White Paper

Enterprise Architecture and ITIL®: Implementing Service Operation

WP0119 | November 2013

Trevor Lea-Cox

Trevor Lea-Cox has over 30 years experience in senior Information, Systems and Technology Management and CEO roles. He is a past Group-level CIO and director.

In this time he has developed and implemented Information, Systems and Technology strategies and business automation programmes for a wide variety of large and small organizations, including companies and groups of companies. A special focus has been the introduction of new Products and Services using lean and agile techniques and subsequently scaling up, including in the contexts of major business change and joint ventures.

In the previous paper "Enterprise Architecture and ITIL®[1]: Implementing Service Transition" we looked at some of the more important concepts in Service Transition (ST). Then we looked at a brief summary of each of the ITIL® Service Transition processes[2] and concluded with a small example applied to an EA[3] department to illustrate the principles.

In summary, Service Transition establishes a consistent approach to transitioning new and upgraded IT Services into Service Operation, including the decommissioning of old IT Services.

In this respect, a key focus is managing the changes to IT Services and their components efficiently, especially where some of these components may be shared with other services or if the changes made are likely to affect related services or their components. But the ST processes also ensure that the risk of making changes is managed, that new releases of IT Services meet customer expectations and that the IT Services do deliver the business value desired.

---

[1] ITIL® is a registered trade mark of AXELOS Limited. (Formerly, ITIL® and IT Infrastructure Library® were Registered Trade Marks of the Cabinet Office of the Government of the United Kingdom).

[2] Please note, a list of the ITIL® processes by each stage of the ITIL® Service Lifecycle is given in Appendix A.

[3] Please note, a list of the acronyms used in this paper and their meaning is given in Appendix B.

In particular, we saw how the Service Transition Plan is used to coordinate the production of a new release of an IT Service and subsequently also its deployment, evaluation and support through its "early life".

In this paper on Service Operation (SO), we will:

- Review (briefly) some important principles used in ITIL® for managing the operation of IT Services.
- Summarise the main ITIL® processes for managing Service Operation and the key IT Operations functions that support them.
- Then show how these principles would be applied to the "EA Publishing Service".

Contents

Service Operation Highlights

The comments in this section are restricted mostly to the content of the introductory ITIL® book "Introduction to the ITIL® Service Lifecycle: 2011 edition"[4]. The main Service Operation book "ITIL® Service Operation, 2011 edition"[5] contains a lot more information.

Introduction to Service Operation

Each of the preceding Service Management stages contributes to the identification and development of good quality IT Services for your organization, but it is only in Service Operation that all this effort is put to the test and IT Services are delivered to Customers to create value. The fundamental importance of Service Operation is that poor service delivery can so easily undermine otherwise very good quality services, but good service delivery can often make up for otherwise imperfect or less up-to-date IT Services and the inevitable interruptions to services by unexpected events. Good quality IT Services including good service delivery is our goal here.

The main purpose of Service Operation is to coordinate and carry out the activities required to manage and deliver IT Services to customers and users and to meet agreed services levels.

The main objectives of Service Operation are:

- To maintain business satisfaction and confidence in IT through the delivery of good quality IT Services.
- To minimize the impact of service outages on day-to-day business activities and in doing so, ensure IT Services are available at agreed times.
- To ensure access to IT Services is provided only to those people authorised to access and receive these services.

Service Operation not only ensures that "Business as Usual" operations are conducted and managed on an effective basis but it fulfils one other crucially important role, that of the collection of IT Service performance data and using this data for the daily monitoring and reporting of the performance of IT Services. Furthermore this role extends beyond the IT Services provided by the organization to those supporting services provided by third-party Service Providers. All service providers in the "service chain" must be able to deliver adequate service levels!

---

[4] Published by "The Stationery Office", ISBN 9780113313099. It is widely available, including from several on-line websites.

[5] Published by "The Stationery Office", ISBN 9780113313068.

The scope of Service Operation

One frequently asked question is; what is the scope of Service Operation? It is a good question and often one not easily answered. However in summary, SO covers the following areas:

- The IT Services that need to be delivered
- The ITIL® SO processes. The following are the SO processes in ITIL®:
  - Event Management
  - Incident Management
  - Request Fulfilment
  - Problem Management
  - Access Management.

