Service Operation

ITIL Lifecycle Certification

Acknowledgements

DOCUMENT INFORMATION

Type - ITIL Certification Course

Program - Service Operation - ITIL Lifecycle Course

Contents

Contents

Contents

Contents

Contents

Chapter 1:

Course Introduction

Objectives

Knowledge & understanding of:

- ITIL Qualification scheme
- Course structure
- Bloom's Taxonomy
- Course materials

Terms-to-Know

Accredited Training Organization (ATO) – An organization that is accredited to provide training in ITIL by a licensed Examination Institute (EI).

Accreditor (APMG) – Organization empowered by the Cabinet Office, the "owner" of ITIL, to establish the ITIL qualification scheme, devise ITIL syllabi and examinations, and oversee Examination Institutes (EI). The current ITIL Accreditor is the APM Group.

Bloom's Taxonomy – A method of classifying learning objectives that provides the basis for formulating different levels of questions for the ITIL Foundation, Intermediate and Advanced examinations.

Exam – The official ITIL exam. ITIL examinations are closed-book and require an independent proctor to monitor the exam security. Many examinations require that the candidate attend an accredited course.

Examination Institute (EI) – An organization licensed by the ITIL Accreditor. EIs operate an ITIL examination scheme through a network of Accredited Training Organizations (ATO), accredited materials.

ITIL Books – The five core books of the IT Infrastructure Library (ITIL): Service Strategy, Service Design, Service Transition, Service Operation and Continual Service Improvement.

ITIL Qualification Scheme – A modular, tiered approach to ITIL certification that comprises a series of certifications focused on different disciplines or areas of ITIL best practice to various degrees of depth and detail.

Practice Paper – An official ITIL exam that is available for practice by the student. Two practice exams are available for most ITIL courses.

Student Manual – A document produced by the ATO and which contains copies of the slides, amplifying information and other course material.

Quiz – Short quizzes within the course to help students track their progress toward understanding the learning objectives of the course.

Chapter 2:

Service Operation Introduction

Objectives

Bloom's Level 2 Objectives - Full understanding of Service Operation terms and core concepts, the functions contained within Service Operations including how they interact to make Service Operation work.

- The Processes and service lifecycle has that Service Operation interfaces with
- The fundamental aspects of Service Operation and be able to define them

Bloom's Level 4 Objectives - Support problem solving by putting theory into practice, interpret principles and relationships.

- How Service Operations organized in relation to Functions, Groups, Teams, Department and divisions.
- How an organization can achieve balance when dealing with internal verse external organizational focus, identifying the issues related to organizations who operate at the extremes of these balances.
- What "Operational Health" means, specifically addressing examples of "self healing systems" and the processes used by them
- The creation , components and implement of a complete communication strategy to be used with Service Operations.

Terms-to-Know

Function – A team or group of people and the tools they use to carry out one or more processes or activities.

Process –A structured set of activities designed to accomplish a specific objective.

Role – A set of responsibilities, activities and authorities granted to a person or team.

Service – A means of delivering a value to customers by facilitating outcomes customers want to achieve without the ownership of specific costs and risks.

Lesson 3

Introduction to Service Operation

Service Operation & the Service Lifecycle

Service Operation coordinates the processes and activities for delivering and managing services at their agreed levels. It is where most of the business community comes in contact with IT because Service Operation "makes IT services happen" in the eyes of the customer.
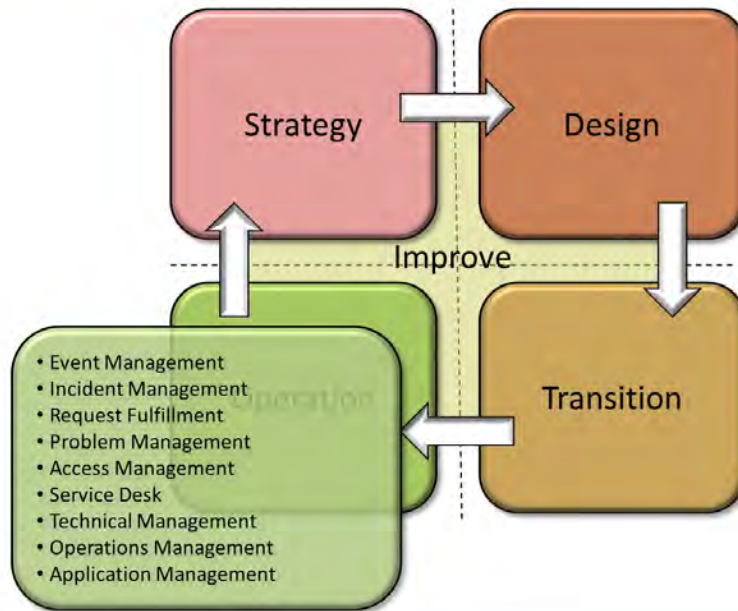
Managing Across the Lifecycle

Service Operation determines how to deliver and support an IT service. It provides inputs to the Continual Service Improvement (CSI) domain on how to improve services, as well as support and delivery processes. It also takes over the support of new or changed services as they transition into operation.

Purpose, Goals & Objectives of Service Operation

The delivery and support of an IT service requires a tremendous amount of coordination of resources (people, technology, processes and functions). This effort provides the IT service at the agreed level of service within the defined resource constraints.

On a day-by-day basis, Service Operation manages the technology under its purview and continually monitors its services and technology to ensure that it is meeting the agreed objectives. Service Operation also continually seeks ways to improve its performance, business confidence and customer satisfaction.

Scope of Service Operation

- **Provided services**
  - Internal & external
- **Service management processes**
  - Service Operation & other lifecycle processes
- **Technology**
  - Managing technology that manages technology
- **People**
  - Consumers of services
  - Providers of services

Scope of Service Operation

Service Operation's scope extends over all of the services provided by IT in support of business processes. This includes services provided by internal staff, as well as those provided by external service providers. Its scope also includes various touch points within the other Service Lifecycle domains such as Continual Service Improvement, Service Transition, Service Design, and Service Strategy.

The functions and processes of Service Operation involve highly complex tasks associated with managing its technology. This requires that all of the technology that supports or manages the IT infrastructure thoroughly integrate into the support processes to enable efficient and effective delivery of IT services.

Similarly, supporting today's complex technological infrastructures demands that IT become a service provider within a multi-provider environment. Many of today's services consist of both internally and externally provided services. However, from the customer's viewpoint, it all "belongs" to the internal IT organization.

Value of Service Operation

- **Service Operation**
  - Upside – "visible" value to the customer
  - Downside – funding, funding, funding & funding
- **All lifecycle processes come together**
  - Service Strategy – models service value
  - Service Design – designs, predicts & validates Cost of Service
  - Service Transition – realizes value
  - Service Improvement – optimizes service & process

Value and the ITSM Lifecycle
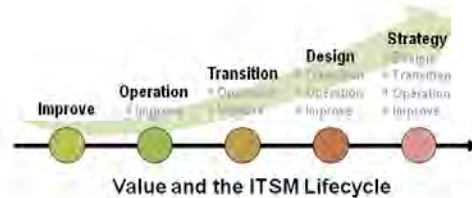
Value of Service Operation

Service Operation brings together the outcomes of all of the phases of the IT Service Lifecycle. Service Strategy models the IT service, Service Design validates it, Service Transition builds it and moves it into operation, and Continual Service Improvement optimizes it.

Up to this point in the IT Service Lifecycle, all of these efforts are transparent to the vast majority of the business customers and user community. However, Service Operation is "where the rubber hits the road." It is the face or visible part of IT that the average business person comes into contact with most often

If there is an upside to Service Operation, it is that the business customers form much of their perception of IT and the services it provides through their interactions with the functions and processes of Service Operation.

If there is a downside to Service Operation, it is that the activities become part of the landscape. It becomes difficult to justify necessary resources to support aging deficient services, support staff and tools, or make an IT service better.

Lesson 4

Principles of Service Operation

Fundamentals of Service Operation

- Provide value through Service Operation
- Optimize Service Operation performance
  - Ongoing improvements
  - Incremental improvements (long term)
- Processes
  - Event Management – manage event lifecycle
  - Incident Management – restore services
  - Problem Management – root cause analysis
  - Request Fulfillment – manage fulfillment lifecycle
  - Access Management – grant authorized users access to services
- Functions
  - Service Desk – single point of contact
  - Technical Management – technical skills
  - Application Management – manage application lifecycle
  - IT Operations Management – executes daily operational activities

Fundamentals of Service Operation

The Service Operation stage of the IT Service Management Lifecycle is where the business first sees the value of the new or changed service realized. Its where "the rubber hits the road." The Service Operation process and activities seek to optimize IT Service performance in two ways; 1) ongoing improvement (short term "tweaks" to improve things) and 2) incremental improvements that have a longer term horizon for the improvement to be realized.

The processes of this stage of the lifecycle include:

- Event Management which manages the entire lifecycle of an event
- Incident Management whose purpose is to quickly restore a failed service
- Problem Management seeks to find and remove errors from the infrastructure
- Request Fulfillment manages on incident related requests for pre-approved services
- Access Management grants rights to users to access agreed services

Service Operation also covers the organizational structures necessary to support live IT Services. Its functions include:

- Service Desk which act as the single point-of-contact for users seeking assistance
- Technical Management manages the technical staff and their associated skills and tools
- Application Management manages the application lifecycle
- IT Operations Management executes the daily operational activities (inclusive of IT Operations Control and Facilities Management)

Balancing External & Internal Views

ITIL defines a service as "a means of delivering value to customers by facilitating outcomes customers want to achieve without the ownership of specific costs and risks." This affords us some insight into the difficulty Service Operation faces in balancing its "internal view" of a service with the customer's "external view" of the same service.

The external view of a service is from the perspective of the business customers and users who "consume" the service; it is their experience with the service. They neither know, nor care, what elegant combinations of hardware, software and engineering genius go into its delivery (nor should they). They experience only the utility and warranty of the service.

On the other hand, IT's internal view of the service is of all of those elegant pieces of hardware and wonderfully written software programs supported by really great tools that make it all work together. Moreover, because most of that elegant technology belongs to vertically integrated functional groups, it is often difficult for one group to see (or care) what other elegant pieces of hardware or software come from other groups.

Although the two views above represent the opposite ends of the spectrum, the challenge is to make sure the IT organization can meet the demands of the business. Too much of a focus on the external view places IT in the position of over promising and under delivering, while too much focus on the internal places the IT in the position of not meeting the needs of the business.

Balancing Stability & Responsiveness

Striking the balance between being responsive to the business while maintaining a stable IT infrastructure and high service availability is a challenging goal to achieve. The business wants to implement changes right away, while IT appreciates the contribution a "steady state" makes to its quality of service (QoS) objectives.

This ongoing demand for changes to technology-enabled business processes can result in a patchwork of infrastructure that places a disproportionate demand on IT resources.

If left unchecked, this environment creates a situation in which many IT organizations act more as "gatekeepers" than service providers. IT finds itself relegated to maintaining the status quo (stable infrastructure) at the cost of responding to the business' need for change. The short-term objectives often seem to outweigh the long-term strategies.

With an extreme focus on IT stability places IT in danger of ignoring changing business requirements while an extreme focus on responsiveness creates the danger of over-spending on changes that might not have been properly vetted.

Balancing Quality & Cost of Service

Life is full of compromises, and balancing the quality of something with its cost creates difficulty for many IT service providers and businesses.

We have all heard the saying, "You can have it good, fast or cheap. Pick any two." The difficulty comes in balancing Quality of Service (QoS) with the Cost of Service (CoS) while viewing "good," "fast" and "cheap" as absolutes.

Goodness and quality are, in effect, the same; the ability of a product, service or process to provide the intended value. How quickly IT can deliver a product, service or process is a direct function of resources, which impact time-to-deliver and cost. Increase one and something, somewhere, must change to accommodate it.

Balancing QoS and CoS focuses on bringing quality in line with the value of the service, NOT its cost! Many businesses tend to confuse cost and value and end up seeing service quality fall off after across-the-board cost-cutting. One basic truth in IT Service Management is "cheap" NEVER ends up being least expensive. A focus on cutting costs risks reduction in a business level of expected quality while a focus on quality typically leads to overspending to deliver higher services levels than needed.

