1.1 CHAPTER SUMMARY

ITIL Service Operation provides best-practice guidance for the service operation stage of the ITIL service lifecycle. Although this publication can be read in isolation, it is recommended that it is used in conjunction with the other core ITIL publications.

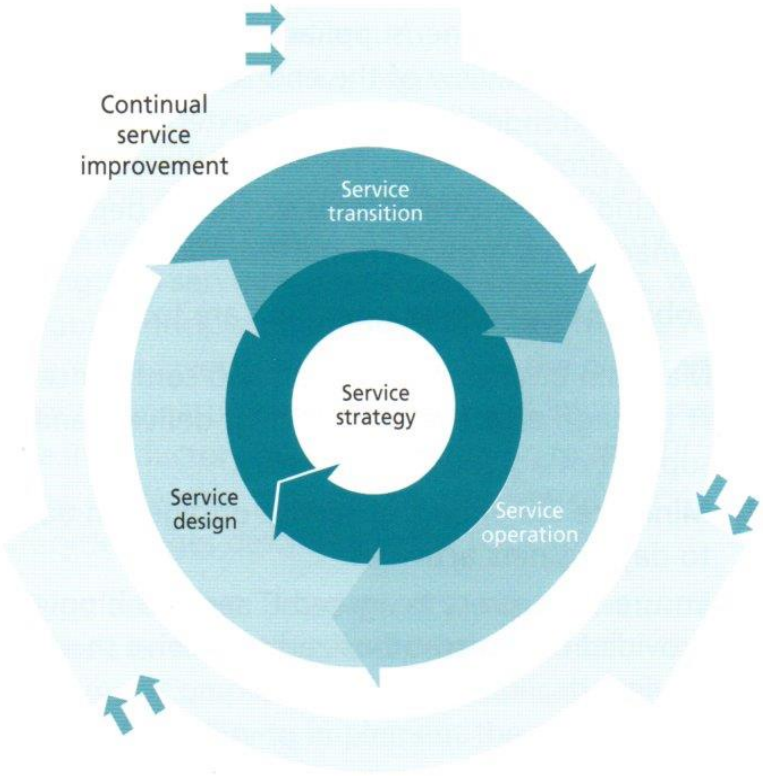

Figure 1.1 The ITIL service lifecycle

1.1.1 Purpose and objectives of service operation

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.

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.

4 Service operation processes

This chapter sets out the processes and activities on which effective service operation depends. These comprise both lifecycle processes and those almost wholly contained within service operation. Each is described in detail, setting out the key elements of that process or activity.

The topics specifically addressed in this chapter are:

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

Some of these processes are used throughout the service lifecycle, but are addressed in this publication because they are central to effective service operation.

The processes and activities described in this chapter are mostly contained within the service operation stage of the lifecycle, but also support other stages, e.g. validating attainment of the service levels set by the service level management (SLM) process within service design.

The purpose and scope of service operation as a whole are set out in section 1.1.

As a reference, an overview of each process is briefly described here and then in more detail later in the chapter. Please note that the roles for each process and the tools used for each process are described in Chapters 6 and 7, respectively.

Event management is the process that monitors all events that occur through the IT infrastructure to allow for normal operation and also to detect and escalate exception conditions.

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

Problem management involves root cause analysis to determine and resolve the underlying causes of events and incidents. Reactive activities seek to understand the underlying causes of incidents, create known error records that document root causes and workarounds, and undertake actions to remove those errors from the IT infrastructure. Known error records are used to document root causes and workarounds and allow quicker diagnosis and resolution if further incidents do occur. Proactive activities undertake efforts to detect and prevent future problems/incidents such that they won't occur in the first place.

Note that without a distinction between incidents and problems, and keeping separate incident and problem records, there is a risk that:

- Incident resolution activities may extend the duration of service outages 'looking for root cause' versus taking direct actions to restore normal state service operation.
- Incident records will be closed too early in the overall support cycle and there will be no actions taken to prevent recurrence – so the same incidents will continue to disrupt the business and have to be fixed over and over again.
- Incident records will be kept open so that root cause analysis can be done and visibility will be lost of when the user's service was actually restored – so SLA targets may not be met even though the service has been restored within users' expectations. This often results in a large number of open incidents, many of which will never be closed unless a periodic 'purge' is undertaken. This can be very demotivating and can prevent effective visibility of current issues.

