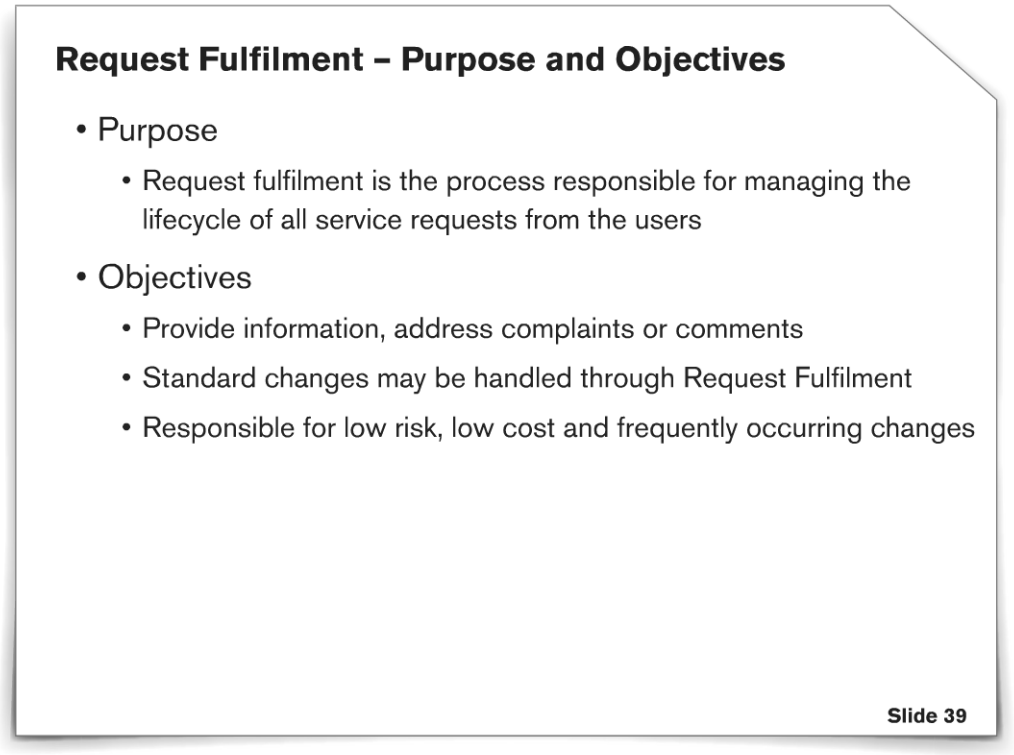
- **Information Security Management**. Providing security-related incident information as needed to support service design activities and gain a full picture of the effectiveness of the security measures as a whole based on an insight into all security incidents. This is facilitated maintaining log and audit files and incident records
- **Capacity Management**. Incident management provides a trigger for performance monitoring where there appears to be a performance problem. Capacity management may develop workarounds for incidents.
- **Availability Management**. Availability management will use incident management data to determine the availability of IT services and look at where the incident lifecycle can be improved.

**Service Transition**

- **Service Asset and Configuration Management**. This process provides the data used to identify and progress incidents. One of the uses of the CMS is to identify faulty equipment and to assess the impact of an incident. The CMS also contains information about which categories of incident should be assigned to which support group. In turn, incident management can maintain the status of faulty CIs. It can also assist service asset and configuration management to audit the infrastructure when working to resolve an incident.
- **Change management**. Where a change is required to implement a workaround or resolution, this will need to be logged as an RFC and progressed through change management. In turn, incident management is able to detect and resolve incidents that arise from failed changes.

**Service Operation**

- **Problem Management**. For some incidents, it will be appropriate to involve problem management to investigate and resolve the underlying cause to prevent or reduce the impact of recurrence. Incident management provides a point where these are reported. Problem management, in return, can provide known errors for faster incident resolution through workarounds that can be used to restore service.
- **Access Management**. Incidents should be raised when unauthorized access attempts and security breaches have been detected. A history of incidents should also be maintained to support forensic investigation activities and resolution of access breaches.




**Request Fulfilment – Purpose and Objectives**

**PURPOSE**: Request fulfilment is the process responsible for managing the lifecycle of all service requests from the users.

Scope: 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. For each request, these activities should be documented into a request model and stored in the SKMS.

Request Fulfilment provides a channel for users to request and receive standard services for which a predefined approval and qualification process exists. It provides information to users and customers about the availability of services and the procedure for obtaining them.

This process is responsible for sourcing and delivering the components of requested standard services (e.g., licenses and software media) and assisting with general information, complaints or comments regarding a service. Request Fulfilment also deals with standard changes that have been defined by Change Management (e.g., users asking for a password reset).

