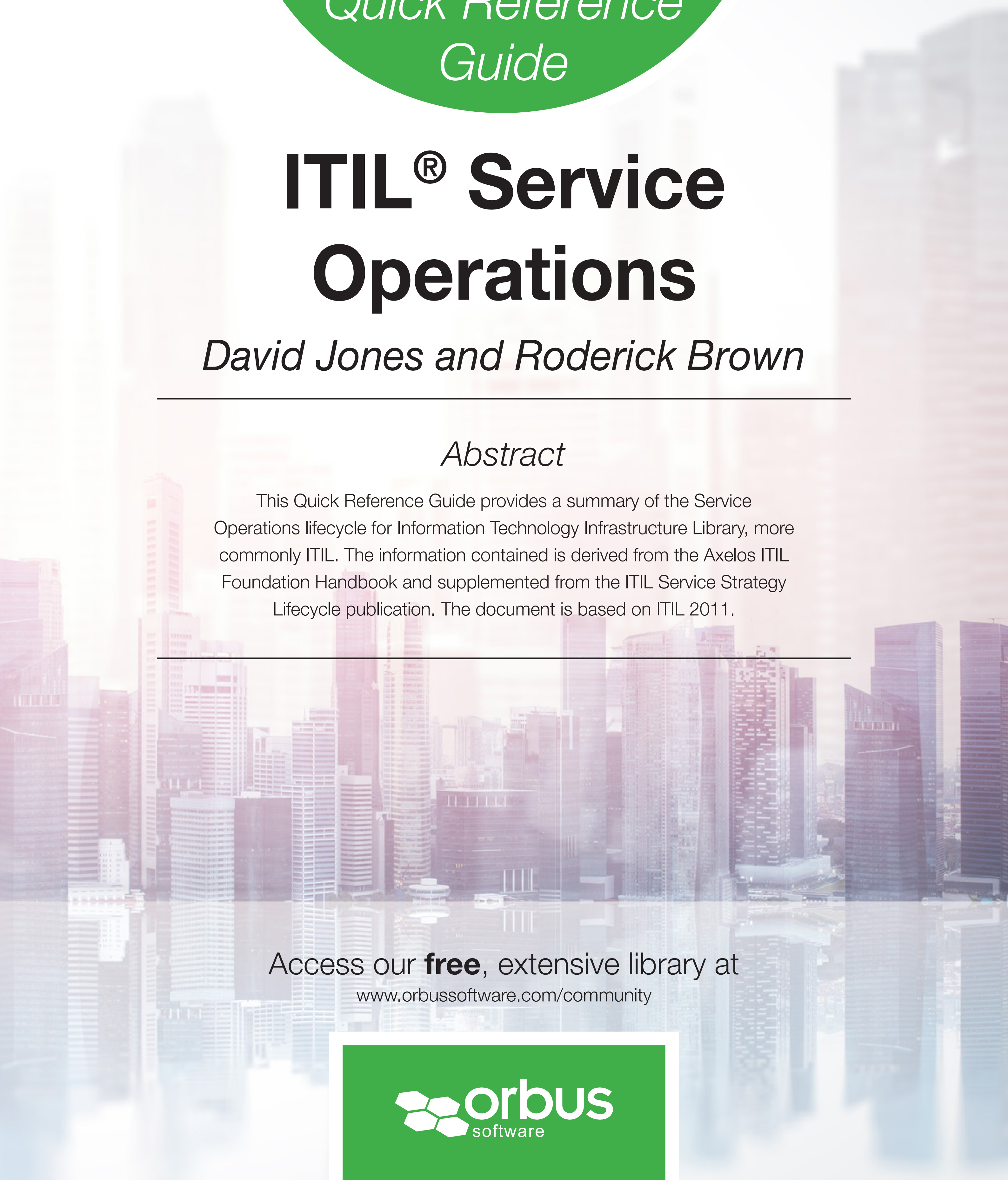
Quick Reference Guide

ITIL® Service Operations

David Jones and Roderick Brown

Abstract

This Quick Reference Guide provides a summary of the Service Operations lifecycle for Information Technology Infrastructure Library, more commonly ITIL. The information contained is derived from the Axelos ITIL Foundation Handbook and supplemented from the ITIL Service Strategy Lifecycle publication. The document is based on ITIL 2011.