Separating the two processes and managing through separate incident and problem records allows support staff to meet the rapid restoration objective for incident management while allowing root cause to be investigated and resolved in a separate, parallel problem management process.

Request fulfilment is the process of managing the lifecycle of customer or user service requests from initial request to fulfilment using separate request fulfilment records/tables to record and track their status. Service requests handle all other interactions with users or customers that are not service disruptions. Examples of service requests might include the solicitation of assistance with the

acquisition of a service, guidance on how to use a service, request for a password change, adding a user, or moving a user workstation (see section 3.1.3.4 for a more complete description of a service request).

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 (see *ITIL Service Design*) with respect to roles, rights and segregation of duties.

4.1 EVENT MANAGEMENT

An event can be defined as 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.

Effective service operation is dependent on knowing the status of the infrastructure and detecting any deviation from normal or expected operation. This is provided by good monitoring and control systems, which are based on two types of tools:

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

4.1.1 Purpose and objectives

4.1.1.1 Purpose

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.

4.1.1.2 Objectives

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. (This is covered in detail in *ITIL Continual Service Improvement.*)

4.2 INCIDENT MANAGEMENT

In ITIL terminology, an 'incident' is defined as an unplanned interruption to an IT service or reduction in the quality of an IT service or a failure of a CI that has not yet impacted an IT service (for example failure of one disk from a mirror set).

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.

4.2.1 Purpose and objectives

4.2.1.1 Purpose

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.

4.2.1.2 Objectives

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.

4.3 REQUEST FULFILMENT

The term 'service request' is used as a generic description for many different types of demands that are placed upon the IT organization by the users. Many of these are typically requests for small changes that are low risk, frequently performed, low cost etc. (e.g. a request to change a password, a request to install an additional software application onto a particular workstation, a request to relocate some items of desktop equipment) or may be just a request for information.

Their scale and frequent, low-risk nature means that they are better handled by a separate process, rather than being allowed to congest and obstruct the normal incident and change management processes. Effective request fulfilment has a very important role in maintaining end user satisfaction with the services they are receiving and can directly impact how well IT is perceived throughout the business.

Section 3.1.3.4 provides more details around service requests and their relationship to IT services, request models, and changes.

4.3.1 Purpose and objectives

4.3.1.1 Purpose

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

4.3.1.2 Objectives

The objectives of the request fulfilment process are to:

- Maintain user and customer satisfaction through efficient and professional handling of all service requests
- Provide a channel for users to request and receive standard services for which a predefined authorization and qualification process exists
- Provide information to users and customers about the availability of services and the procedure for obtaining them
- Source and deliver the components of requested standard services (e.g. licences and software media)
- Assist with general information, complaints or comments.

4.4 PROBLEM MANAGEMENT

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.

4.4.1 Purpose and objectives

4.4.1.1 Purpose

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.

4.4.1.2 Objectives

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.

4.5 ACCESS MANAGEMENT

Access management is the process of granting authorized users the right to use a service, while preventing access to non-authorized users. It has also been referred to as rights management or identity management in different organizations.

4.5.1 Purpose and objectives

4.5.1.1 Purpose

The purpose of access management is to provide the right for users to be able to use a service or group of services. It is therefore the execution of policies and actions defined in information security management.

4.5.1.2 Objectives

The objectives of the access management process are to:

- Manage access to services based on policies and actions defined in information security management (see *ITIL Service Design*)
- 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.

6.2.1.1 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 request for change (RFC). 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.

6.2.1.2 Technical management

Technical management provides detailed technical skills and the 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 (see section 6.10.1). In many organizations, the technical management departments are also responsible for the daily operation of a subset of the IT infrastructure. Figure 6.1 shows that, although they are part of a technical management department, staff who perform these activities are logically part of the IT operations management function.

6.2.1.3 IT operations management

IT operations management is the function responsible for 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. This is illustrated in Figure 6.1 by the overlap between the technical and application management functions. IT operations management has two sub-functions that are unique and are generally organizationally distinct. These are:

- **IT operations control** This is generally staffed by shifts of operators 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** This 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. In some organizations many physical components of the IT infrastructure have been outsourced and facilities management may include the management of the outsourcing contracts.