## Request Fulfilment – Roles

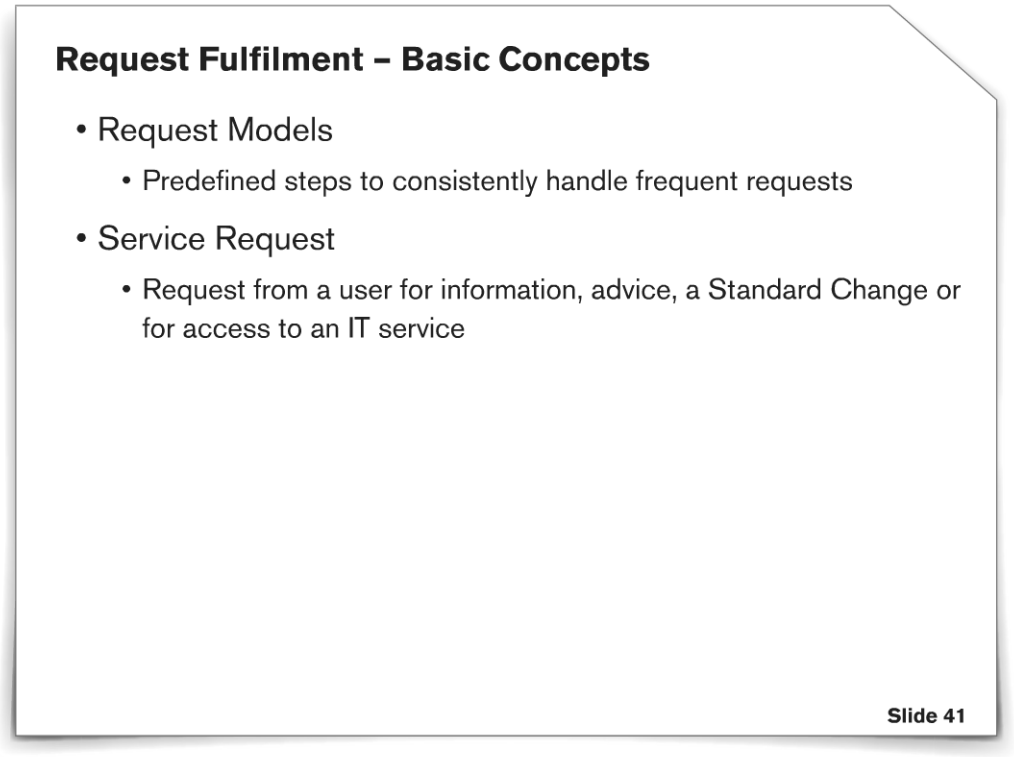
- Service Desk staff
  - Service Desk and Incident Management staff provides initial response and handles the request
- Staff in other appropriate functions
  - Responsible for ensuring eventual fulfillment of the request
- External Suppliers, as appropriate
  - As per the request from the organizations, fulfill the Service Request

Slide 40

**Request Fulfilment – Roles**

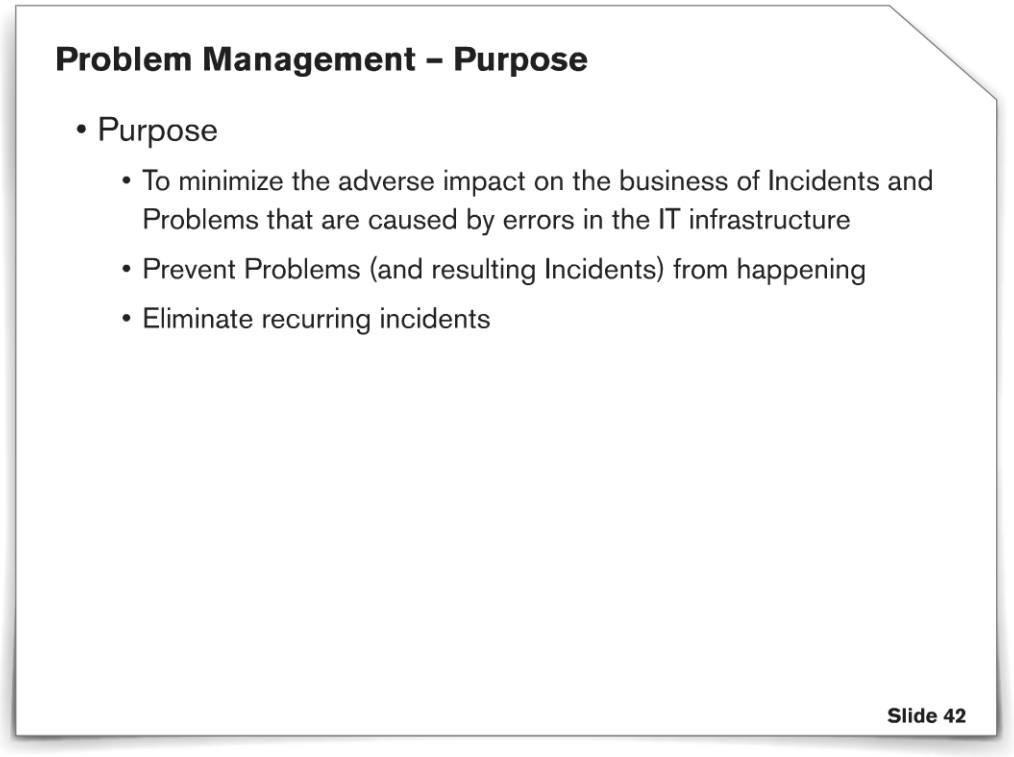
Initial handling of Service Requests will be undertaken by the Service Desk and Incident Management staff. Eventual fulfillment of the request will be undertaken by the proper Service Operation team(s) or departments and/or by external suppliers, as appropriate. Often, Facilities Management, procurement and other business areas aid in the fulfillment of Service Requests.