However it is important to remember that some ITIL® processes from other Service Lifecycle stages such as Change and Configuration Management are also used in SO.

- The Technology Infrastructure. All IT Services require technology to enable them to be supported and delivered. Managing this technology is not a separate issue but an integral part of these IT Services. As we will see, SO in particular is dependent on a number of supporting operating functions in this respect.
- Finally SO is primarily about People; the people who help to deliver the IT Services as well as the people requesting and benefiting from these IT Services. It is important that Service Operations staff are perceived as well-trained Service Delivery teams[6].

The scope of IT Service Operations is summarised in *Figure 1*.

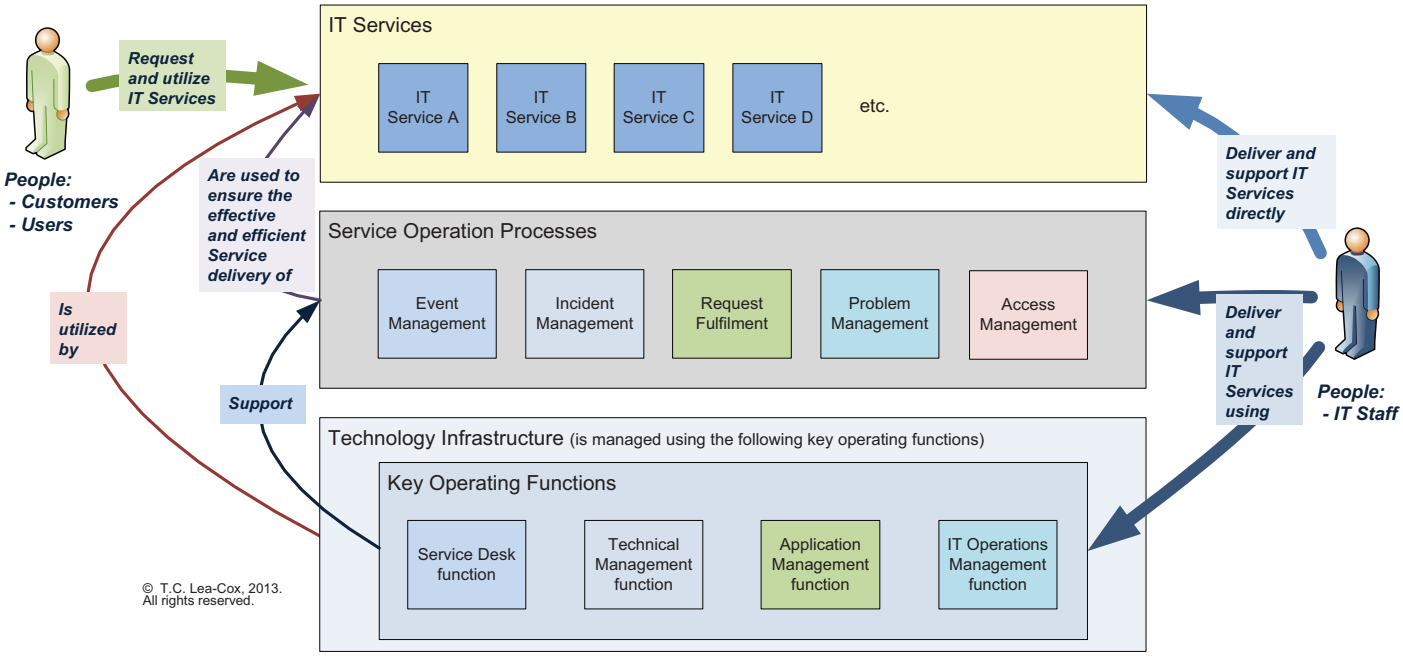

Figure 1: The scope of Service Operation

[6] The Introductory book ITIL® does not say much on the importance and involvement of "People". There is a lot more in the main ITIL® Service Operation book on this subject, especially on roles and responsibilities and the organization of Service Operation.