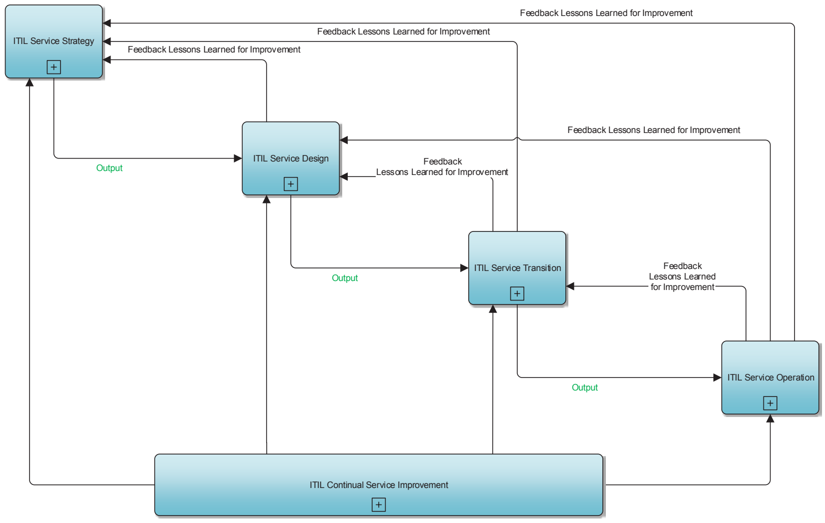
Introducing ITIL Service Operation

Background

ITIL is the well-known set of practices for IT service management (ITSM) that focuses on aligning IT services with the needs of business.

Figure 1 provides a high level overview of the complete ITIL service lifecycle. This Quick Reference Guide (QRG) is the 4th and penultimate in a series of Quick Reference Guides for ITIL and covers the Service Operation lifecycle phase of ITIL.

So far, we have learned some of the key concepts of ITIL Service Management, Service Strategy, Service Design and Service Transition. Each of these has demonstrated how it contributes to service quality, but it is in Service Operation that the business customer sees the quality of the strategy, the design and the transition come to life in everyday use of the services.



Feedback Lessons Learned for Improvement
ITIL Service Strategy
Feedback Lessons Learned for Improvement
Feedback Lessons Learned for Improvement
Feedback Lessons Learned for Improvement
ITIL Service Design
Output
Feedback
Lessons Learned for Improvement
ITIL Service Transition
Output
Feedback
Lessons Learned
for Improvement
ITIL Service Operation
Output
ITIL Continual Service Improvement

Figure 1: Service Operation Context

Figure1 shows that Service Operation is the stage in the service lifecycle where value is realized from the other stages

Overview

Service operation is the phase in the ITIL service management lifecycle that is responsible for business-as-usual activities. It can be viewed as the ‘factory’ of IT. This implies a closer focus on the day-to-day activities and infrastructure that are used to deliver services. The overriding purpose of service operation is to deliver and support services. Management of the infrastructure and the operational activities must always support this purpose.