> Often Service Provider organizations base their decisions primarily on cost. When this happens at the expense of other considerations such as time or quality, hidden costs end up exceeding any apparent savings in cost. Therefore, the cheapest approach to doing something is not always the least expensive.

Balancing Reactive & Proactive

- Reactive organization – waits for stuff to happen
  - Firefighting is a way of life
  - Heroes are revered
- Proactive organization – constantly looking for improvement
  - Fire prevention is a way of life
  - Heroes are acknowledged
  - Investigate what went wrong

Balancing Reactive & Proactive

Any IT professional who has been around for any length of time has probably accumulated a whole drawer full of "hero badges." These are the accolades or kudos bestowed upon our IT service provider's heroes for rushing in and saving the day through their extraordinary efforts.

In a "reactive organization," where fire fighting is the normal way of life, the heroes are revered, get big raises and coveted promotions. But organizations that are constantly fire fighting tend to consume their valuable technical functional resources "fixing stuff" instead of "doing stuff" that would help the business be more successful.

A "proactive organization," on the other hand, is always looking for ways to improve things. Here fire prevention is a way of life. Although heroes are recognized for their contribution to the organization, a proactive organization always investigates the situation that led to the need for a hero and sees if there are ways to avoid the use of heroism again. Reactive organizations aren't able to effectively support the business strategy, while a primary proactive focus means that services that aren't broken will get "fixed," resulting in higher costs to the customer.

Making the move to a proactive organization depends on a number of different things:

- The overall maturity of the IT organization
- The organizational culture
- IT's role within the business
- Level of process and tool integration
- Maturity and scope of Knowledge Management

Providing Service

The concept of a service culture undoubtedly manifests itself most clearly within the Service Operation portion of the Service Lifecycle. All of the other domains lay the foundation, but it is here that the service culture concepts actually go to work.

In short, a service culture recognizes that its major objective is customer satisfaction as it helps customers to achieve their business objectives. Looking inward, this means that IT values its technical and performance achievements as mileposts in the journey to customer satisfaction.

IT achieves a service culture by making each staff member aware of the larger picture of business goals and objectives, and the value of his or her participation in it. IT must look upon service as a profession and adjust its performance metrics and recruitment requirements accordingly.

SO & Other Lifecycle Stages

Service Operation and its processes have a significant level of interaction with other stages of the IT Service Management Lifecycle.

Service Strategy - Service Operation provides data about current cost of operations at a given level of capability. This helps in the identify the impact of the chosen strategies and points out areas of operational risk.

Service Design - Service Operation interacts with the design stage to help it define service objectives and performance criteria. It seeks to link the specification for the service to its performance, thus defining its operational performance requirements. It helps map services to their supporting technology.

Service Transition - Service Operation staff is trained on new or changed services during the transition stage. It performs review of acceptance tests and is a major participant in planning the transition. It also participates in various transition tasks, including the provision of early life support for a new or changed service.

Continual Service Improvement - Service Operation is a key source of operational data on live services. Its daily involvement with the delivery of services positions it as major contributor when assess the impact of a proposed improvement. It provides for the daily execution of the operational tasks required to support service (and process) monitoring. In its role of providing direct support for IT Services it is in a unique position to identify improvement opportunities.

Operational Health

- Check for normal operation
- Determine the "vital signs"
  - Support of vital business functions
  - Operating envelope (normal ranges)
- Define healthy & unhealthy
- Determine in Service Design
- Test & refine in Service Transition
- Optimize in CSI

Operational Health

Achieving operational health is very similar to achieving personal health. A normal, healthy person concerns him- or herself with maintaining a healthy lifestyle and occasional monitoring what the health profession terms Vital Signs.

Although current technology has the capability to monitor almost every sign of health, it is costly in terms of devices and resources, and can adversely impact performance. Thus, selecting a set of vital functions to monitor avoids the expense of constantly monitoring too deeply.

As with human health, though, operational health should check its systems more thoroughly from time to time. This could mean more intensive monitoring of a disk that is functioning perfectly, but is nearing the end of its Mean Time Between Failures (MTBF) threshold.

Good Availability Design and Problem Management processes help to build a reliable and maintainable infrastructure, which, in turn, prevents incidents and problems.

Finally, IT can further sustain operational health by investing in 'self-healing' systems that apply Availability, Capacity, Knowledge, Incident and Problem Management concepts to design systems that can withstand threats to operating conditions and automatically detect, diagnose and recover from Incidents and Known Errors. This may be as complex as multiple, redundant processors, or as simple as developing a set of diagnostic scripts.

Communication's Role in Service Operation

- Communication must have
  - Intended purpose or result in specific action
  - Intended audience
- Communication checklist
  - Who needs to know about it?
  - What is to be communicated?
  - Where does the communication occur?
  - When do they need to know?
  - Why does it need to be communicated?
  - How does the communication take place?

The 5 "Ws" and 1 "H" of Communications

Communication's Role in Service Operation

In its daily activities, Service Operation communicates frequently with both internal and external recipients about topics such as inter-shift operations handover, performance and project reporting, changes, exceptions, emergencies, training on new processes and service designs, and strategy and design information for internal Service Operation teams.

The most important thing to remember about communication is that it derives from the word "to commune" or "to share." In other words, communication must always be a two-way process. It must always have an intended audience, and it must always communicate the message to the audience in the language and method the audience expects.

The most effective communication relies on a checklist similar to the journalist's credo of Who? What? Where? When? Why? and How? A successful communications document or campaign answers each of these questions and specifically targets its intended audience.

> **The 5 "Ws" and 1 "H" of Communications**– **Who**? Who is the communication intended for? Who initiated the communication? **What**? What is the topic of the communication? **Where**? Where does the communication apply? What is its scope? **When**? When does the subject topic of the communication take place? In the future? Has it already happened? **Why**? Why is it necessary to release the communication? Does the recipient need to do or know something? **How**? How will the subject topic of the communication happen? Does the communication need to include instructions for doing something?

Service Operation Documentation

- Process
  - Definition
    - All lifecycle phases
  - Maintenance
- Technical procedures
  - Defined within higher processes
  - Maintained under change control

Service Operation Documentation

Documentation is one of the keys to ensuring the consistent execution of operations procedures and activities. Service Operation documentation breaks down into four areas.

Standard Operation Procedures, known as SOPs, represent the detailed instructions the operations staff follows in the day-to-day execution of the procedures and activities of managing the IT infrastructure. The scope of SOPs extends over all of the devices and systems under management, and includes defined standards of performance. Operational Level Agreements (OLAs) often reference these performance standards.

Operations logs record what was done, by whom, when and what the outcomes were. The logs provide the "paper trail" for the execution of operations procedures. They can be in hardcopy written form or electronic, and must be covered by a policy that includes guidance on the retention of the logs.

Shift schedules and reports document the schedule of activities that the Operations staff carry out in each shift. It coordinates activities across multiple shifts and ensures consistency in their execution. Tools used to support operations scheduling can be as simple as a handwritten sheet of paper or as sophisticated as an enterprise scheduling product.

Operations schedules provide a high-level overview of planned operations. They not only include normal operations activities, but also outline changes to routine jobs, anything added on a one-off basis, and scheduled maintenance by Technical Management staff or external service providers.

Lesson 5

Service Operation Summary

Service Operation Summary

Purpose – To deliver, support & manage services.
Goals – Agreed service levels met.
Objectives – Coordinate processes and common activities.

Principles
- Balancing
  - Internal vs. External view
  - Stability vs. Responsive
  - Quality vs. Cost
  - Reactive vs. Proactive
- A "culture of service"
- Integral part of the lifecycle

Scope
- Internal & external
- Service Operation & other lifecycle processes
- Technology
- Technology that manages technology
- Consumers of services
- Providers of services

Processes
- Event Management
- Incident Management
- Request Fulfillment
- Problem Management
- Access Management
- Functions – Service Desk, Technical Management, Operations Management, Application Management

Value
Service Operation brings all lifecycle processes together; Service Strategy – service value modeled; Service Design – Cost of Service (CoS) designed, predicted & validated; Service Transition – realized value; and Service Improvement – service & process optimization. Service Operation provides "visible" value to the customer, at the cost of ongoing funding requirements.

Service Operation Summary

The Service Operation Phase of the IT Service Management Lifecycle is all about the capability to balance competing interests in the delivery of IT Services. Part of the balancing acts requires that IT organizations create and maintain effective communication channels with all of the stakeholders. Through effective communication, they can anticipate and respond more effectively to the needs of the customer.

The processes, activities and functions are not passive in the delivery of IT Services. Service Operation constantly monitors the operational health of the services it delivers. This is critical to their ability to keep IT Services in operation and enable the business to achieve its desired business outcomes.

Checkpoint
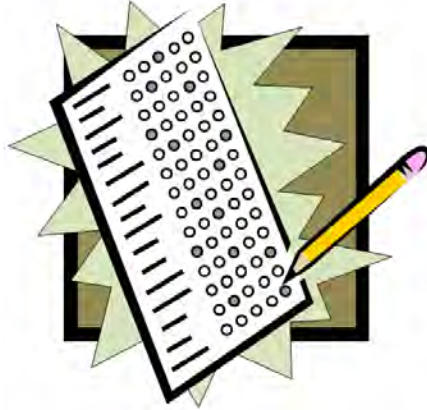
Checkpoint Instructions

Refer to the Checkpoint booklet for relevant quizzes and exercises.

Chapter 3:

Service Operation Processes

Objectives

Bloom's Level 4 Objectives – Support problem solving by putting theory into practice, interpret principles and relationships.

- The use of and interaction of each of the five key processes that make up Service Operation
- The value to the business that each of the Service Operation processes contributes
- The use of and interaction of all other lifecycle operational activities that contribute to Service Operation

Terms-to-Know

Call Type – A category that is used to distinguish incoming request to a Service Desk. Common Call Types are Incident, Service Request and Complaint.

Classification – The act of assigning a category to something. Classification ensures a consistent management and reporting.

Closure – The act of changing the status of an incident, problem, change, etc. to Closed.

Detection – A stage in the Incident Lifecycle. Detection results in the incident becoming know to the user or Service Provider..

Diagnosis – A stage in the incident and problem lifecycles The purpose of diagnosis is to identify a workaround for an incident or the root cause of a problem.

Escalation – An activity that obtains additional resources when these are needed to meet Service Level Targets or customer expectations. There are two types of Escalation; Functional and Hierarchical.

Event – A change of state that has significance to the management of a Configuration Item or IT Service.

Failure – Loss of ability to operate to specifications, or deliver the required output.

Incident – An unplanned interruption of an IT Service or reduction in the quality of an IT Service, or the failure of a Configuration Item that has not yet affected an IT Service..

Known Error – A problem that has a documented root cause and a workaround.

Monitoring – Repeated observation of a Configuration Item, IT Service or Process to detect events and to ensure that the current status is known.

Problem – A cause of one or more incidents.

Recovery – Returning a Configuration Item or an IT Service to a working state..

Restore – Taking action to return an IT Service to the users after repair and recovery from an incident.

The Service Operation Model
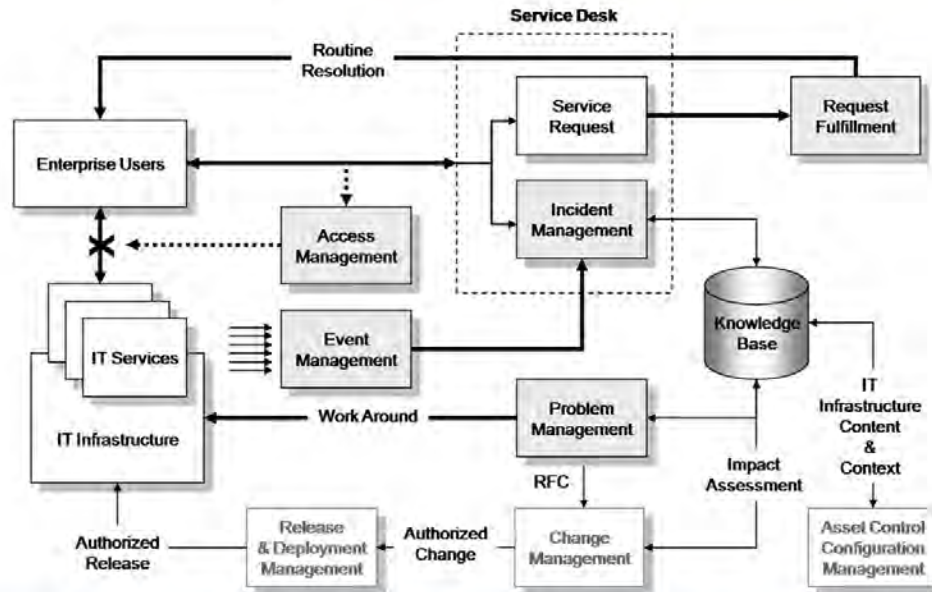
The Service Operation Model

This is a high-level diagram of how the functions and processes of Service Operation relate to each other, other Service Lifecycle processes and the business users.