In exceptional cases where a very high number of Service Requests are handled or where the requests are of critical importance to the organization, it may be appropriate to have one or more of the Incident Management teams dedicated to handling and managing Service Requests.




**Request Fulfilment – Basic Concepts**

Certain Service Requests will regularly occur and will require handling in a consistent manner to meet agreed upon service levels. To assist with this, many organizations will wish to create predefined Request Models (that typically include some form of pre-approval by Change Management).




**Problem Management – Purpose**

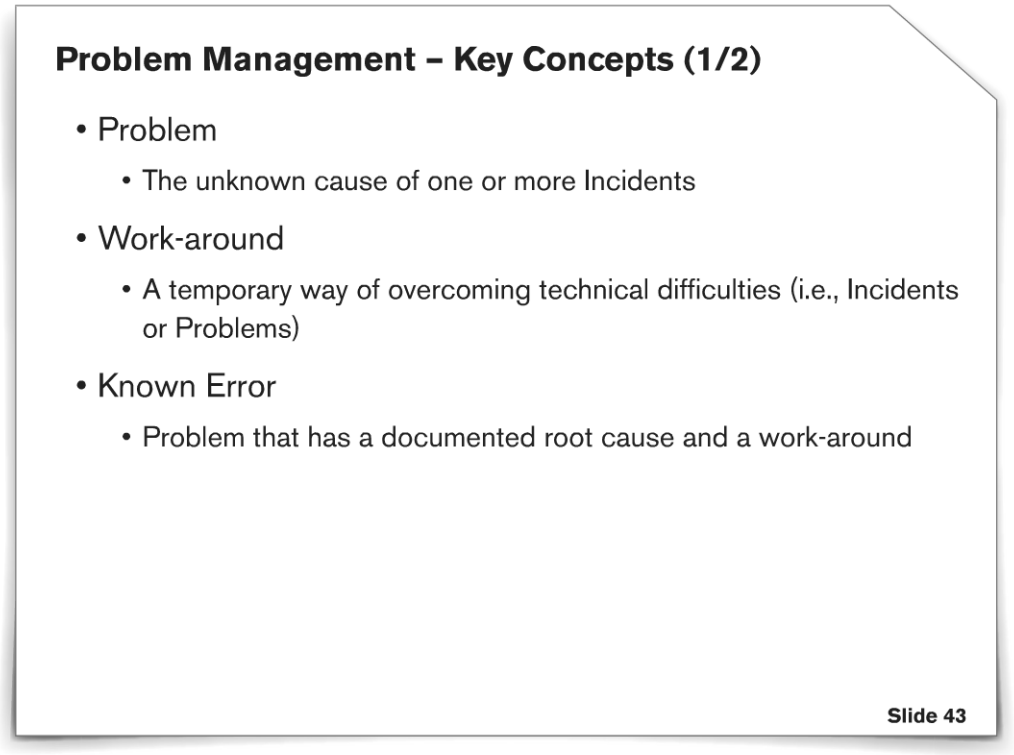
**PURPOSE**: To minimize the adverse impact of Incidents and Problems on the business that are caused by errors within the IT infrastructure, and to prevent the recurrence of Incidents related to these errors

ITIL defines a **Problem** as "*the unknown cause of one or more Incidents*."

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

Although Incident and Problem Management are separate processes, they are closely related and will typically use the same tools, and may use similar categorization, impact and priority coding systems. This will ensure effective communication when dealing with related Incidents and Problems.

The main difference between Problem Management and Incident Management is that Problem Management uses techniques that address the root-cause of the symptoms and Incident Management uses techniques that address the symptoms only.