6.2.1.4 Application management

Application management is 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. Application management is usually divided into departments based on the application portfolio of the organization (see the examples in Figure 6.1), thus allowing easier specialization and more focused support. In many organizations application management departments have staff who perform daily operations for those applications. As with technical management, these staff logically form part of the IT operations management function.

Special note on information security management

Although most would agree that information security management is a function, it is highly specialized and spans several stages of the lifecycle. It is also responsible for the oversight of many activities within all service operation functions. For a more in-depth description of information security management, please refer to *ITIL Service Design*.

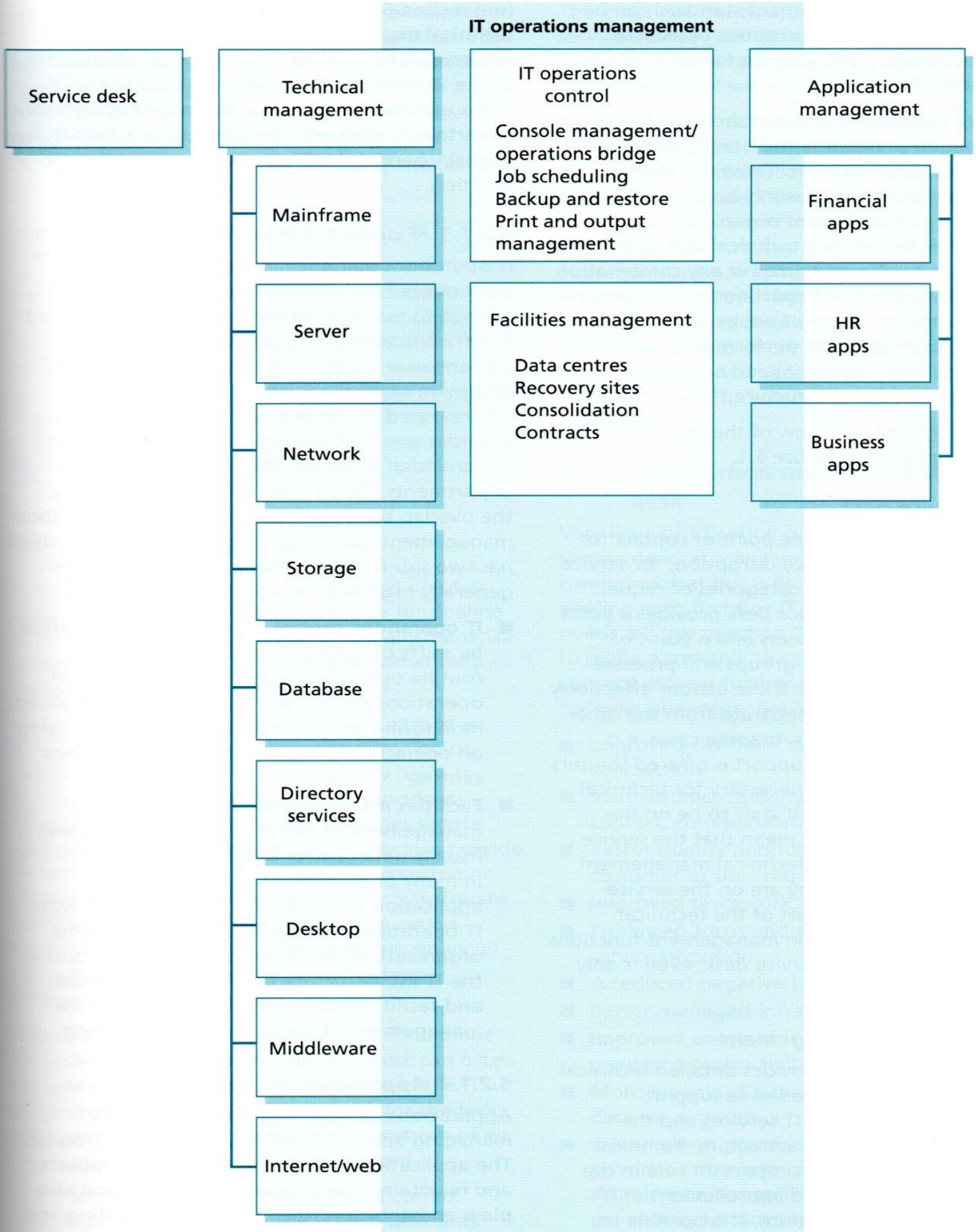

Figure 6.1 Service operation functions