The Processes of Service Operation

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

The Processes of Service Operation

The following sections will examine the five Service Operation processes.

- Incident Management - Coordinating IT resources to restore an IT service.
- Event Management - Monitoring events throughout the IT infrastructure.
- Request Fulfillment - Managing customer & user requests that are not the result of an incident.
- Problem Management - Finding the root cause of events & incidents.
- Access Management - Granting authorized users the right to use a service.

Lesson 6

Event Management

Introduction

- **Event Management**
- Incident Management
- Request Fulfillment
- Problem Management
- Access Management
- Service Desk
- Technical Management
- Operations Management
- Application Management

Strategy → Design

Improve

Transition

Introduction

Within the Service Lifecycle, Service Operation holds witness to the full realization of the strategic objectives; this is where it all comes together and this is where the customers see the service and the organization supporting it.

Event Management orchestrates the monitoring of, and the response to events throughout the IT infrastructure. This supports normal on-going operations and enables the detection and escalation of exception events.

Purpose, Goals & Objectives

- **Purpose**
  - Manage the event lifecycle
- **Goals**
  - Provide event
    - Detection, analysis & determine control actions
- **Objectives**
  - Basis for comparison of IT Service behavior
    - Against standards
    - Against design criteria
    - Against agreements
  - Basis automating routine operational activities
  - Provide input to Continual Service Improvement

Objective

A myriad of events occur each minute and hour within a typical IT infrastructure. Event Management provides the overarching process that manages the detection, analysis and the determination of the appropriate control actions for these events.

Through the management of infrastructure events, Event Management measures the actual behavior of individual IT services against performance standards and the IT Service design criteria, as well as Service Level Agreements (SLA) and their associated Operating Level Agreements (OLA) and Under-pinning Contracts (UC).

It also serves as the basis for automating routine operational activities and provides important input for the continual improvement of IT Services and the processes of the IT Service Lifecycle.

Scope

- Configuration Items events associated with
  - CI state changes
  - CI status changes
- Operational environmental events
  - Fire detection, suppression, etc.
- Software licensing
- Security
  - Intrusion detection
- Normal operation
  - Availability
  - Performance

Scope

Event Management has a rather broad scope within IT Service Management.

At the heart of Event Management is dealing with events that signify a change of either the state or status of a Configuration Item (CI). This can include CIs involved with the IT operational environment, such as electrical distribution, fire suppression, heating, ventilation and air conditioning; in other words anything that participates in or supports the delivery of an IT Service.

Event Management also extends into the management of enterprise software licenses, including their utilization and allocation, and activities associated with the normal operation of the infrastructure as it relates to performance (availability and capacity).

Value to the Business

Event Management's value to the business is mostly indirect. This is due to the nature of the process and its role in triggering other IT Service Lifecycle processes. Thus, any value to the business ascribed to the Event Management process grows out of its ability to improve the efficiency and effectiveness of the triggered process.

In general terms, Event Management aids in the proactive intervention of degraded IT Services or outright IT Service outages. It also helps reduce personnel costs by freeing expensive technical staff from performing routine tasks.

Concepts

- Events generate & detect **meaningful** notifications about a CI or service
- Events can signify
  - Regular operation
  - An exception
- Events can be
  - Informational
  - Warnings
  - Exceptions

Concepts

The components within the IT infrastructure constantly generate events. These events provide information about Configuration Items (CI), warnings about abnormal operation, or exceptions to expected behavior. The key to Event Management is determining which events are meaningful, what criteria define an event as meaningful, and what control actions, if any, are necessary.

Activities of Event Management

Determining how to manage events is unique to each IT organization, and it depends on the size and complexity of their IT infrastructure, IT Services and supported business processes. The following discussion of the activities of the Event Management process provides solely a high-level reference.

- Occurrence & Notification - Event occurrence and formulation of the notification
- Detection & Filtering - Receipt of the event by some tool and the application of filtering criteria
- Significance & Correlation - Determination of event type and the significance of the event
- Response Trigger & Selection - Determination of an event trigger and selection of the appropriate response
- Review & Closure - Review of events handled and process closure

Event Occurrence & Notification

Events occur continuously throughout the IT infrastructure. However, only those deemed "meaningful" actually fall into the "managed" bucket. Their importance, determined during the IT Service's design, development and ongoing management and support, determines how to deal with them.

Notification formalizes and communicates information about the event. This can occur when a monitoring tool actively polls or interrogates a device or when the device recognizes some predefined criteria and generates the notification. Some sort of monitoring tool or tool set serves up the receipt and interpretation of event notifications.

The notification can be very terse (and often cryptic to humans) or verbose (containing amplifying information). Further interpretation ensures the notification goes to the appropriate group or initiates the correct automated response.

A general rule of thumb is that the more descriptive and complete the information about an event is, the better the decision-making process will be able to establish the appropriate response trigger and response selection. An event notification that reads "PRN1234: Error" is less likely to be dealt with as efficiently as one that includes amplifying information such as, "PRN1234: Warning - Low toner level."

Event Detection & Filtering

- Highly dependent on enabling tools
- Event detection – read & interpret meaning
- Logging
- 1st level event correlation & filtering
  - Filter wanted from unwanted events
- Categorize event type
  - Informational
  - Warning
  - Exception

Event Detection & Filtering

Event detection in the context of Event Management is the processing of the notification event by some agent or management tool specifically designed to interpret the meaning of specific events. Similar to the conundrum, "if a tree falls in the forest and there is no one there to hear it, does it make a sound?" the design of event notifications must keep the event detection mechanism in mind.

Once detected, events go through a filtering process, which reads them and disregards unwanted events (those the process deems as not being "meaningful"). In this context, there are three primary event types - informational, warning or exception.

Event Significance & Correlation

Each IT organization formulates its own criteria for filtering and correlating events. This largely depends on the size and complexity of the IT infrastructure as well as the IT Service and the supported business processes.

Typical event categories are:

Informational - Normally requires no action, and it does not represent an exception to normal operation. Normally informational events confirm the status of a device or service and often provide the basis for generating usage statistics or supporting forensic investigations.

Warning - A warning indicates that the event activity has approached a threshold level. The intent of a warning is to provide time to take the appropriate action to avoid degraded service or an outright service outage.

Exception - An exception indicates that a component or an IT Service is operating in an abnormal fashion by measuring it against criteria established within an SLA or supporting OLAs or UCs.

Correlation is the determination of the reciprocal relationship between two or more things. In this case, the correlation of events assesses the relationship between the event and its impact on the CI, IT Service or supported business process and aides in determining the appropriate control action.

The "correlation engine" is usually one of the features of monitoring and management tools. Correlation looks at standards established during the design of an IT Service, as well as derived through its normal operation.

Event Response Trigger & Selection

- Correlation determines if a response is required
- Event response selection
- Response is "triggered"
- Response selected based on specific criteria
- Selected response or combination of responses
  - Event logging
  - Auto response
  - Alert & human intervention
  - Incident, problem or change

Event Response Trigger & Selection

Once event correlation determines that an action is required, it initiates a response trigger. A trigger can be any act or event that serves as a stimulus and initiates or precipitates a reaction or series of reactions. An Event Management trigger precipitates the initiation of other processes, such as Incident, Problem or Change Management or work tasks, for execution by the Operations, Technical or Application Management functions.

Criteria specific to the CI, the IT Services it participates in, or the business process it supports, forms the selected response to an event. The event can trigger a single response or a combination of responses, ranging from logging the event, initiating an automated response, getting a human involved, or initiating a process' lifecycle.

Event Review & Closure

- Ensures significant events were handled
- Looks at trends & event types
- Ensures handoff to appropriate
  - Functions
  - Process
- Most events are not "opened"
- Events linked to control actions
  - Incidents, problem, etc.

Event Review & Closure

It is not necessary to review all events. The intent of the review activity is to ensure that IT infrastructure reviews significant events that trigger control actions for proper handling. In other words, if it was important enough to take action on, did it do so? This provides the necessary feedback to ensure that inter-process communication has occurred and that the response trigger and selected response was appropriate for that event.

The use of such terms as "open and close" in relation to events is a bit of a misnomer. Most events are not opened by anyone, yet infrastructure must be concerned with "closing the loop" on those events that required some sort of control action to be taken. This often means linking the selected response's output back to the event.

Triggers, Inputs & Outputs

The Event Management process is triggered when something "unusual" or "noteworthy" occurs in the infrastructure. In other words, some exception to "normal" occurs and something needs to happen as a result. An exception can come from many different sources.

The process inputs fall into two main categories; 1) things that support its capability and 2) things that it needs to deal with (exceptions).

The process outputs focus on record keeping and communication. Event Management is about taking an event and letting someone know about it. It really doesn't deal directly with the cause of the event.

Process Relationships

Strategy (SS)
Strategy Management
Service Portfolio Management
Financial Management
Demand Management
Business Relationship Management

Design (SD)
Design Coordination
Service Catalog Management
Service Level Management
Availability Management
Capacity Management
Continuity Management
Security Management
Supplier Management

Improvement (CSI)
7-Step Improvement Process

Operation (SO)
Event Management
Incident Management
Request Fulfillment
Problem Management
Access Management

Transition (ST)
Planning & Support
Change Management
Configuration Management
Release & Deployment
Evaluation
Knowledge Management
Validation & Testing

Process Relationships

Event Management shares relationships with several processes and functions among various IT Service Lifecycle domains.

Within Service Operation, an event may trigger some action by Service Desk staff, an Incident or a request for service, which in turn may result in Access Management handling the actual fulfillment via the Technical, Application or Operations functions. Events may also trigger the identification of a problem, or linking of an incident to a problem record.

Within Service Transition, an event may trigger a Request for Change (RFC), which will kick off the Change Management lifecycle. Informational events can be a source for Knowledge Management and further utilization in the management of CIs and IT Services.

Within Service Design, Event Management can integrate with Access Management to execute the Information Security and Availability Management policies. Event Management also participates in handling of availability-, capacity-, continuity- and security-related events.

Within Continual Service Improvement, Event Management provides information to track and evaluate service and process performance trends, and may provide clues as to how to improve them.

Critical Success Factors

The Critical Success Factors for the Event Management process fall into two major categories; 1) capability and 2) execution.

The CSFs that focus on capability seek to ensure that the Service Provider's organization has the capability to successfully manage events within the IT Infrastructure. These include measuring things that prove the process is setup and running. The other CSFs measure how well its doing its job of handling and communicating exceptions.

Challenges

The dependence on enabling technology presents a major challenge to the successful design, implementation and execution of the Event Management process. This particular challenge breaks down into three areas. First is the difficulty in defining enabling tool requirements; in other words, driving tool selection from a developed set of requirements as opposed to accepting the existing feature set of an incumbent tool set, or vendor's offering. Second deals with availability (or lack) of skilled personnel capable of fulfilling the required roles and responsibilities of the Event Management process. The last (but not insignificant) problem is the total cost of ownership of the enabling technology, the cost of skilled people to use it, and the indirect nature of the value created for the business. These combine to make funding Event Management difficult to sell.

Once the enabling technology and trained staff exist, the next challenge is analyzing, designing and developing (tool configuration) the filtering and correlation criteria. Mature organizations accomplish this as the IT Service progresses from Design through Transition to Operation. This ensures that the design stage identifies meaningful events, and builds them in (instrumented) so that the IT Service and ongoing operation of the IT Service can tweak the criteria as "conditions on the ground" develop.

IT is unique in its reliance on technology to monitor and manage the technology it uses to provide its services. Event Management ensures that the IT infrastructure monitors only the devices that require monitoring, and that it continuously evaluates events that occur at levels appropriate to their contribution to operations.