**Problem Management – Key Concepts (1/2)**

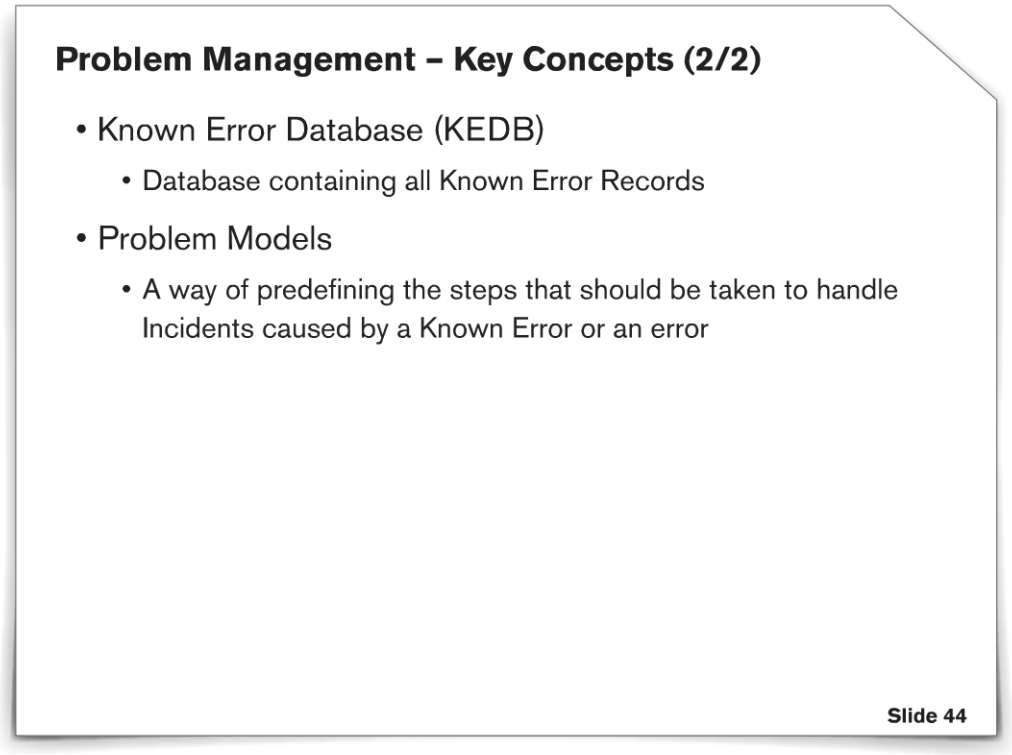
**Problem**

The unknown cause of one or more Incidents is a Problem.

**Known Error**

Known Errors have a known underlying cause.

When diagnosis is complete and particularly when a work-around has been found (even though it may not yet be a permanent resolution), a Known Error Record must be raised and placed in the Known Error Database. This ensures that if further Incidents or Problems arise, that they may be identified and the service restored more quickly. There may also be scenarios where a permanent solution has been identified, but not yet applied; in that case, an error should be recorded in the Known Error Database.




**Problem Management – Key Concepts (2/2)**

**Known Error Database (KEDB)**

The purpose of a Known Error Database is to allow storage of Incidents and Problems—and how they were overcome—to allow quicker diagnosis and resolution if they recur.

The Known Error Record should hold exact details of the fault and the symptoms that occurred, together with precise details of any work-around or resolution action that may have been taken to restore the service and/or resolve the Problem.

The Known Error Database is used in the Incident Management process as an initial diagnosis activity to determine if any Incidents with the same or similar symptoms already exist. If they do exist, most likely there is a work-around that may be used to restore the service.