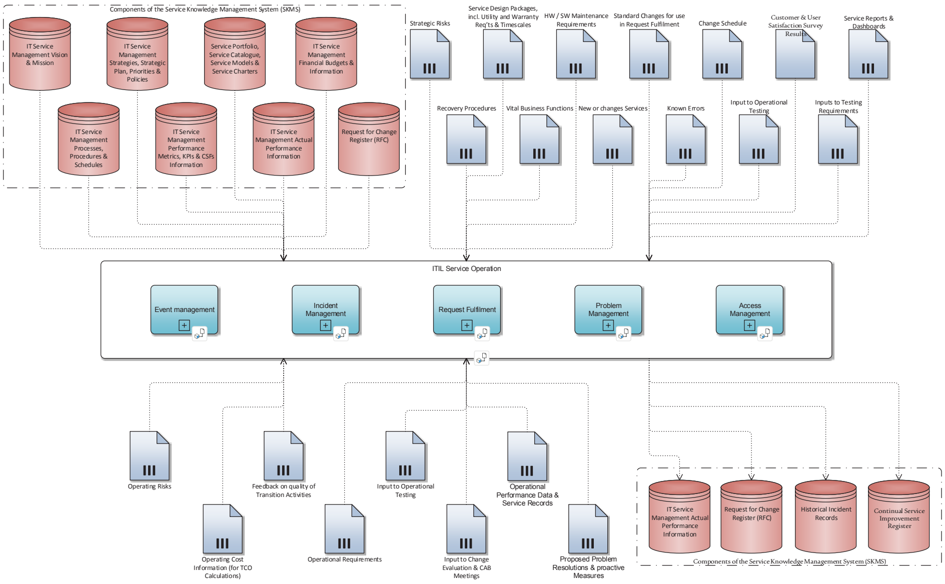

Components of the Service Knowledge Management System (SKMS)
IT Service Management Vision & Mission
IT Service Management Strategies, Strategic Plan, Priorities & Policies
Service Portfolio, Service Catalogue, Service Models & Service Charters
IT Service Management Financial Budgets & Information
IT Service Management Processes, Procedures & Schedules
IT Service Management Performance Metrics, KPIs & CSFs Information
IT Service Management Actual Performance Information
Request for Change Register (RFC)
Strategic Risks
Service Design Packages, incl. Utility and Warranty Req’ts & Timescales
HW / SW Maintenance Requirements
Standard Changes for use in Request Fulfilment
Change Schedule
Customer & User Satisfaction Survey Results
Service Reports & Dashboards
Recovery Procedures
Vital Business Functions
New or changes Services
Known Errors
Input to Operational Testing
Inputs to Testing Requirements
ITIL Service Operation
Event management
Incident Management
Request Fulfilment
Problem Management
Access Management
Operating Risks
Feedback on quality of Transition Activities
Input to Operational Testing
Operational Performance Data & Service Records
Operating Cost Information (for TCO Calculations)
Operational Requirements
Input to Change Evaluation & CAB Meetings
Proposed Problem Resolutions & proactive Measures
IT Service Management Actual Performance Information
Request for Change Register (RFC)
Historical Incident Records
Continual Service Improvement Register
Components of the Service Knowledge Management System (SKMS)

Figure 3: Service Operation Overview

Service Operation describes the processes, functions, organization and tools used to underpin the ongoing activities required to deliver and support services and includes:

- Services
- Service Management processes
- Technology
- People

Effective communication are a key component in Service Operation and ensures that all teams and departments are able to execute the standard activities involved in delivering IT services and managing the IT infrastructure. Such communication will include:

- Routine operational communication
- Communication between shifts
- Performance reporting
- Communication in projects
- Communication related to changes
- Communication related to exception
- Communication related to emergencies
- Communication with users and customers.

Purpose and Objectives

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

Service Operation is a critical stage of the service lifecycle. Well planned and well implemented processes are to no avail if the day-to-day operation of those processes is not properly conducted, controlled and managed. Nor will service improvements be possible if day-to-day activities to monitor performance, assess metrics and gather operational data are not systematically conducted during service operation.

The objectives of service operation are to:

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

Service Operation Processes

The processes contained within the ITIL Service Operation lifecycle are:

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

Incident Management

Purpose and Objectives

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

The objectives of the incident management process are to:

- Ensure that standardized methods and procedures are used for efficient and prompt response, analysis, documentation, ongoing management and reporting of incidents
- Increase visibility and communication of incidents to business and IT support staff
- Enhance business perception of IT through use of a professional approach in quickly resolving and communicating incidents when they occur
- Align incident management activities and priorities with those of the business
- Maintain user satisfaction with the quality of IT services.