The primary risk to Event Management centers around funding its enabling technology. Its expensive and can derail a successful implementation if improperly or over deployment of monitors.

Summary

Purpose – Provide the basis for operational monitoring & control.
Goal – Monitor all events to enable the achievement of normal operation.
Objective – Detect, analyze & direct appropriate control actions.

Scope
- Configuration Items
- Environmental status
- License monitoring
- Security
- Normal activities

Activities
- Notification
- Detection
- Filtering
- Correlation
- Trigger
- Response
- Closure

Measures
- EM integrated services
- EM designed into services
- Event response
  - Evaluated
  - Effective

Value
Event Management (EM) is clearly focused on the generation and detection of meaningful notification about the status of Configuration Items and IT Services.

Summary

Event Management has the responsibility for ensuring the monitoring of all of the events throughout the IT infrastructure. This supports normal on-going operations and enables the detection and escalation of exception events.

ITIL defines an Event as a change of state that has significance for the management of a Configuration Item or IT service. Sometimes the term also means an Alert or notification created by any IT service, Configuration Item or monitoring tool. In this context, it is imperative that the Service Level Agreement (SLA) defines what normal service operation is.

In today's IT infrastructure, there are many "moving parts." Many events occur during a typical day, and the Event Management process helps make sense out of them by:

- Early detection and warning of Incidents
- Exception monitoring
- Integration with Availability & Capacity Management
- Support of automated operations

Chapter 5:

Service Operation Functions

Objectives

Bloom's Level 4 Objectives - Support problem solving by putting theory into practice, interpret principles and relationships.

- The objective, activities and roles of each of the four functions of Service Operation. Know how to build a Service Operation model based on these functions
- Service Operation roles and responsibilities where and how they are used as well as how a Service Operation organization would be structured to use these roles.

Terms-to-Know

Application – Software that provides functions that are required by an IT Service.

Call Center – An organization or business unit that handles large numbers of incoming and outgoing telephone calls.

Diagnostic Script – A structured set of questions used by Service Desk staff to ensure they ask the correct questions, and to help them classify, resolve and assign incidents..

Follow-the-Sun – A methodology for using multiple physical Service Desks and support groups around the world to provide seamless 24/7 service.

Help Desk – A point of contact for users to log incidents. A Help Desk is usually more technically focused than a Service Desk and does not provide a single point-of-contact for all interactions. Often used as a synonym for Service Desk.

Single Point-of-Contact – Provides a single consistent way to communicate with an organization or business unit..

Super User – A user who helps other users, and assists in communication with the Service Desk or other parts of the IT Service Provider's organization. Super Users typically provide support for minor incidents and training.

Introduction to Service Operation Functions

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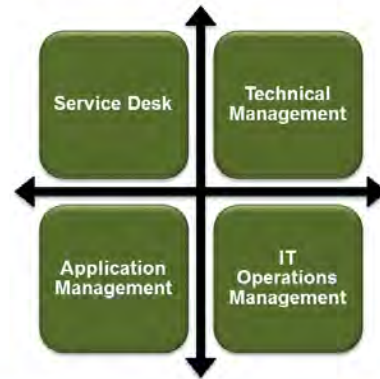
Introduction

The definition of a function is a team or group of people and the tools they need to carry out one or more processes or activities. As discussed in the ITIL Concepts chapter, many organizations newly exposed to the ITIL and to some of the core processes tend to try to organize their functional groups around the process. In some cases, this is appropriate. In many cases, however, the process extends beyond a single functional group and calls for functional group participation, not a reorganization by functional group.

The following sections will explore each of the major functional areas of Service Operation.

Lesson 16

Technical Management

Introduction to Technical Management

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

Service Desk	Technical Management
Application Management	IT Operations Management

Introduction

ITIL defines a function as, "a team or group of people and the tools they use to carry out one or more processes or activities." Within the Service Operation Lifecycle domain, the Technical Management function provides the technical expertise and resources for the overall management of the IT infrastructure, thus its IT Services. It works in conjunction with the other Service Operation functions; Service Desk, IT Operations and Application Management.

Technical Management – Objectives

- Plan, Implement & Maintain IT Infrastructure
  - Technical Topology
    - Well Designed, Resilient & Cost Effective
  - Maintain & Optimize Technical Skills
  - Rapid Deployment of Resources In Support of
    - Incident Management
    - Problem Management
    - Request Fulfillment
    - Other Lifecycle Processes

Technical Management - Objectives

The objectives of the Technical Management Function generally support the achievement of IT Service planning, implementation and maintenance. These objectives are realized through;.

- Technical Topology - the deployment of a well designed, highly resilient and cost effective technical topology
- Maintain & Optimize Technical Skills - Ensure that the Technical Management staff have the requisite skills and that those skills are properly maintained
- Rapid deployment of Resources in Support of the Service Operation and other Service Lifecycle processes

Technical Management – Organizational Structures

- Spread among multiple departments
- Specialization or division of labor
  - Grouped by skill sets
  - Determined by technology to be managed
- Technological areas
  - Specific to components
  - System
  - Platform

Technical Management - Organizational Structures

IT organizations can organize the Technical Management Function is many different ways. Today's complex infrastructures preclude organizing this function into a single department. Most often the function is spread across multiple groups within IT as well as some external service providers.

The normal division of labor is around specific skill sets, such as network, servers, storage, etc. It also can group around a specific technology, such as Windows, UNIX and Linux servers. While these groups manage different "flavors" of servers, they share significant commonality, and staff with requisite skill set and experience can serve as their managers.

In some instances IT organizations can field a structure based on managing a specific set of components, system or platform. This is normally the case when the considerations for the management of the infrastructure calls for specific as opposed to generalized skills. An example of this would be the support and management of UNIX servers used in a robotic production line.

Technical Management – Design, Maintenance & Support

- Technical specialist
  - Architects & designers
  - Maintenance & support
- Normally part of single function
  - Can be split into
    - Design
    - Support
- Involvement must be across the lifecycle

Technical Management - Design, Maintenance & Support

Most groups within the Technical Management Function divide the staff into two complementary functional groups that are involved in the design and support of IT Services. These staff are split along the lines of technical specialization. One group specializes in the IT infrastructure's architecture and design in support of an IT Services. The other group specializes in the maintenance and support of that infrastructure.

While the two groups perform different functions they must participate in each other's role because good architectural design requires an understanding of the practical aspects required to maintain and support it. Conversely, good maintenance and operational procedures require the input from the people involved in the infrastructure's design.

While each group is specialized for design or support they both must participate across the entire IT Service Lifecycle.

Technical Management – Metrics

- Agreed outputs
- Process metrics
- Technology performance
- Availability
- Maintenance
- Training

Technical Management - Metrics

Similar to metrics associated with processes, the intent of measuring the performance of the Technical Management Function is to ensure it achieves the required levels of effectiveness (delivers the required output products of the function) and efficiency (optimum utilization of resources).

The metrics used within the Technical Management Function can be grouped by:

- Measurement of Agreed Outputs - what was contributed, transaction rates, training accomplished, etc.
- Process Metrics - measures of the function's participation is performing their roles within the IT Service Lifecycle processes
- Technology Performance - measurement of the performance of supported technologies
- Availability - measurement of the achievement of required levels of availability
- Maintenance - measurement of proficiency in the diagnosis of incidents and restoration of service
- Training - measurement of skills acquisition and maintenance

Technical Management - Documentation

- Technical documentation
  - Technical manuals
  - Management & administration
  - CI user manuals
- Maintenance schedules
- Skills inventory

Technical Management - Documentation

Technical Management has the responsibility for the creation and maintenance of several types of technical documentation:

- Technical Manuals - used in the direct support of specific technologies
- Management & Administration - used in the management and administration of specific technologies within the infrastructure
- User Manuals - used by technical staff for the operation of specific configuration items

In addition, the Technical Management staff prepares and maintains the maintenance schedule for their respective areas of responsibility. This will include maintenance procedures that are performed by both technical and operations staff.

In order to achieve the objective to establish and maintain the requisite technical skills, the function will record and maintain a skills inventory of their respective staff. Such an inventory can also be included within the Service Portfolio and be used to assess organizational capability in the support of a proposed IT Service. Most often staff skills inventories are held within a Human Resources application, with interface or maintenance capability extended to the management team of the Technical Management Function.

Chapter 6:

Service Operation Considerations

Objectives

Bloom's Level 4 Objectives - Support problem solving by putting theory into practices, interpret principles and relationships.

- Service Operation roles and responsibilities, where and how they are used as well as how a Service Operation organization would be structured to use these roles.
- The technology that support Service Operation, where an how these can be used.
- The technology required to support each of the Service Operation processes and functions.
- Strategies and models for managing Change in Service Operation and how to implement this activity within an organization.
- Implement Service Operation technologies within a company.
- How to assess and manage risk within a Service Operation group, including the interaction that needs to occur with the service Design and Transition personnel.
- The challenges and risks related to Service Operation and the details behind how each challenge can be addressed.
- The Critical Success Factors related to Service Operation as well as a detailed model for measuring and monitoring Service Operation's Critical Success Factors.

Terms-to-Know

Active Monitoring – Monitoring a configuration Item or an IT Service that uses automated regular checks to discover the current status.

Alert – A warning that a threshold has been reached, something has change, or a failure has occurred.

Component – A general term that is used to mean one part of something more complex.

Configuration – A generic term, used to describe a group of Configuration Items that work together to deliver an IT Service, or a recognizable part of an IT Service.

Configuration Item – Any component that needs to be managed in order to deliver an IT Service.

Correlation – A clausal, complementary, parallel, or reciprocal relationship, especially a structural, functional, or qualitative correspondence between two comparable entities.

Detection – A stage in the Incident Lifecycle; results in the incident becoming know to the IT Service Provider.

Directory Service – An application that manages information about IT infrastructure available on a network, and a corresponding user access rights.

Escalation – An activity that obtains additional resources when these are needed to meet Service Level Targets or customer expectations.

Event – A change of state that has significance for the management of a Configuration Item, or IT Service.

Failure – Loss of ability to operate to specification, or to deliver the required output.

Monitoring – Repeated observation of a Configuration Item, IT Service or process to detect events and to ensure that the current status is known.

Passive Monitoring – Monitoring of a Configuration Item, IT Service, or process that relies on an alert or notification to discover the current status.

Remediation – Recovery to a known state after a failed change or release.

Repair – The replacement or correction of a failed Configuration Item.

Work Instruction – A document containing detailed instructions that specify exactly what steps to follow to carry out an activity, and contains much more detail than a procedure.

Appendix:

Service Operation Lifecycle Syllabus

This appendix contains the complete syllabus provided by the Official Accreditor, The APM Group (APMG), for the ITIL Service Operation Lifecycle Certification Course. It is provided here as reference for the use of the student.

Document Control Information

Document Details	
Document Name	The ITIL Intermediate Qualification Service Operation Certificate v5.2
Purpose of Document	Provide a detailed syllabus for the ITIL Intermediate Qualification: Service Operation Certificate
Document Version Number	5.2
Document Status	Live
Document Owner	APM Group-The Accreditor
Prepared By	Examination Panel
Date Approved	June 2011
Approved By	Chief Examiner
Next Scheduled Review Date	

Version History		
Version Number	**Date Approved**	**Change / Reason for Change / Comments**
5.0	01 June 2011	Aligned to the 2011 edition of the ITIL core guidance
5.1	22 June 2011	Updated to reflect additional changes to core guidance
5.2	18 July 2011	Bullet wording clarified in learning unit SO03

**PROFESSIONAL
QUALIFICATION SCHEME**

INTERMEDIATE QUALIFICATION

SERVICE LIFECYCLE

SERVICE OPERATION CERTIFICATE

SYLLABUS

APM Group-The Accreditor

Official Accreditor of the OGC ITIL® Portfolio

Contents

THE ITIL INTERMEDIATE SERVICE LIFECYCLE: SERVICE OPERATION CERTIFICATE

The ITIL Intermediate Qualification: Service Operation Certificate is a free-standing qualification but is also part of the ITIL intermediate lifecycle stream, and one of the modules that leads to the ITIL Expert Certificate in IT Service Management. The purpose of this training module and the associated exam and certificate is, respectively, to impart, test, and validate the knowledge on industry practices in service management as documented in the *ITIL Service Operation* publication.