In this diagram, People (Customers and Users) request and utilise IT Services. The Technology Infrastructure is utilised to deliver these IT Services and is managed by a number of key operating functions. These operating functions support the SO Processes to ensure the IT Services are delivered on an efficient and effective basis. But ultimately again it is People (IT Staff) that deliver and support the IT Services, both directly and through the SO Processes and the key operating functions managing the technology.

Key Service Operation Principles

Service Operations are in the best overall position to monitor the "health" of the organization's IT Services and their components and to alert Service Management when something is not performing adequately. This leads to three important principles:

- Actively manage the health of IT Services
- Regularly assess and mitigate the risks, especially technical risks, that threaten the adequate performance of IT Services
- Monitor and report the performance and condition of IT Services on a continual basis.

The Health of IT Services

An important outcome of Service Management is to have healthy functioning IT Services over their entire lifetimes. The health analogy is a good one for IT Services; for like an organism, a service has a number of "vital signs" that provide an immediate measure of its condition. These vital signs need to be monitored continually to ensure they are within the normal range expected for the service. If they are, then the IT Service can be considered healthy and that it does not require any further attention. (We will consider below in Monitoring and Control what happens when they are out of the expected range).

The key implication here is that it is not necessary to monitor every component of an IT Service all the time to ensure it is functioning well. Measures of performance (KPIs) and measures of quality and condition are not equal in this respect. Some are leading indicators and some are not. Here we are primarily interested in those measures that reflect the "vital signs" of an IT Service. However, because different measures provide different information, we will use other measures not considered as vital to investigate and understand what is going on when an IT Service does not perform as expected. In fact, as with living organisms it is important to periodically do more comprehensive checks to help identify emerging problems and trends in performance.

In my own opinion, getting this area right by balancing the need for monitoring and control activity against the reactive effort required to

manage and resolve incidents and problems (to meet agreed service levels) is a critical component of managing operating workloads and controlling operating costs.

Assessing Operating Risks

Much of the operating risk faced by Service Operation emanates from changes to Services and their underlying components, especially in the technology used. But there are other significant sources of risk, particularly from changes in the business environment in which the IT Services operate and from changes that do not take place in the supporting technology resulting in "legacy" infrastructure. As budgets are constantly under pressure the latter is easily ignored and consequently, often results in a crisis response when the technology is proven as no longer fit for purpose as the breaking point has been breached.

As a result it is important that general operating risk assessments are done on a regular basis. These will often be annually but there is good reason to do more focused risk assessments for specific IT Services or their components if the indicators imply that this is required.

Monitoring and control

"Measurement and control of IT Services is based on a continual cycle of monitoring, reporting and subsequent action. This cycle is … fundamental to the delivery, support and improvement of services"[7]. It is in this respect that Service Operation fulfils one of its most important roles; to measure and report on all the operating indicators deemed necessary for each IT Service.