Process Activities

Key activities for incident management are:

- *Incident identification:* Incidents may be detected by event management, by calls to the service desk, from web or other self-help interfaces, or directly by technical staff.
- *Incident logging:* All incidents must be logged and time-stamped, regardless of how they are received. The log must include sufficient data to enable the incident to be managed.
- *Incident categorization:* Categories are used to identify the type of incident and to identify service requests so they can be passed to the request fulfilment process. Categories are also checked when the incident is closed.
- *Incident prioritization:* A priority code is assigned based on impact and urgency. Priorities are dynamic and may be changed during the life of the incident.
- *Initial diagnosis:* If possible, the incident should be resolved while the user is on the telephone. Sometimes the service desk analyst will continue to work on the incident and contact the user when it has been resolved.
- *Incident escalation:* ‘Functional escalation’ is transferring the incident to a technical team with a higher level of expertise; ‘hierarchic escalation’ is informing or involving more senior levels of management.

- *Investigation and diagnosis:* All actions taken by support groups should be recorded in the incident record.
- *Resolution and recovery:* The resolution must be fully tested and documented in the incident record, before the incident is passed back to the service desk for closure.
- *Incident closure:* Check and confirm the incident categories, carry out a user satisfaction survey, ensure all incident documentation is up to date, check to see if a problem record should be raised and then close the incident with the appropriate closure categorization.
- *Rules for reopening incidents:* Despite all adequate care, there will be occasions when incidents recur even though they have been formally closed. Because of such cases, it is wise to have predefined rules about if and when an incident can be reopened.

Triggers, Inputs and Outputs

Triggers

- A user calls the service desk or completes a web-based log of an incident
- An incident is automatically raised via event management tools
- Technical staff may notice potential failures and raise an incident
- Incidents may be raised at the request of suppliers.

Inputs

- Information about CIs and their status
- Information about known errors and workarounds
- Communication about incidents and their symptoms
- Communication about Requests for Change (RFCs) and releases
- Communication of events
- Operational and service level objectives
- Customer feedback
- Agreed criteria for prioritizing and escalating incidents.

Outputs

- Resolved incidents and resolution actions
- Updated incident management records
- Problem records
- Feedback on incidents related to changes and releases
- Identification of CIs associated with or impacted by incidents
- Satisfaction feedback.

Problem Management

Purpose and Objectives

The purpose of problem management is to manage problems through their lifecycle from first identification through investigation, documentation and eventual resolution and closure. Problem management seeks to minimize the adverse impact of incidents and problems on the business caused by underlying errors within the IT Infrastructure, and to proactively prevent recurrence of incidents related to these errors.

The objectives of the problem management process are to:

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

Process Activities

The key activities for problem management are:

- *Problem detection:* By the service desk, technical support, event management, notification by a supplier, or from incident trend analysis.

  Problem logging: All details must be recorded, including links to related incidents.

- *Problem categorization:* Usually uses the same categorization codes as incidents.
- *Problem prioritization:* Differs from incident prioritization in that this is based on frequency and impact of linked incidents, plus severity of the incident (impact on the infrastructure, cost to fix, time to fix).
- *Problem investigation and diagnosis:* Determine Root Cause using techniques such as chronological analysis, pain value analysis, Kepner-Tregoe, brainstorming, Ishikawa diagram and Pareto analysis.
- *Workarounds:* A workaround to the related incidents can reduce the impact of the problem until full resolution is achieved.
- *Raising a known error record:* For use by the service desk to identify the symptoms and restore service quickly, using the workaround if one exists. Create when diagnosis is complete, but can raise earlier if useful.

- *Problem resolution:* Usually requires a change request. If the resolution is not cost-effective, then the problem may be left open and the workaround should continue to be used.
- *Problem closure:* After the change has been successfully reviewed – review related incident records, update known error records, check problem data and formally close.
- *Major problem review:* A review of every major problem should be conducted to learn lessons for the future. Major problem is defined by the priority system.