Target Candidate

The course syllabus covers the management-level concepts and core information of the activities and techniques within service operation, but not specific details about each of the supporting processes.

The main target group for the ITIL Intermediate Qualification: Service Operation Certificate includes, but is not restricted to:

- Chief information officers (CIOs)
- Chief technology officers (CTOs)
- Managers
- Supervisory staff
- Team leaders
- Service designers
- IT architects
- IT planners
- IT consultants
- IT audit managers
- IT security managers
- ITSM trainers involved in the ongoing management, co-ordination and integration of operation activities within the service lifecycle
- Individuals who require a detailed understanding of the ITIL service operation stage of the ITIL service lifecycle and how it may be implemented to enhance the quality of IT service provision within an organization
- IT professionals working within or about to enter a service operation environment and requiring an understanding of the concepts, processes, functions and activities involved
- Individuals who have attained the ITIL Foundation Certificate in IT Service Management and wish to advance to higher level ITIL certifications
- Individuals seeking the ITIL Expert Certification in IT Service Management for which this qualification can be one of the prerequisite modules
- Individuals seeking progress toward the ITIL Master Certificate in IT Service Management for which the ITIL Expert is a prerequisite.

Prerequisite Entry Criteria

Candidates wishing to be trained and examined for this qualification must already hold the ITIL Foundation Certificate in IT Service Management which must be presented as documentary evidence to gain admission

Candidates who hold the following ITIL qualifications are also eligible, and similar evidence will be required:

- Earlier ITIL (V2) Foundation plus Foundation Bridge
- ITIL Expert Certificate in IT Service Management (achieved via Service Manager or Practitioner bridging routes)

Eligibility for Examination

To be eligible for the ITIL Intermediate Qualification: Service Operation examination, the candidate must have fulfilled the following requirements:

- At least 21 contact hours (hours of instruction, excluding breaks, with an Accredited Training Organization (ATO) or an accredited e-learning solution) for this syllabus, as part of a formal, approved training course/scheme
- A basic IT literacy and around 2 years IT experience are highly desirable
- Hold the ITIL Foundation Certificate in IT Service Management (or other appropriate earlier ITIL and bridge qualifications– see *Prerequisite Entry Criteria* on p5)
- It is also recommended that candidates should complete at least 21 hours of personal study by reviewing the syllabus and the *ITIL Service Operation* publication in preparation for the examination, specifically *Chapter 2: Service management as a practice*

Syllabus at a Glance

Learning Unit SO01: Introduction to service operation

Bloom's Level 2 Objectives – Full understanding of service operation terms and core concepts.
- The purpose, objectives and scope of service operation
- The value to the business
- The context of service operation in the ITIL service lifecycle
- The fundamental aspects of service operation and the ability to define them.

Learning Unit SO02: Service operation principles

Bloom's Level 4 Objectives – The knowledge, interpretation and analysis of service operation principles, techniques and relationships and their application to the delivery and support of services at agreed levels.
- How an understanding of the basic conflict between maintaining the status quo and adapting to changes in business needs can lead to better service operation
- Other service operation principles including: involvement in other lifecycle stages; understanding operational health; the need for good documentation and communication including a communication strategy
- Service operation inputs and outputs.

Learning Unit SO03: Service operation processes

Bloom's Level 4 Objectives – The knowledge, interpretation and analysis of service operation principles, techniques and relationships and their application to the delivery and support of services at agreed levels.
- The use, interaction and value of each of the service operation processes: event management, incident management, request fulfilment, problem management, and access management.

Learning Unit SO04: Common service operation activities

Bloom's Level 4 Objectives – The knowledge, interpretation and analysis of service operation principles, techniques and relationships and their application to the delivery and support of services at agreed levels.
- How the common activities of service operation are co-ordinated for the ongoing management of the technology that is used to deliver and support the services
- How monitoring, reporting and control of the services contributes to the ongoing management of the services and the technology that is used to deliver and support the services
- How the operational activities of processes covered in other lifecycle stages contribute to service operation
- How IT operations staff should look for opportunities to improve the operational activities.

Learning Unit SO05: Organizing for service operation

Bloom's Level 4 Objectives – The knowledge, interpretation and analysis of service operation principles, techniques and relationships and their application to the delivery and support of services at agreed levels.
- The role, objectives and activities of each of the four functions of service operation: service desk, technical management, IT operations management, and application management
- Service operation roles and responsibilities, where and how they are used as well as how a service operation organization would be structured to use these roles.

Learning Unit SO06: Technology considerations

Bloom's Level 4 Objectives – The knowledge, interpretation and analysis of service operation principles, techniques and relationships and their application to the delivery and support of services at agreed levels.
- The generic requirements of technologies that support service management across all lifecycle stages
- The specific technology required to support the service operation processes and functions.

Learning Unit SO07: Implementation of service operation

Bloom's Level 4 Objectives – The knowledge, interpretation and analysis of service operation principles, techniques and relationships and their application to the delivery and support of services at agreed levels.

- Specific issues relevant to implementing service operation including: managing change in service operation; assessing and managing risk in service operation; operations staff involvement in service design and service transition
- Planning and implementing service management technologies within a company.

Learning Unit SO08: Challenges, critical success factors and risks

Bloom's Level 4 Objectives – The knowledge, interpretation and analysis of service operation principles, techniques and relationships and their application to the delivery and support of services at agreed levels.

- The challenges (e.g. engagement with staff outside service operation, justifying funding), critical success factors (e.g. management and business support, staff retention) and risks (e.g. loss of service) related to service operation.

Qualification Learning Objectives

This qualification provides a complete management-level overview of service operation including all its related activities.

Candidates can expect to gain competencies in the following upon successful completion of the education and examination components related to this certification:

- Introduction to service operation
- Service operation principles
- Service operation processes
- Common service operation activities
- Organizing for service operation: functions
- Technology considerations
- Implementation of service operation
- Challenges, critical success factors and risks

In addition the training for this certification should include examination preparation, including a mock examination opportunity.

Level of Difficulty

All ITIL service management qualifications use the Bloom's taxonomy in both the construction of the learning units and in the examination which is based on this syllabus.

A learning taxonomy is a scale of the degree of difficulty in the learning process. These levels apply to the cognitive, affective and psychomotor domains of learning but, in the ITIL Qualification Scheme, we deal only with the cognitive sphere.

Bloom defines six levels of learning in the COGNITIVE domain which are both sequential and cumulative. They move from the simple to the complex. This implies that in order to achieve the sixth level of learning, for example, the instructor must ensure that the previous five levels have been mastered.

Level 1 - The KNOWING level: The candidate is able to bring to mind or remember the appropriate material. The examination questions associated with this level tax the candidate's memory and include such tasks as defining, recalling, listing, recognizing, describing and naming.

Level 2 - The COMPREHENDING stage: The candidate is able to understand or grasp the meaning of what is being communicated and make use of the idea without relating it to other ideas or materials and without seeing the fullest possible meaning or translation of the idea. Examination questions at this level would include scenarios giving examples of, illustrating, inferring, summarizing and interpreting. These actions involve the knowing which has taken place at the first level.

Level 3 - The APPLYING level: The candidate should be able to use ideas, principles and theories in new, particular and concrete situations. Examination questions at this level involve both knowing and comprehension, and might include choosing appropriate procedures, applying principles, using an approach or identifying the selection of options.

Level 4 - The ANALYSING level: The candidate is able to break down a communication (rendered in any form) into constituent parts in order to make the organization and significance of the whole clear. Breaking down, discriminating, diagramming, detecting, differentiating and illustrating are important tasks at this level and can be seen to include the previous levels of knowing, comprehending and applying. Here the significance of the constituent parts of an entity are examined in order to understand the whole more fully.

Level 5 - The SYNTHESIS level: At this level the candidate is able to put back together again the various parts or elements of a concept into a unified organization or whole. This putting together again and making sense of small parts is a crucial factor in intelligence and learning. Examination questions at this level would include scenarios involving creating, writing, designing, combining, composing, organizing, revising and planning. In order for this level of learning to occur, it must include the first four levels – knowing, comprehending, analysing and applying. This level of learning is probably the most intense and exciting for the candidate.

Level 6 - The EVALUATING phase: In this phase the candidate is able to arrive at an overview and to judge the value and relative merit of ideas or procedures by using appropriate criteria. At this level of learning the candidate will be able to compare, judge, appraise, justify, criticize and contrast theories, procedures, methods and concepts. This level involves mastery of the five previous levels of knowing, comprehending, applying, analysing and synthesizing.

For the purposes of the ITIL Qualifications Scheme, the Bloom's level will appear in each syllabus module to identify the highest level of cognitive difficulty that the course content should deliver in order to meet the learning outcome and ensure the competence required to meet the examination level of difficulty.

The following table illustrates the use of the taxonomy in ITIL professional qualifications.

Bloom's Levels and taxonomy	Used by ITIL certification	Intellectual activity in learning outcome and exam proficiency
1. Knowing 2. Comprehending	ITIL service management Foundation Level	The ability to recall, recite, name, and understand the meaning of ITIL terminology and basic practice fundamentals. *Vernacular examples used in Syllabus:* Understand; describe; identify
3. Applying 4. Analysing	ITIL service management Lifecycle Stream Capability Stream Managing Across the Lifecycle	The ability to use the practices and concepts in a situation or unprompted use of an abstraction. Can apply what is learned in the classroom in workplace situations. Can separate concepts into component parts to understand structure and can distinguish between facts and inferences. *Vernacular examples used in Syllabus:* Analyse; demonstrate; apply; distinguish; justify; produce; decide
5. Synthesis 6. Evaluating	ITIL service management Managing Across the Lifecycle – level 5 only ITIL Master	The ability to create patterns or structure from composite elements to achieve a new meaning or outcome. Can make judgements, weigh options of ideas and elements to justify and support an argument or case *Vernacular examples used in Syllabus:* Evaluate; justify; summarize; plan; modify; manage; control

Intermediate stream qualifications will examine according to the Bloom's level assigned to each syllabus learning unit within each of the service lifecycle and service capability streams. This means that a candidate must be prepared to be tested up to and including that level for any question related to that learning unit or units.

The examination format of complex multiple choice will offer a scenario and questions with a corresponding series of possible answers. Each is constructed to test a candidate's competency up to and including the Bloom's level associated with the syllabus learning unit that the question is mapped to. Instructors should ensure that the module curriculum offers discussion, practical exercises and instruction that will ensure the candidate has the competence required to meet the exam level of difficulty.

The intermediate modules are expected to provide a practical level of proficiency to enable a candidate to utilize the knowledge learned in their work environment. The examinations test a level of proficiency that allows candidates to apply the knowledge learned in the course to correctly select the correct sequence of possible answers.

Service Operation Syllabus

The ITIL Intermediate Qualification: Service Operation Certificate is awarded to those who complete the following eight units of study described below and who successfully pass the relevant multiple choice examination.

Core guidance references with publication reference (SS - *ITIL Service Strategy*, SD – *ITIL Service Design*, ST – *ITIL Service Transition*, SO – *ITIL Service Operation*, CSI – *ITIL Continual Service Improvement*) and section numbers are included along with indicative contact study hours.

The contact hours are shown in each learning unit and are suggested to provide adequate time to cover the core guidance content. However, Accredited Training Organizations (ATOs) are encouraged to combine or re-order the learning units in any way that suits the flow of their courseware content delivery. All ATOs must ensure, however, that the minimum contact hours for eligibility for examination are met.

Section numbers are indicated as "chapter . section . subsection" (X.X.X). Unless otherwise indicated, instructional coverage of the content of the entire section referenced is assumed.