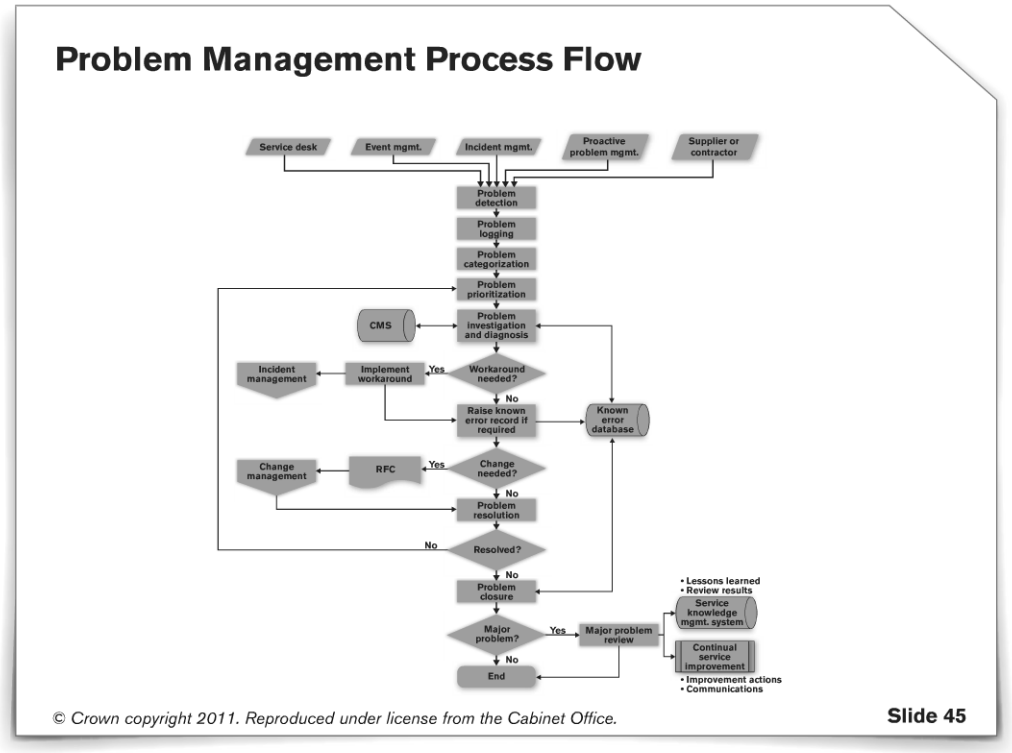
The Known Error Database is owned by Problem Management.

**Problem Model**

Many Problems will be unique and will require handling in an individual way. However, it is conceivable that some Incidents may reoccur because of dormant or underlying Problems (for example, where the cost prohibits a permanent resolution, so leadership decides to instead "live with the Problem").

A Problem Model is a way of predefining the steps that should be taken to handle a process (in this case a process for dealing with a particular type of Problem) in an agreed upon way. Support

tools may then be used to manage the required process. This will ensure that "standard" Problems are handled in a predefined path and within predefined timeframes. This is similar concept to Incident Models.




## Problem Management Process Flow

### *Problem Detection*

It is likely that multiple ways of detecting Problems will exist in all organizations. These will include:

- Suspicion or detection of an unknown cause of one or more Incidents by the Service Desk,
- Analysis of an Incident by a technical support group
- Automated detection of an infrastructure or application fault, using event/alert tools
- A notification from a supplier or contractor that a Problem exists that has to be resolved.
- Analysis of Incidents as part of proactive Problem Management – resulting in the need to raise a Problem Record so that the underlying fault can be investigated further.

### *Problem Logging*

Regardless of the detection method, all the relevant details of the Problem must be recorded so that a full historic record exists. This must be date and time stamped to allow suitable control and escalation.

### *Problem Categorization*

Problems must be categorized in the same way as Incidents (and it is advisable to use the same coding system) so that the true nature of the Problem can be easily traced in the future and meaningful management information can be obtained.

### *Problem Prioritization*

Problems must be prioritized in the same way and for the same reasons as Incidents – but the frequency and impact of related Incidents must also be taken into account. Problem prioritization should also take into account the severity of the Problems.

### *Problem Investigation and Diagnosis*

An investigation should be conducted to try to diagnose the root cause of the Problem – the speed and nature of this investigation will vary depending upon the impact, severity and urgency of the Problem – but the appropriate level of resources and expertise should be applied to finding a resolution commensurate with the priority code allocated and the service target in place for that priority level.

### *Work-arounds*

In some cases it may be possible to find a work-around to the Incidents caused by the Problem – a temporary way of overcoming the difficulties. In cases where a work-around is found, it is therefore, important that the Problem Record remains open, and details of the work-around are always documented within the Problem Record.

### *Raising a Known Error Record*

As soon as the diagnosis is complete, and particularly where a work-around has been found (even though it may not yet 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*

Ideally, as soon as a solution has been found, it should be applied to resolve the Problem – but in reality safeguards may be needed to ensure that this does not cause further difficulties. **Note**: There may be some Problems for which a Business Case for resolution cannot be justified (e.g. where the impact is limited but the cost of resolution would be extremely high). In such case, a decision may be taken to leave the Problem Record open but to use a work-around description in the Known Error Record to detect and resolve any recurrences quickly.

### *Problem Closure*

When any change has been completed (and successfully reviewed), and the resolution has been applied, the Problem Record should be formally closed – as should any related Incident Records that are still open. The status of any related Known Error Record should be updated to shown that the resolution has been applied.