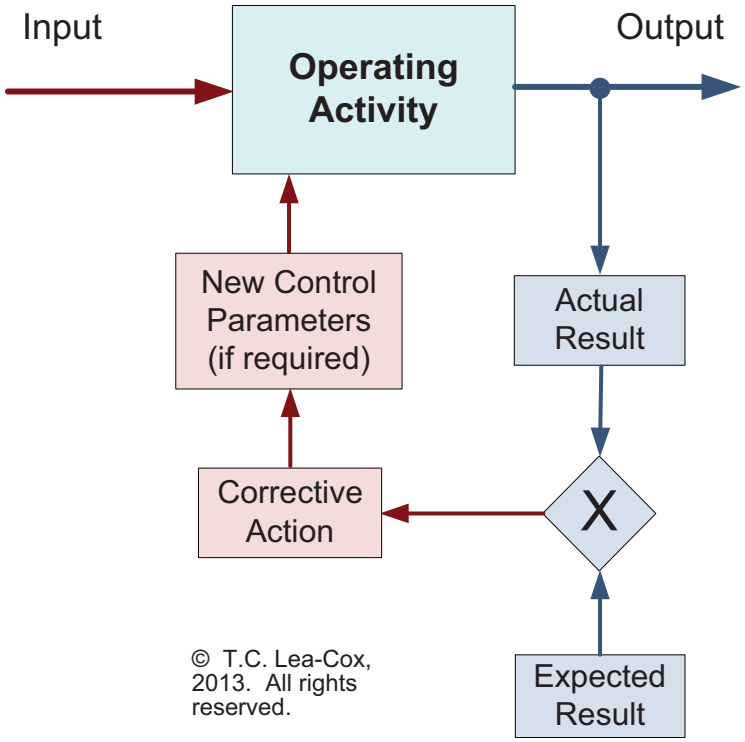

Figure 2: Operations monitoring control loop

From this you will infer correctly that service monitoring and control is not purely an operating matter. Service managers and designers also need to be involved, not only in identifying and developing appropriate indicators for each IT Service, but often also in the interpretation of the results[8].

At the heart of the monitoring and control is a very simple concept.

[7] "Introduction to the ITIL® Service Lifecycle: 2011 edition", page 127.

[8] In fact, all stages of managing the Service Lifecycle should ensure that appropriate measures and controls are identified, implemented and the results acted upon.

The output from a single activity is measured and the result is compared to a pre-defined norm or standard to determine if this result is within an acceptable range of performance or quality. If it is within range no action is required. If it is out of range then corrective action may be required. We will discuss this further under Event Management.

This is known as a "Control Loop". Typically there are two types of control loop:

- Open loop systems, designed to perform a specific activity independent of the environmental conditions, for example, performing a data backup.
- Closed loop systems, designed to respond to changes in the environment. In this situation, the monitoring system provides feedback to the control system which then regulates the control variables, for example, in a load-balancing system.

ITIL® Processes for managing Service Operation[9]

Event Management

Key Objective of the Process:
To ensure relevant IT Services and their components are constantly monitored, to filter and categorize events and to decide any control action required.

Additional Notes:
The main purpose of Event Management is to manage operating events through their lifecycle, especially detection, analysis and determining what control action is required, if any. In this respect Event Management also provides a substantial basis for operating management and control.

Event Management exploits the operations monitoring control loop and uses the concepts established by Shewhart[10] to identify:

- Output that is within the expected range of values for the technological component (or Configuration Item) being monitored. These result in event values that are "informational" only. The Configuration Item (CI) concerned can be considered as operating normally.
- Output that is beyond the expected range of values but not seriously so. These are warnings that something may be wrong. Further analysis is usually required to determine whether or not this warning should be considered an Incident requiring resolution.

---

[9] A significant additional source of information for this section is the "IT Process Maps GbR", which includes the set of ITIL® process maps provided by Orbus Software.

[10] For more information, see http://en.wikipedia.org/wiki/Control_chart

- Output that is beyond the expected range of values and seriously so. These are alerts and they require an immediate response. These are Incidents and will be recorded and in and resolved using the Incident Management processes. They often also indicate an underlying problem that needs to be resolved.

Figure 3 shows an example of a Shewhart Control Chart to illustrate the decision-making that is often done automatically by monitoring software.