Learning Unit	Curriculum subjects covered	Level of Difficulty
ITIL SL: SO01 Introduction to service operation	This learning unit covers the introduction of the core concepts and terminology of service operation in relation to the execution and co-ordination of the activities and processes required to deliver, manage and support services at agreed levels to business users and customers. To meet the learning outcomes and examination level of difficulty, the candidates must be able to understand and describe: • The main purpose and objective of service operation Core Guidance References – SO 1.1.1 • The scope of service operation Core Guidance References – SO 1.1.2 • The context of service operation and the service lifecycle Core Guidance References – SO 1.2 • The value to the business Core Guidance References – SO 1.1.4 • Service operation fundamentals Core Guidance References – SO 3.1	Up to Bloom's level 2 Knowing and Comprehending The ability to recall, recite, name and understand the meaning of ITIL terminology and basic practice fundamentals.
	Contact hours recommended – 0.5	
ITIL SL: SO02 Service operation principles	This learning unit addresses service operation principles. All aspects related to operations are covered including achieving balance in service operations, providing good service, involvement in other lifecycle stages and operational health. To meet the learning outcomes and examination level of difficulty, the candidates must be able to understand, describe, identify, demonstrate, apply, distinguish, produce, decide or analyse: • Achieving balance in service operation Core Guidance References – SO 3.2 • Providing good service	Up to Bloom's level 4 Applying and Analysing The candidate should reach a level of competence of the knowledge, interpretation and analysis of service operation

Learning Unit	Curriculum subjects covered	Level of Difficulty
	Core Guidance References – SO 3.3 • Involvement in other lifecycle stages Core Guidance References – SO 3.4 • Operational health Core Guidance References – SO 3.5 • Communication Core Guidance References – SO 3.6 • Documentation Core Guidance References – SO 3.7 • Service operation inputs and outputs Core Guidance References – SO 3.8	principles, techniques and relationships and their application to the delivery and support of services at agreed levels.
	Contact hours recommended – 1.0	
ITIL SL: **SO03** **Service operation processes**	This unit covers the managerial and supervisory aspects of the ITIL processes covered in the service operation stage (but excludes the day-to-day operation of the processes which is covered in the Operational Support and Analysis Capability (OSA) Capability module). This unit should be considered from the management perspective; i.e., those aspects that would be required to understand each process and its interfaces, oversee the implementation of each process, and judge the effectiveness and efficiency of each process. For each core process, all sub-sections in the book should be covered. Candidates must have a good overview of the activities, but will not be expected to have a detailed understanding of process activities or a detailed understanding of specific methods and techniques - unless otherwise stated below. The recommended contact hours for this learning unit should be taken as a guide to the level of detail that can be achieved. For each of the processes the following subsections of the books will be included or excluded: Included: • Purpose and objectives Core Guidance References – SO 4.x.1 • Scope Core Guidance References – SO 4.x.2 • Value to Business Core Guidance References – SO 4.x.3 • Policies, principles and basic concepts Core Guidance References – SO 4.x.4 • Process activities, methods and techniques Core Guidance References – SO 4.x.5 • An understanding of the basic flow and activities. This will be facilitated by the following figures;	**Up to Bloom's level 4** Applying and Analysing The candidate should reach a level of competence of the knowledge, interpretation and analysis of service operation principles, techniques and relationships and their application to the delivery and support of services at agreed levels.

Learning Unit	Curriculum subjects covered	Level of Difficulty

	Event management – SO Figure 4.2
	Incident management – SO Figure 4.3
	Request fulfilment – SO Figure 4.6
	Problem management – SO Figure 4.7
	Access management – SO Figure 4.9
	
	• Triggers, inputs, outputs and interfaces
	Core Guidance References – SO 4.x.6
	
	• Critical success factors and key performance indicators
	Core Guidance References – SO 4.x.8
	
	• Challenges and risks
	Core Guidance References – SO 4.x.9
	
	Excluded
	
	• Process activities, methods and techniques
	Core Guidance References – SO 4.x.5
	
	   • *A detailed knowledge of these activities or a detailed understanding of specific methods and techniques is not required - unless stated below*
	
	• Process information management
	Core Guidance References – SO 4.x.7
	
	To meet the learning outcomes and examination level of difficulty, the candidates must be able to understand, describe, identify, demonstrate, apply, distinguish, produce, decide or analyse:
	
	• Event management
	Core Guidance References – SO 4.1 - subsections as described above
	
	• Incident management
	Core Guidance References – SO 4.2 - subsections as described above
	
	(Candidates must have an understanding of:
	
	   • *the service desk's involvement in incident management (4.2.5.1, 4.2.5.9 and 6.3.2)*
	
	   • *the categorization and prioritization of incidents (4.2.5.3, 4.2.5.4))*
	
	• Request fulfilment
	Core Guidance References – SO 4.3 - subsections as described above
	
	(Candidates must have an understanding of:
	
	   • *the service desk's involvement in request fulfilment (4.3.5.1, 4.3.5.8 and 6.3.2)*
	
	   • *the categorization and prioritization of requests (4.3.5.3, 4.3.5.4))*	

The ITIL Intermediate Qualification Service Operation Certificate v5.2 – July 2011
Version 5.2 (Status – Live)   Document owner – APM Group-The Accreditor
Page 12 of 18

Page 301

Learning Unit	Curriculum subjects covered	Level of Difficulty
	• Problem management Core Guidance References – SO 4.4 - subsections as described above *(Candidates must have an understanding of the categorization and prioritization of problems as described in 4.4.5.3 and 4.4.5.4)* *(Candidates do not require a detailed understanding of the problem analysis techniques described in SO 4.4.4.3)* • Access management Core Guidance References – SO 4.5 - subsections as described above	
	Contact hours recommended – 7.0	
ITIL SL: **SO04** **Common service operation activities**	This unit covers the activities commonly performed in service operation. To meet the learning outcomes and examination level of difficulty, the candidates must be able to understand, describe, identify, demonstrate, apply, distinguish, produce, decide or analyse: • Monitoring and control Core Guidance References – SO 5.1 • IT operations Core Guidance References – SO 5.2 • Server and mainframe management and support Core Guidance References – SO 5.3 • Network management Core Guidance References – SO 5.4 • Storage and archive Core Guidance References – SO 5.5 • Database administration Core Guidance References – SO 5.6 • Directory services management Core Guidance References – SO 5.7 • Desktop and mobile device support Core Guidance References – SO 5.8 • Middleware management Core Guidance References – SO 5.9 • Internet/web management Core Guidance References – SO 5.10 • Facilities and data centre management Core Guidance References – SO 5.11 • Operational activities of processes covered in other lifecycle stages Core Guidance References – SO 5.12 • Improvement of operational activities Core Guidance References – SO 5.13	**Up to Bloom's level 4** Applying and Analysing The candidate should reach a level of competence of the knowledge, interpretation and analysis of service operation principles, techniques and relationships and their application to the delivery and support of services at agreed levels.

Learning Unit	Curriculum subjects covered	Level of Difficulty
	Contact hours recommended – 3.0	

ITIL SL:
 	
SO05
 	
Organizing for service operation
	This learning unit explores the organization of service operation through the service operation functions (e.g. service desk, technical management, IT operations management and application management) and maps these functions to roles, responsibilities and activities as well as organizational structures.
	
	To meet the learning outcomes and examination level of difficulty, the candidates must be able to understand, describe, identify, demonstrate, apply, distinguish, produce, decide or analyse:
	
	• Functions
	
	   • Service desk function
	     Core Guidance References – SO 6.3
	
	   • Technical management function
	     Core Guidance References – SO 6.4
	
	   • IT operations management function
	     Core Guidance References – SO 6.5
	
	   • Application management function
	     Core Guidance References – SO 6.6
	
	• Roles
	  Core Guidance References – SO 6.7
	
	• Service operation organizational structures
	  Core Guidance References – SO 6.10
		Up to Bloom's level 4
		
		Applying and Analysing
		
		The candidate should reach a level of competence of the knowledge, interpretation and analysis of service operation principles, techniques and relationships and their application to the delivery and support of services at agreed levels.

	Contact hours recommended – 4.5	

ITIL SL:
 	
SO06
 	
Technology considerations
	This unit covers technology as part of implementing service management process capabilities. It also covers the special technology functions and features that are related to service operation practices.
	
	To meet the learning outcomes and examination level of difficulty, the candidates must be able to understand, describe, identify, demonstrate, apply, distinguish, produce, decide or analyse:
	
	• Technology, tools and telephony requirements for the service operation processes and functions, including:
	
	   • Generic requirements
	     Core Guidance References – SO 7.1
	
	   • Event management
	     Core Guidance References – SO 7.2
	
	   • Incident management
	     Core Guidance References – SO 7.3
	
	   • Request fulfilment
	     Core Guidance References – SO 7.4
	
	   • Problem management
	     Core Guidance References – SO 7.5
	
	   • Access management
		Up to Bloom's level 4
		
		Applying and Analysing
		
		The candidate should reach a level of competence of the knowledge, interpretation and analysis of service operation principles, techniques and relationships and their application to the delivery and support of services at agreed levels.

Learning Unit	Curriculum subjects covered	Level of Difficulty
	Core Guidance References – SO 7.6 • Service desk Core Guidance References – SO 7.7	
	Contact hours recommended – 1.0	
ITIL SL: SO07 Implementation of service operation	This unit covers how implementation considerations contibute to service operation. To meet the learning outcomes and examination level of difficulty, the candidates must be able to understand, describe, identify, demonstrate, apply, distinguish, produce, decide or analyse: • Managing change in service operation Core Guidance References – SO 8.1 • Service operation and project management Core Guidance References – SO 8.2 • Assessing and managing risk in service operation Core Guidance References – SO 8.3 • Operational staff in design and transition Core Guidance References – SO 8.4 • Planning and implementing service management technologies Core Guidance References – SO 8.5	**Up to Bloom's level 4** Applying and Analysing The candidate should reach a level of competence of the knowledge, interpretation and analysis of service operation principles, techniques and relationships and the application of them to the delivery and support of services at agreed levels.
	Contact hours recommended – 2.0	
ITIL SL: SO08 Challenges, critical success factors, and risks	This unit covers the challenges and risks facing service operation and how critical success factors (CSF) contribute to service operation. To meet the learning outcomes and examination level of difficulty, the candidates must be able to understand, describe, identify, demonstrate, apply, distinguish, produce, decide or analyse: • Challenges Core Guidance References – SO 9.1 • Critical success factors Core Guidance References – SO 9.2 • Risks Core Guidance References – SO 9.3	**Up to Bloom's level 4** Applying and Analysing The candidate should reach a level of competence of the knowledge, interpretation and analysis of service operation principles, techniques and relationships and their application to the delivery and support of services at agreed levels.
	Contact hours recommended – 0.5	
ITIL SL: SO09	This unit summarizes the material covered in the previous units and prepares candidates for the examination. It is likely that most course providers will wish to offer and	

Learning Unit	Curriculum subjects covered	Level of Difficulty
Summary, exam preparation and directed studies	review at least one opportunity for a mock examination.	
	Contact hours recommended – 1.5	

Lecture and Exercises

Meeting the learning objectives of this syllabus can be aided by the use of practical exercises during the delivery of an accredited course. It is recommended that course providers make use of exercises to enhance the reinforcement of the learning objectives in this syllabus. To aid course providers, there are areas within each learning unit whose learning objective includes such phrases as "identify, describe, analyse", etc, which may be considered as opportunities to introduce practical course exercises. These are not mandated areas for practical exercises, but provided as suggestions for use by course providers.

Format of the Examination

Type	Eight (8) multiple choice, scenario-based, gradient-scored questions. Each question will have 4 possible answer options, one which is worth 5 marks, one which is worth 3 marks, one which is worth 1 mark, and one which is a distracter and achieves no marks.
Duration	Maximum 90 minutes for all candidates in their respective language
Provisions for additional time relating to language	Candidates completing an exam: • in a language that is not their mother tongue, **and** • where the language of the exam is **not** their primary business language, have a maximum of 120 minutes to complete the exam and are allowed the use of a dictionary
Prerequisite	• ITIL Foundation Certificate in IT Service Management (or other appropriate earlier ITIL and bridge qualifications– see *Prerequisite Entry Criteria* on p5) • Completion of an Accredited course from an ITIL Accredited Training Provider
Supervised	Yes
Open Book	No
Pass Score	28/40 or 70%

Criteria of Training Competence

This syllabus can only be delivered to target groups by an accredited provider/trainer. Any provider/trainer must hold the following qualifications to be eligible to provide this syllabus:

Criteria	Eligibility	Degree of proficiency validation
Accredited Training Organization	Required	The company shall be registered and in good standing with the Official Accreditor
ITIL Service Operation Certification	Required	Instructor must present a valid certificate issued by an accredited Examination Institute
ITIL Expert Certification	Required	Instructor must present a valid certificate issued by an accredited Examination Institute

Approved Delivery Structure

Structure	Operational Standard Requirements
Training Delivery	• Training providers are free to structure and organize their training in the way they find most appropriate, provided the units of the syllabus are sufficiently covered. • Training must be delivered via an ATO and based on this syllabus. Training can be delivered virtually, via an e-learning / learning technology solution.