Triggers, Inputs and Outputs

Triggers

- Reactive problem management
- One or more incidents via service desk staff
- Other problem records, and corresponding known error records, e.g. during testing
- Supplier's notification of potential faults or known deficiencies
- Proactive problem management
- Identification of patterns and trends of incidents
- Reviews of other sources, e.g. operation or event logs, operation communications.

Inputs

- Incident records
- Incident reports for proactive problem trending
- Information about CIs and their status
- Communication about RFCs and releases
- Communication of events
- Operational and service level objectives
- Customer feedback
- Agreed criteria for prioritizing and escalating problems
- Output from risk management and risk assessment activities..

Outputs

- Resolved problems and resolution actions
- Updated problem management records
- RFCs
- Workarounds for incidents
- Known error records
- Problem management reports
- Output and improvement recommendations from major problem reviews.

Event Management

Purpose and Objectives

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

Event management is therefore the basis for operational monitoring and control. If events are programmed to communicate operational information as well as warnings and exceptions, they can be used as a basis for automating many routine operations management activities.

The objectives of the event management process are to:

- Detect all changes of state that have significance for the management of a CI or IT service
- Determine the appropriate action for events and ensure communication to the appropriate functions
- Provide the trigger for the execution of many processes and operations management activities
- Provide comparison of actual operating performance against design standards and SLAs

Process Activities

The key activities for event management are:

- *Event occurs:* This event may not even be detected
- *Event notification:* Either the CI generates a notification or a management tool detects a status change by polling
- *Event detection:* By an agent running on the same system or a management tool
- *Event logged:* The event should be recorded together with any actions taken
- *First level event correlation and filtering:* To eliminate duplicates and unwanted events that cannot be disabled
- *Significance:* Events are categorized as informational, warning or exception

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

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

- Monitoring and control of the status of CIs
- Environmental conditions
- Software licence monitoring to ensure optimum/legal licence utilization and allocation
- Security
- Normal activity.

- *Second level event correlation and filtering:* Is normally performed by a ‘correlation engine’, usually part of a management tool that compares the event with a set of criteria and rules in a prescribed order. These are often referred to as business rules
- *Response selection:* All events are logged; other responses might include automated recovery, alert and human intervention, logging an incident problem or change
- *Review actions:* To check that significant events have been handled correctly
- Close event.

Triggers, Inputs and Outputs

Triggers

- Exceptions to any level of CI performance defined in the design specifications, OLAs or standard operating procedures (SOPs)
- Exceptions to an automated procedure or process
- An exception within a business process monitored by event management
- Completion of an automated task or job
- A status change in a server or database CI
- Access of an application or database by a user or automated procedure or job
- A predefined threshold is reached, e.g. by a device, database or application.

Inputs

- Operational and service level requirements (SLRs) associated with events
- Alarms, alerts and thresholds for recognizing events
- Event correlation tables, rules, event codes and automated response solutions
- Roles and responsibilities for recognizing and communicating events
- Operational procedures for recognizing, logging, escalating and communicating events.

Outputs

- Events communications and escalations
- Event logs
- Events that indicate an incident has occurred
- Events that indicate the potential breach of an SLA or OLA objective
- Events and alerts that indicate completion status of deployment, operational or other support activities
- Populated service knowledge management system (SKMS) with event information and history.

Request Fulfilment

Purpose and Objectives

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

The objectives of the request fulfilment process are to:

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

Process Activities

The key activities for request fulfilment are:

- *Receive request:* Fulfilment of service request should not start until a formalized request has been received, normally by the service desk
- *Request logging and validation:* All requests must be logged with the appropriate information and initially validated
- *Request categorization:* Should involve allocating a suitable request categorization coding
- *Request prioritization:* Involves the allocation of an appropriate priority to the request
- *Request authorization:* No work should take place until the request has been properly authorized

- *Request review:* Determines the function and need for the request is valid
- *Request model execution:* Required activities and work flows are executed to fulfil the request
- *Request closure:* Once completed the request should be closed
- *Rules for reopening requests:* Predefined rules should exist for deciding when a closed service request can be reopened.