### *Major Problem Review*

After every major Problem (as determined by the organization's priority system), while memories are still fresh a review should be conducted to learn any lessons for the future. Specifically, the review should examine:

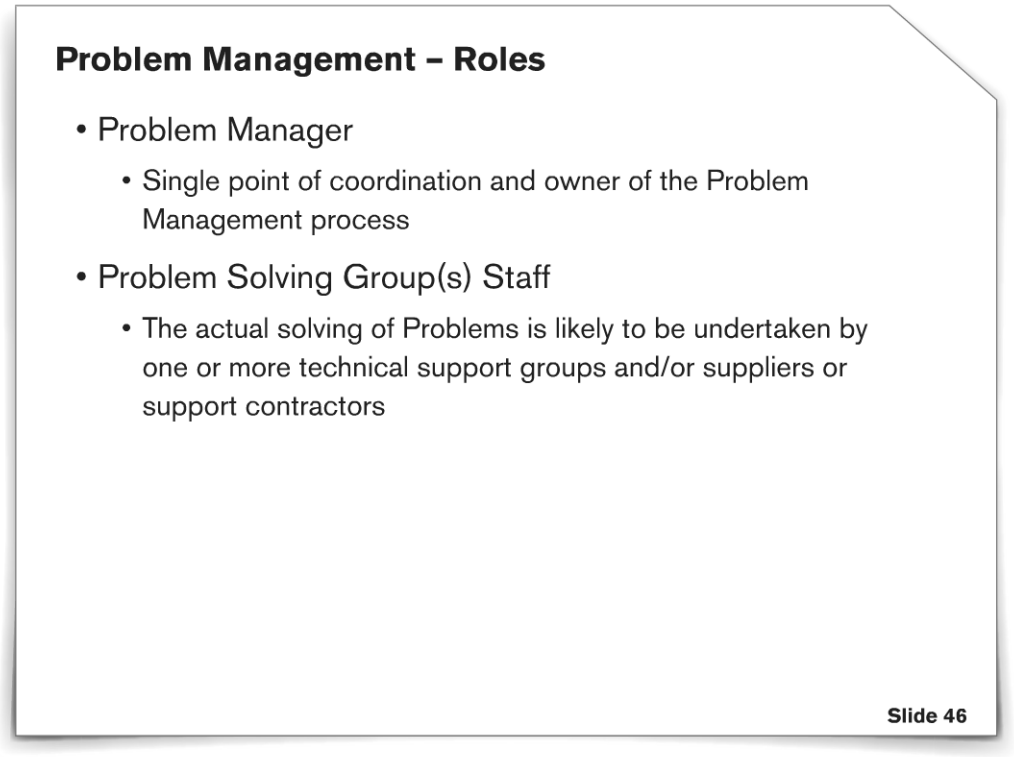
- Those things that were done correctly
- Those things that were done wrong

- What could be done better in the future
- How to prevent recurrence
- Whether there has been any third-party responsibility

***Errors detected in the development environment***

It is rare for any new applications, systems or software releases to be completely error-free. It is more likely that during testing of such new applications, systems or releases a prioritization system will be used to eradicate the more serious faults, but it is possible that minor faults are not rectified – often because of the balance that has to be made between delivering new functionality to the business as quickly as possible and ensuring totally fault free code or components.

Where a decision is made to release something into the production environment that includes known deficiencies, these should be logged as Known Errors in the KEDB, together with details of work-arounds or resolution activities.




**Problem Management – Roles**

**Problem Manager**

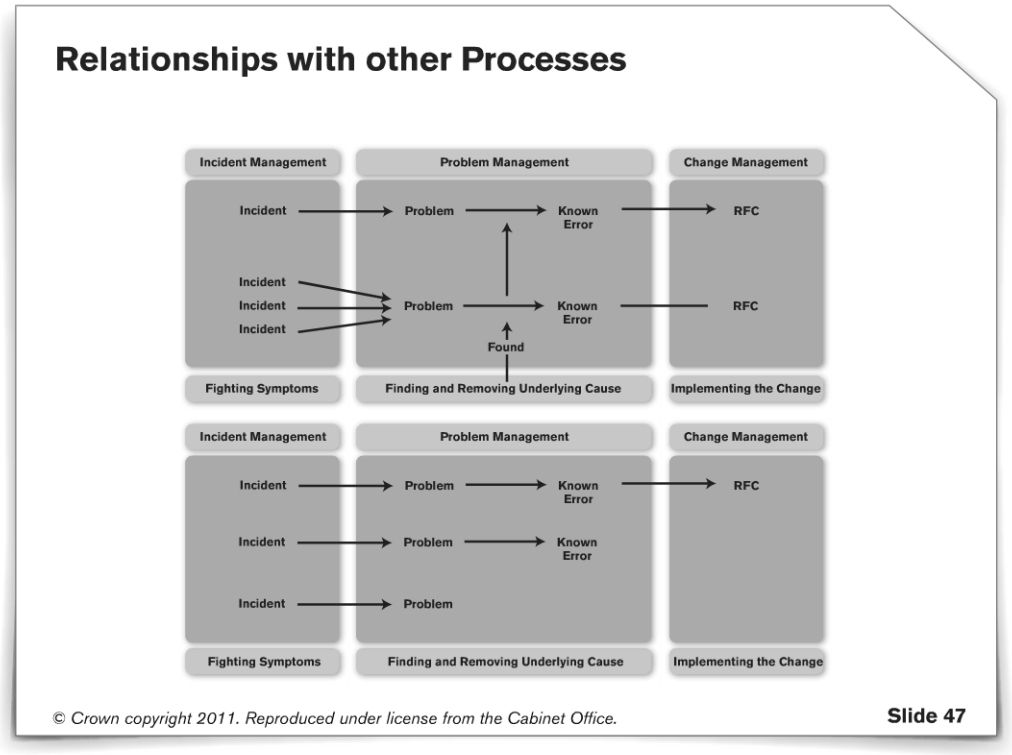
The Problem manager is the single point of coordination and owner of the Problem Management process, with responsibilities that include:

- Coordinating all Problem Management activities
- Acting as the liaison with all Problem resolution groups to ensure the swift resolution of Problems within SLA targets
- Ownership and protection of the Known Error Database
- Gatekeeper for the inclusion of all Known Errors and management of search algorithms
- Formal closure of all Problem Records
- Acting as the liaison with suppliers and contractors to ensure that third parties fulfill their contractual obligations for Problem resolution
- Arranging, running, documenting and all follow-up activities relating to Major Problem Reviews

**Problem Solving Groups**

The actual solving of Problems is likely to be undertaken by one or more technical support groups and/or suppliers or support contractors under the coordination of the Problem manager.

When an individual Problem is serious enough to warrant it, a dedicated Problem Management team should be assembled to work together in overcoming that particular Problem. The Problem manager will help ensure that the correct number and level of resources is available on the team, and manage the escalation and communication up the management chain of all organizations concerned.




### Relationships with other Processes

It is possible for Problems to be identified and corrected in various ways. One of the primary benefits of Problem Management is demonstrated in the "Many to One" relationship between Incidents and Problems. This enables an IT Service Provider to resolve many Incidents in an efficient manner by correcting the underlying root cause.

However, it may be seen that not all Problems are diagnosed, perhaps because the root cause of the Problem is not always found. It may also be seen that some Known Errors are not fixed. Some possible explanations for this may include costs that exceed the benefits of fixing the error, or that the error may be fixed by an upcoming patch or update from a third party.

## Access Management – Purpose

- Purpose
  - To grant authorized users the right to use a service while *preventing* access to non-authorized users in order to protect the confidentiality, integrity and availability (CIA) of information and infrastructure
- Execution of policies and actions defined in Security and Availability Management
- The objectives of the access management process are to:
  - Manage access to services based on policies and actions defined in information security management
  - Efficiently respond to requests for granting access to services, changing access rights or restricting access, ensuring that the rights being provided or changed are properly granted
  - Oversee access to services and ensure rights being provided are not improperly used.

**Slide 48**

**Access Management – Purpose**

**PURPOSE**: To *grant* authorized users the right to use a service while *preventing* access to non-authorized users in order to protect the confidentiality, integrity and availability (CIA) of information and infrastructure.

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

Scope of Access management is effectively the execution of the policies in information security management, in that it enables the organization to manage the confidentiality, availability and integrity of the organization'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 is a process that is executed

by all technical and application management functions and is usually not a separate function.