Terminology List

After studying this course, the candidate is expected to understand the meanings of the following terms in the context of service operation. This list does not include terms that are explicitly mentioned within the learning units of this syllabus - for example, "operational health".

active monitoring	follow the sun	recovery
alert	function	request model
availability	functional escalation	restore
backup	hierarchic escalation	risk management
budgeting	identity	root cause
business case	incident	root cause analysis
business objective	information security management system	second-line support
business relationship management	interactive voice response	service catalogue
call	IT operations control	service design
call centre	IT service continuity plan	service hours
capacity	job scheduling	service knowledge management system
change advisory board	key performance indicator	service level
change schedule	known error	service level agreement
computer telephony integration	known error database	service level target
configuration item	live environment	service portfolio
configuration management system	major incident	service request
continual service improvement	management information system	standard change
CSI register	Management of Risk (M_o_R)	standard operating procedures
customer-facing service	management system	storage management
dashboard	monitor control loop	super user
diagnosis	operational level agreement	supplier
diagnostic script	operations bridge	support group
downtime	outcome	support hours
driver	passive monitoring	technical management
early life support	Plan-Do-Check-Act	technical support
effectiveness	priority	third-line support
efficiency	proactive monitoring	threshold
escalation	proactive problem management	underpinning contract
event	problem	urgency
expanded incident lifecycle	project	user
facilities management	quality	workaround
first-line support	reactive monitoring	

-------------------- END OF DOCUMENT --------------------

Appendix:

SO Process Flow Diagrams

The Service Operation stage of the IT Service Management Lifecycle has five processes;

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

The following are the flow diagrams for each process.

64 | Service operation processes
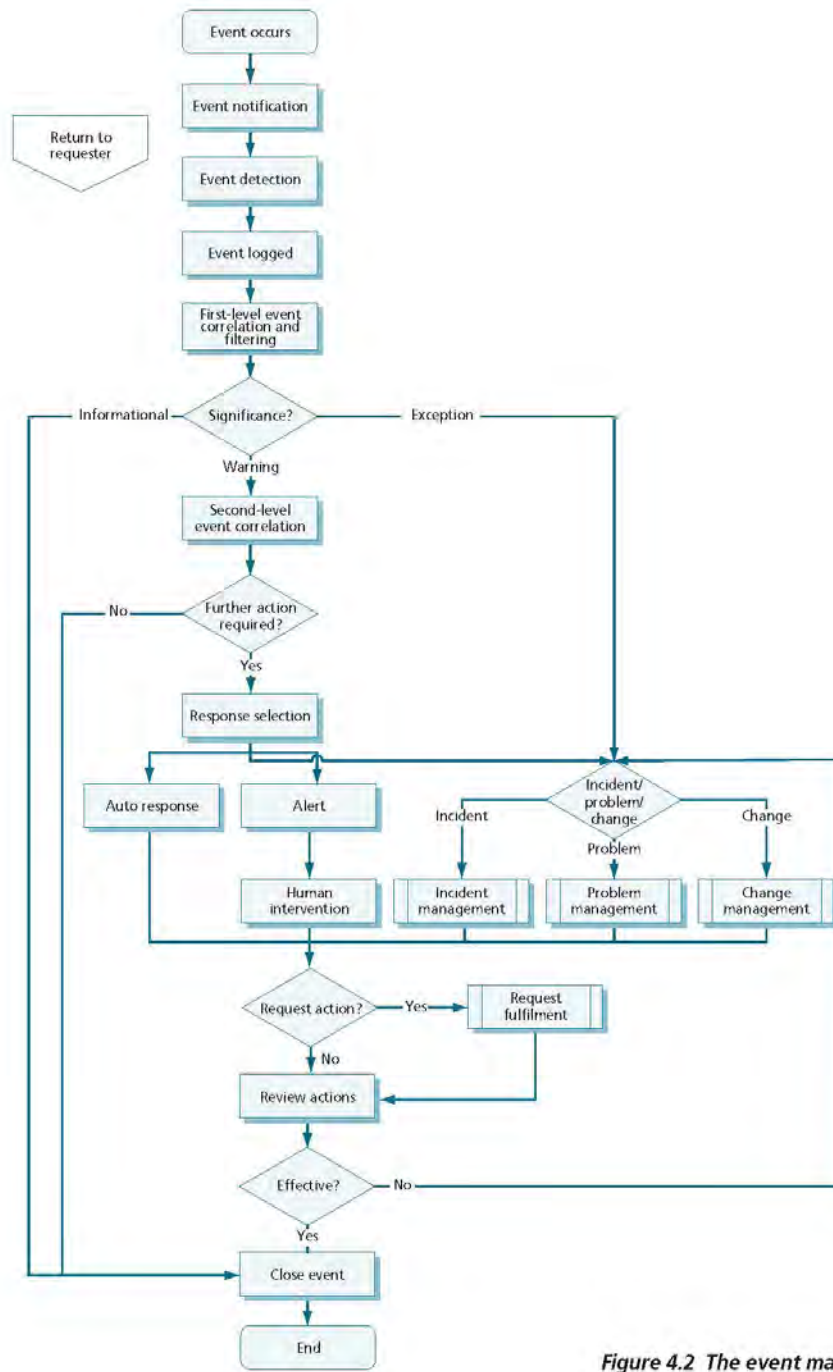
Figure 4.2 The event management process

ITIL Glossary

A

Acceptance
Formal agreement that an IT Service, process, plan, or other deliverable is complete, accurate, reliable and meets its specified requirements. Acceptance is usually preceded by Evaluation or Testing and is often required before proceeding to the next stage of a project or process.

Access Management
The Process responsible for allowing users to make use of IT Services, data, or other assets. Access Management helps to protect the Confidentiality, Integrity and Availability of Assets by ensuring that only authorized users are able to access or modify the assets. Access Management is sometimes referred to as Rights Management or Identity Management.

Account Manager
A role that is very similar to Business Relationship Manager, but includes more commercial aspects. Most commonly used when dealing with external customers.

Accounting
The Process responsible for identifying actual Costs of delivering IT Services, comparing these with budgeted costs, and managing variance from the Budget.

Accredited
Officially authorized to carry out a role. For example, an Accredited body may be authorized to provide training or to conduct audits.

Active Monitoring
Monitoring of a Configuration Item or an IT Service that uses automated regular checks to discover the current status.

Activity
A set of actions designed to achieve a particular result. Activities are usually defined as part of processes or plans, and are documented in procedures.

Agreement
A document that describes a formal understanding between two or more parties. An dgreement is not legally binding unless it forms part of a contract.

Alert
A warning that a threshold has been reached, something has changed, or a Failure has occurred. Alerts are often created and managed by System Management tools and are managed by the Event Management Process.

Application
Software that provides functions that are required by an IT Services. Each Application may be part of more than on IT Service. An Application runs on one or more Servers or Clients. See also Application Management, Application Portfolio.

Application Management
The Function responsible for managing Applications throughout their lifecycle.

Application Portfolio
A database or structured document used to manage Applications throughout their lifecycle. The Application Portfolio contains key attributes of all applications. The Application Portfolio is sometimes implemented as part of the Service Portfolio, or as part of the Configuration Management System.

Application Sizing
The activity responsible for understanding the resource requirements needed to support a new application, or a major change to an existing application. Application Sizing helps to ensure that the IT Service can meet it agreed Service Level Targets for capacity and performance.

Architecture
The structure of a system or IT Service, including the relationships of components to each other and to the environment they are in. Architecture also includes the standards, and guidelines that guide the design and evolution of the system.

Assessment
Inspection and analysis to check whether a standard or set of guidelines is being followed, that records are accurate, or that efficiency and effusiveness targets are being met.

Asset
Any Resource or Capability. Assets of a Service Provider including anything that could contribute to the delivery of a service. Assets can be one of the following types; Management, Organization, Process, Knowledge, People, Information, Applications, Infrastructure, and Financial Capital.

Asset Management
Asset Management is the process responsible for tracking and reporting the value and ownership of financial assets throughout their lifecycle. Asset Management is part of an overall Service Asset and Configuration Management Process.

Attribute
A piece of information about a Configuration Item. Examples are; name, location, Version number and Cost. Attributes of CIs are recorded in the Configuration Management Database (CMDB).

Audit
Formal inspection and verification to check whether a standard or set of guidelines is being followed, that records are accurate, or that efficiency and effectiveness targets are being met. An Audit may be carried out by internal or external groups.

Authority Matrix
See RACI

Automatic Call Distribution (ACD)
Use of the information Technology to direct an incoming telephone call to the most appropriate person in the shortest possible time. ACD is sometimes called Automated Call Distribution.

Availability
Ability of a Configuration Item or IT Service to perform its agreed Function when required. Availability is determined by Reliability, Maintainability, Serviceability, Performance, and Security. Availability is usually calculated as a percentage. This calculation is often based on Agreed Service Time and Downtime. It is Best Practice to calculate Availability using measures of the Business output of the IT Service.

Availability Management
The process responsible for defining, analyzing, Planning, measuring and improving all aspects of the availability of IT Services. Availability Management is responsible for ensuring that all IT infrastructure, processes, tools, roles, etc. are appropriate for the agreed Service Level Targets for availability.

Availability Management Information System (AMIS)
A set of tools, data and information that is used to support Availability Management. See also Service Knowledge Management System.

Availability Plan
A plan to ensure that existing and future Availability Requirements for IT Services can be provided cost effectively.

B

Back-out
See Remediation

Backup
Copying data to protect against loss of Integrity or Availability of the original.

Balanced Scorecard
A management tool developed by Drs. Robert Kaplan (Harvard Business School) and David Norton, A Balanced Scorecard enables a Strategy to be broken down into Key Performance Indicators. Performance against the KPIs is used to demonstrate how well the Strategy is being achieved. A Balanced Scorecard has four major areas, each of which has a small number of KPIs. The same four areas are considered at different levels of detail throughout the Organization.

Baseline
A Benchmark used as a reference point. For example: An ITSM Baseline can be used as a starting point to measure the effect of a Service Improvement Plan. A Performance Baseline can be used to measure change in Performance over the lifetime of an IT Service. A Configuration Management Baseline can be used to enable the IT Infrastructure to be restored to a known Configuration if a Change or Release fails.

Benchmark
The recorded state of something at a specific point in time. A Benchmark can be created for a configuration, a process, or any other set of data. For example, a benchmark can be used in Continual Service Improvement, to establish the current state for managing improvements or Capacity Management, to document performance characteristics during normal operations.

Benchmarking
Comparing a Benchmark with a Baseline or with Best Practice. The term Benchmarking is also used to mean creating a series of Benchmarks over time, and comparing the results to measure progress or improvement.

Best Management Practice (BMP)
The Best Management Practice portfolio is owned by the Cabinet Office, part of HM Govermnent. The BMP portfolio includes guidance on IT Service Management and Project, Program, Risk Portfolio and Value Management.

Best Practice
Proven Activities or Processes that have been successfully used by multiple Organizations. ITIL is an example of Best Practice.

Billing
Part of the charging proces. Billing is the activity responsible for producing an invoice or a bill and recovering the money from customers. See also Pricing.

Brainstorming
A technique that helps a team to generate ideas. Ideas are not reviewed during the Brainstorming session, but at a later stage. Brainstorming is often used by Problem Management to identify possible causes.

British Standards Institution (BSI)
The UK national standards body, responsible for creating and maintaining British Standards.

Budget
A list of all the money an organization or business Unit plans to receive, and plans to pay out, over a specified period of time.

Budgeting
The Activity of predicting and controlling the spending of money. Consists of a periodic negotiation cycle to set future budgets (usually annual) and the day-to-day monitoring and adjusting of current budgets.

Build
The Activity of assembling a number of Configuration Items to create part of an IT Service. The term Build is also used to refer to a release that is authorized for distribution. For example Server Build or laptop Build.