Triggers, Inputs and Outputs

Triggers

- Typically via a user calling the service desk or a user completing self-help web-based request form.

Inputs

- Work requests
- Authorization forms
- Service requests
- RFCs
- Requests from various sources such as phone calls, web interfaces or email
- Request for information.

Outputs

- Authorized/rejected service requests
- Request fulfilment status reports
- Fulfilled service requests
- Incidents (rerouted)
- RFCs/standard changes
- Asset/CI updates
- Updated request records
- Closed service requests
- Cancelled service requests.

Access Management

Purpose and Objectives

1The purpose of access management is to provide the right for users to be able to use a service or group of services. It is therefore the execution of policies and actions defined in ISM.

The objectives of the access management process are to:

- Manage access to services based on policies and actions defined by ISM
- Efficiently respond to requests for granting access to services, changing access rights or restricting access, ensuring that the rights being provided or changed are properly granted
- Oversee access to services and ensure rights being provided are not improperly used.

Process Activities

The key activities in access management are:

- *Requesting access:* This may come from a human resources system, an RFC, a service request or by executing a pre-authorized script or option from a staging server. The rules for requesting access are normally documented in the service catalogue.
- *Verification:* Ensures that the user requesting access is who they say they are, and that they have a legitimate requirement. Usually requires independent verification.
- *Providing rights:* Access management does not decide who has access; it executes policies and regulations defined during service strategy and design. It also manages requests for exceptions. Access management often sends requests to supporting teams to actually make the changes; where possible the granting of rights should be automated.
- *Monitoring identity status:* Management of role changes due to job changes, promotions, transfers, resignation, death, retirement etc. The typical user lifecycle needs to be documented with tools to support the management of these changes.

- *Logging and tracking access:* Access monitoring and control needs to be included in all service operation functions. Exceptions are handled by incident management, ideally using incident models. A record of access may be needed for use in forensic investigations; this is normally provided by operations management staff, but is part of the access management process.
- *Removing or restricting rights:* Access management is responsible for reducing and removing access rights, as well as providing them. Rights may need to be removed after death, resignation, dismissal or transfer to a different area; rights may be restricted if the user is under investigation (but still needs some services), when the user has changed roles and needs different access, or when the user is away on a temporary basis.

Triggers, Inputs and Outputs

Triggers

- An RFC
- A service request
- A request from human resources
- A request from a manager.

Inputs

- Information security policies
- Operational and SLRs for granting access to services, performing access management administrative activities and responding to access management related events
- Authorized RFCs to access rights
- Authorized requests to grant or terminate access rights.

Outputs

- Provision of access to IT services in accordance with information security policies
- Access management records and history of access granted to services
- Access management records and history where access was denied and the reasons for denial
- Timely communications concerning inappropriate access or abuse of services.

David Jones and **Roderick Brown**

David Jones is a Senior Consultant with Enterprise Architects in Australia, specializing in Enterprise Architecture, particularly Business Architecture. He is also an experienced practitioner in business process improvement and simplification. David has worked with many sector clients, undertaking assignments in Financial Services, Telecommunications and Power Utilities.

Roderick Brown is a freelance Consultant working in Melbourne, Australia, specializing in Business Architecture, particularly in Process Architecture. He is also an experienced practitioner in business process improvement and simplification. Roderick has worked with many sector clients, undertaking assignments in Banking, Investment Management and Wealth Management.

David and Roderick are passionate about helping organizations understand and document their own business processes, using frameworks such as APQC's Process Classification Framework and standards such as BPMN as well as applying simple approaches to improve and simplify these business processes.

Orbus Software
3rd Floor
111 Buckingham Palace Road
London
SW1W 0SR
United Kingdom

+44 (0) 870 991 1851
enquiries@orbussoftware.com
www.orbussoftware.com