**Access Management – Basic Concepts**

**Access**

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

**Identity**

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

**Rights (or Privileges)**

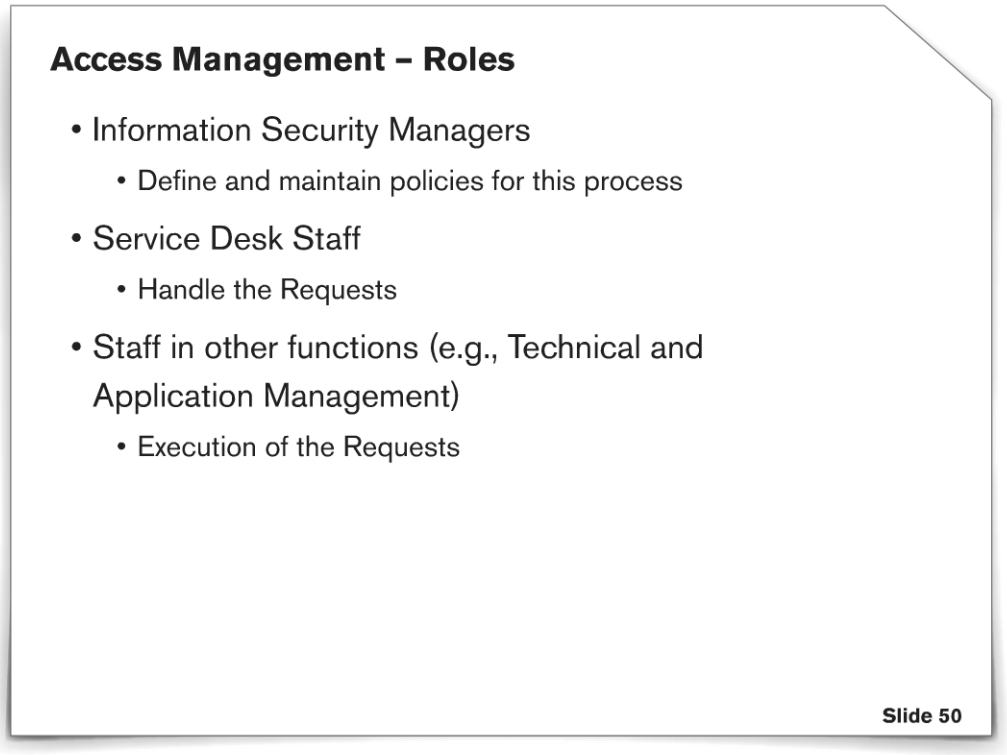
Rights are the actual settings whereby a user is provided access to a service or group of services. Typical rights, or levels of access, include read, write, execute, change and delete.

**Services or Service Groups**

The ability to grant each user (or group of users) access to the whole set of services that they are entitled to use at the same time.

**Directory Services**

Directory Services is a specific type of tool that is used to manage access and rights.




**Access Management – Roles**

Since Access Management is an execution of Security and Availability Management, these two areas will be responsible for defining the appropriate roles.

It is unusual for an organization to appoint an Access Manager, although it is important that there is a single Access Management process and a single set of policies related to managing rights and access. This process and the related policies are likely to be defined and maintained by **Information Security Management**, and executed by the various Service Operation functions. Their activities may be summarized as follows:

**The Role of the Service Desk**

The Service Desk is typically used as a means to request access to a service. Usually, this is handled through a Service Request. The Service Desk will validate the request by checking that the request has been approved at the appropriate level of authority, that the user is a legitimate employee, contractor or customer and that they qualify for access.

Once they have performed these checks (usually by accessing the relevant databases and Service Level Management documents), they will pass the request to the appropriate team to provide access. It is quite common for the Service Desk to be delegated responsibility for providing access for simple services during the call. The Service Desk is responsible for communication with the user when access has been granted, and to ensure that the user receives any other required support.

The Service Desk is also well positioned to detect and report Incidents related to access. For example, users attempting to access services without authority, or users reporting Incidents that a system or service has been used inappropriately (e.g., by a former employee using an old username to gain access and make unauthorized changes, or by users sharing login credentials, etc.).

**The Role of Technical and Application Management**

Technical and Application Management play several important roles, as follows:

- During Service Design, they will ensure that mechanisms are created to simplify and control Access Management on each service that is designed. They will also specify ways in which abuse of rights may be detected and stopped.
- During Service Transition, they will test the service to ensure that access may be granted, controlled and prevented as designed.
- During Service Operation, these teams will typically perform Access Management for the systems under their control. It is unusual for teams to have a dedicated person to manage Access Management, but each manager or team leader will ensure that the appropriate procedures are defined and executed according to the process and policy requirements.
- Technical and Application Management will also be involved in dealing with Incidents and Problems related to Access Management.
- If Access Management activities are delegated to the Service Desk or IT Operations Management, Technical and Application Management must ensure that the staff members are adequately trained and that they have access to the appropriate tools to enable them to perform these tasks.

**The Role of IT Operations Management**

Where IT operations is separated from Technical or Application Management, it is common for operational Access Management tasks to be delegated to IT Operations Management. Operators for each area will be tasked with providing or revoking access to key systems or resources. The circumstances under which they may do so, and the instructions for how to do so, must be included in the standard operating procedures for those teams.

The Operations Bridge, if it exists, may be used to monitor events related to Access Management and may even provide first-line support and coordination in the resolution of those events where appropriate.

## Service Operation – Summary

- Terminology
  - Event, Alert, Incident, Service Request, Problem, Work-around, Known Error, Known Error Database
- Processes
  - Event Management
  - Incident Management
  - Request Fulfilment
  - Access Management
  - Problem Management
- Functions
  - Service Desk
  - Technical Management
  - Application Management
  - IT Operations Management

**Slide 51**