Business
An overall corporate entity or organization formed of a number of Business Units. In the context of ITSM, the term Business includes public sector and not-for-profit organizations, as well as companies. An IT Service Provider provides IT Services to a customer within a Business. The IT Service Provider may be part of the same Business as its customer (Internal Service Provider), or part of another Business (External Service Provider).

Business Capacity Management
In the context of ITSM, Business Capacity Management is the sub-process of Capacity Management responsible for understandng future business requirements for use in the Capacity Plan.

Business Case
Justification for a significant item of expenditure. Includes information about costs, benefits, options, issues, Risks, and possible problems.

Business Continuity Management
The business process responsible for managing risks that could seriously affect the business.

Business Customer
A recipient of a product or a service from the business. For example, if the business is a car manufacturer then the business customer is someone who buys a car.

Business Impact Analysis (BIA)
BIA is the activity in Business Continuity Management that identifies Vital Business Functions and their dependencies. These dependencies may include Suppliers, people, other business processes, IT Services etc. BIA defines the recovery requirements for IT Services. These requirements include Recovery Time Objectives, Recovery Point Objectives and minimum Service Level Targets for each IT Service.

Business Objective
The Objective of a business process, or of the business as a whole. Business Objectives support the business vision, provide guidance for

the IT Strategy, and are often supported by IT Services.

Business Operations
The day to day execution, monitoring and management of business processes.

Business Perspective
An understanding of the Service Provider and IT Services from the point of view of the business, and an understanding of tthe business from the point of view of the Service Provider.

Business Process
A Process that is owned and carried out by the Business. A Business Process contributes to the delivery of a product or service to a business customer.

Business Relationship Management
The process or function responsible for maintaining a relationship with the business. Business Relationship Management usually includes: managing personal relationships with usiness managers, providing input to Service Portfolio Management, ensuring that the IT Service Provider is satisfying the business needs of the customers.

Business Relationship Manager
A role responsible for maintaining the relationship with one or more customers. This role is often combined with the Service Level Manager role.

Business Service
An IT Service that directly supports a business process, as opposed to an infrastructure service, which is used internally by the IT Service Provider and is not usually visible to the business.

Business Service Management (BSM)
An approach to the management of IT Services that considers the business processes supported and the Business value provided. The term also means the management of Business Services delivered to business customers.

Business Unit
A segment of the business that has its own plans, Metrics, income and costs. Each Busi-

ness Unit owns assets and uses these to create value for customers.

C

Call
A telephone call to the Service Desk from a user. A call could result in an incident or a Service Request being logged.

Call Center
An Organization or Business Unit that handles large numbers of incoming and outgoing telephone calls.

Call Type
A Category that is used to distinguish incoming requests to a Service Desk. Common call types are Incident, Service Request and Complaint.

Capability
The ability of an organization, person, process, application, IT Service or other Configuration Item to carry out an activity. Capabilities are intangible assets of an organization. See also resource.

Capability Maturity Model Integration (CMMI)
A process improvement appoach developed by the Software Engineering Institue (SEI) of Carnegie Mellon University. CMMI provides organizations with the essential elements of effetive processes.It can be used to guide process improvement across a project, a division or an entire organization. CMMI helps integrate traditionally separate organizational functions, set process improvement goals and priorties, provide guidance for quality processes and current process.

Capacity
The maximum throughput that a Configuration Item or IT Service can deliver while meeting agreed Service Level Targets. For some types of CI, Capacity may be the size or volume, for example a disk drive.

Capacity Management
The process responsible for ensuring that the Capacity of IT Services and the IT

Infrastructure is able to deliver agreed Service Level Targets in a cost effective and timely manner. Capacity Management considers all resources required to deliver the IT Service and plans for short, medium and long term business requirements.

Capacity Management Information System
A set of tools, data and information that is used to support Capacity Management See also Service Knowledge Management System.

Capacity Plan
A Capacity Plan is used to manage the resources required to deliver IT Services. The plan contains scenarios for different predictions of business demand, and costed options to deliver the agreed Service Level Targets.

Capacity Planning
The Activity within Capacity Management responsible for creating a Capacity Plan.

Capital Cost
The cost of purchasing something that will become a financial asset. The value of the asset depreciates over multiple accounting periods.

Capital Expenditure (CAPEX)
The cost of purchasing something that will become a financial asset, for example, computer equipment and buildings. The value of the asset is depreciated over multiple accounting periods.

Category
A named group of things that have something in common. Categories are used to group similar things together. For example, Cost Types are used to group similar types of Cost, Incident Categories are used to group similar types of Incidents, CI Types are used to group similar types of configuration Items.

Certificate
Issuing a certificate to confirm Compliance to a standard. Certification includes a formal audit by an independent and accredited body. The term Certification is also used to mean

awarding a certificate to verify that a person has achieved a qualification.

Certification
Issuing a certificate to confirm compliance to a standard. Cetrification includes a formal audit by an independent and accredited body. The term is also use dto men awading a certificate to provide evidence that a person ahas acheived a qualification.

Change
The addition, modification or removal of anything that could have an effect on IT Services. The scope should include all IT Services, Configuration Items, processes, documentation, etc.

Change Advisory Board (CAB)
A group of people that advises the Change Manager in the assessment, prioritization and scheduling of Changes. This board is usually made up of representatives from all areas within the IT Service Provider, representatives from the business and third parties such as suppliers.

Change Case
The Process responsible for controlling the lifecycle of all changes. The primary objective of Change Management is to enable beneficial Changes to be made, with minimum disruption to IT Services.

Change Evaluation
The process responsible for formal assessment of a new or changed IT Service to ensure that risks have been managed and to help determine whether to authorize the change.

Change Management
The process responsibile for controlling the lifecycle of all changes, enabling beneficial changes to be made with minimum disruption to IT Services.

Change Model
A repeatable way of dealing with a particular Category of Change. A Change Model defines specific pre-defined steps that will be followed for a change of this Category. Change Models may be very simple, with no requirement for approval (e.g. Password Reset) or may be very complex with many steps that require approval (e.g. major software release). See also Standard Change, Change Advisory Board.

Change Proposal
A document that includes a high level description of a potential service introduction or significant change along with a corresponding business case and an expected implementation schedule. Change proposals are normally created by the Service Portfolio Management process and are passed to Change Management for authorization. Change Management will review the potential impact on other services, on shared,resources, and on the overall change schedule. Once the change proposal has been authorized, Service Portfolio Management will charter the service.

Change Record
A Record containing the details of a Change. Each Change Record documents the lifecycle of a single Change. A Change Record is created for every Request for Change that is received, even those that are subsequently rejected. Change Records should reference the Configuration Items that are affected by the Change. Change Records are stored in the Configuration Management System.

Change Schedule
A document that lists all approved Changes and their planned implementation dates. A Change Schedule is sometimes called a Forward Schedule of Change, even though it also contains information about Changes that have already been implemented.

Charging
Requiring payment for IT Services. Charging for IT Services is optional and many Organizations choose to treat their IT Service Provider as a Cost Center.

Charging Policy
A policy specifiying the objective of the charging process and the way in which charges will be calculated.

Charging Process
The process responsible for deciding how much customer should pay (pricing) and recovering money from them (billing). This process is not described in detail within the core ITIL publications.

Charter
A document that contains details of a new service, a signficant change or other significant project. Charters are typically authorized by Service Portfolio Managmeent or by a Project Management Office. The term charter is also used to describe the act of authorizing the work required to complete the service change or project.

Chronological Analysis
A technique used to help identify possible causes of Problems. All available data about the problem is collected and sorted by date and time to provide a detailed time line. This can make it possible to identify which events may have been triggered by others.

Classification
The act of assigning a category to something. Classification is used to ensure consistent management and reporting. CIs, Incidents, Problems, Changes etc. are usually classified.

Client
A generic term that means a Customer, the Business or a Business Customer. For example, Client Manager may be used as a synonym for Accounting Manager.

Closed
The final status in the Lifestyle of an Incident, Problem, Change etc. When the status is closed no further action is taken.

Closure
The act of changing the Status of an Incident, Problem, Change etc. to Closed.

CoBIT
Control Objectives for information and related Technology (CoBIT) provides guidance and Best Practice for the management of IT Processes. CoBIT is published by the IT Governance Institute. See www.isaca.org for more information.

Code of Practice
A guideline published by a public body or a standards organization, such as ISO or BSI. Many standards consist of a code of practice and a specification. The code of practice describes recommended best practice.

Commercial Off-The-Shelf (COTS)
Application software or Middleware that can be purchased from a Third Party.

Compliance
Ensuring that a Standard or a set of Guidelines is followed, or that proper, consistent accounting or other practices are being employed.

Component
A general term that is used to mean one part of something more complex. For example, a computer System may be a Component of an IT Service, an Application may be a Component of a Release Unit. Components that need to be managed should be Configuration Items.

Component Capacity Management
The Process responsible for understanding the Capacity, Utilization and Performance of Configuration Items. Data is collected, recorded and analyzed for use in the Capacity Plan. See also Service Capacity Management.

Component CI
A Configuration Item that is part of an assembly. For example, a CPU or memory CI may be part of a server CI.

Component Failure Impact Analysis (CFIA)
A technique that helps to identify the impact of CI failure on IT Services. A matrix is created with IT Services on one edge and CIs on the other. This enables the identification of critical CIs (that could cause the failure of multiple IT Services) and of fragile IT Services (that have multiple Single Points of Failure.)

Computer Telephony Integration (CTI)
Computer telephony Integration (CTI) is a general term covering any kind of integration between computers and telephone Systems. It is most commonly used to refer to systems where an application displays detailed screens relating to incoming or outgoing telephone

calls. See also Automatic Call distribution, Interactive Voice Responses.

Concurrency
A measure of the number of Users engaged in the same Operation at the same time.

Confidentiality
A security principle that requires that data should only be accessed by authorized people.

Configuration
A generic term used to describe a group of Configuration Items that work together to deliver an IT Service, or a recognizable part of an IT Service. Configuration is also used to describe the parameter settings for one or more CIs.

Configuration Baseline
The baseline of a configuration that has been formally agreed and is managed through the Change Management process. A Configuration Baseline is used as a basis for future builds, releases and changes.

Configuration Control
The activity responsible for ensuring that adding, modifying or removing a CI is properly managed, for example by submitting a Request for Change or Service Request.

Configuration Item (CI)
Any component that needs to be managed in order to deliver an IT Service. Information about each CI is recorded in a Configuration Record within the Configuration Management System and is maintained throughout its Lifecycle by Configuration Management. CIs are under the control of Change Management. CIs typically include IT Services, hardware, software, buildings, people, and formal documentation such as Process documentation and SLAs.

Configuration Management
The Process responsible for maintaining information about Configuration Items required to deliver an IT Service, including their Relationships. This information is managed throughout the Lifestyle of the CI. Configuration Management is part of an overall Service Asset and Configuration Management Process.

Configuration Management Database (CMDB)
A database used to store Configuration Records throughout their Lifecycle. The Configuration Management System maintains one or more CMDBs, and each CMDB stores Attributes of CIs, and Relationships with other CIs.

Configuration Management System (CMS)
A set of tools and databases that are used to manage an IT Service Provider's Configuration Data. The CMS also includes information about Incidents, Problems, Known Errors, Changes and Releases; and it may contain data about employees, Suppliers, locations, Business Units, Customers and Users. The CMS includes tools for collecting, storing, managing, updating, and presenting data about all Configuration Items and their Relationships. The CMS is maintained by Configuration Management and is used by all IT Service Management Processes. See also Configuration Management Database, Service Knowledge Management System.

Continual Service Improvement (CSI)
A stage in the Lifestyle of an IT Service and the title of one of the Core ITIL publications. Continual Service Improvement is responsible for managing improvements to IT Service Management Processes and IT Services. The performance of the IT Service Provider is continually measured and improvements are made to Processes, IT Services, and IT Infrastructure in order to increase Efficiency, Effectiveness, and Cost Effectiveness. See also Plan-Do-Check-Act.

Contract
A legally binding Agreement between two or more parties.

Control
A means of managing a Risk, ensuring that a Business Objective is achieved, or ensuring that a Process is followed. Example: Controls include policies, procedures, roles, RAID, door locks etc. A Control is sometimes called a countermeasure or safeguard. Control also