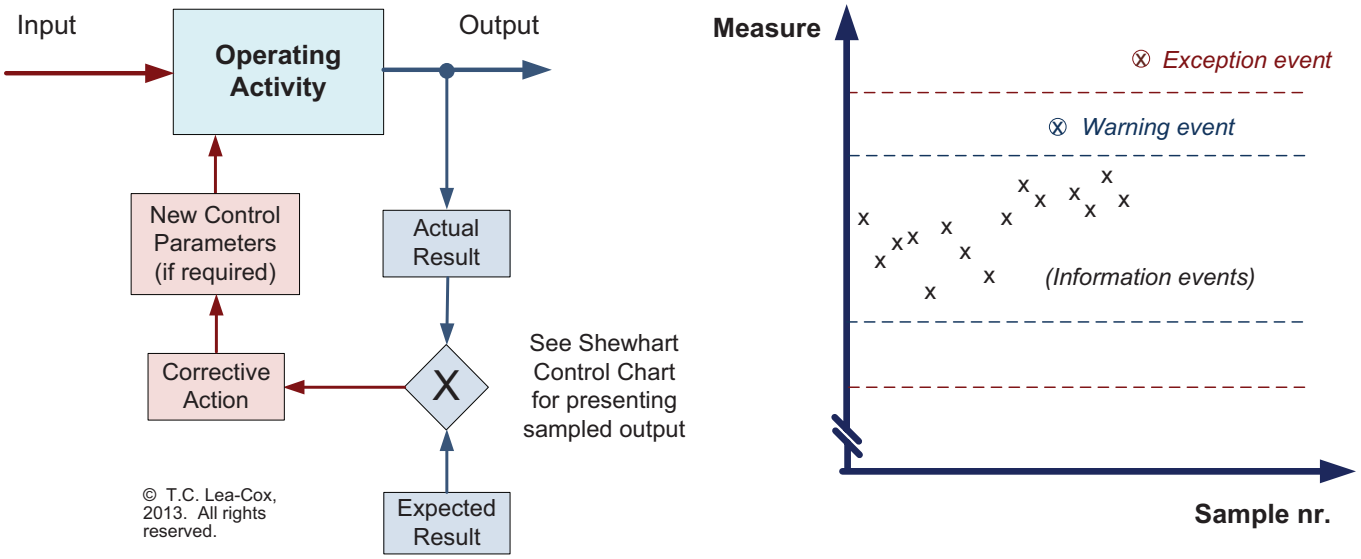

Figure 3: Shewhart Control Charts

If an automated control system is used to manage the CI concerned, the control system will use much of this output to take decisions automatically and to adjust the control parameters to regulate the CI.

Overall Approach:

- Maintain Event monitoring mechanisms and rules.
- Perform Event filtering and first level "correlation"[11].
- Perform second level correlation (if the event is significant) and select a response.
- Implement the response.
- Close the Event and Review as required.

Incident Management

Key Objective of the Process:
To manage all Incidents over their lifecycle and to return disrupted IT Services to full (normal) operation as quickly as possible.

Additional Notes:
Together with Problem Management, Incident Management makes a major contribution to helping minimize unplanned operating workloads

[11] ITIL® uses the word "correlation" although this is not always correlation in the statistical sense.

and stabilising IT Operations. To understand how let us start by looking at the ITIL® definition of an Incident.

The ITIL® Definition of an Incident
An Incident is an unplanned interruption to an IT Service or reduction in the quality of an IT Service. The failure of a component of an IT Service (Configuration Item) is also an Incident, even if the failure has not yet affected the IT Service.

In other words an Incident includes any event which disrupts an IT Service or could disrupt an IT Service and they include events observed and reported by people as well as those reported by automatic monitoring tools.

An important implication of this definition is that an Incident needs to be recorded as affecting one or more Configuration Items (CIs) in the Configuration Management Database (CMDB).

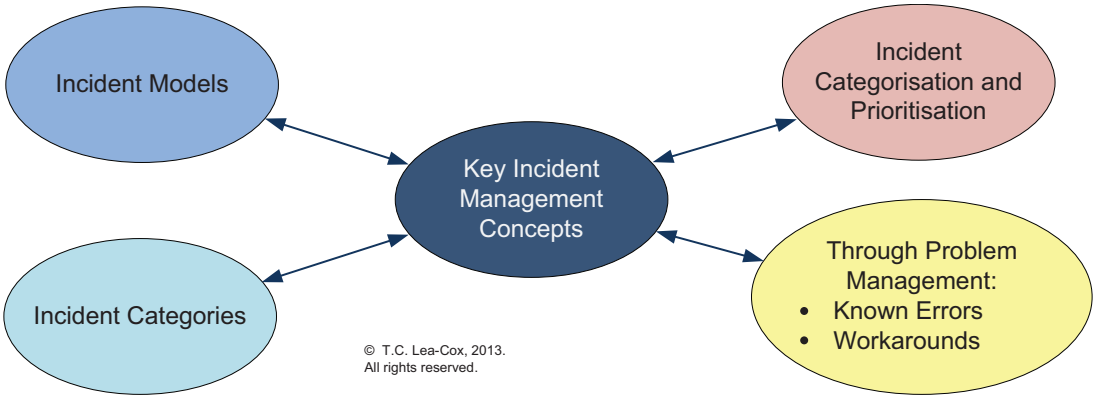

Figure 4: Important concepts used in Incident Management

Incident Categories
In any organization there will be a wide variety of Incidents; from failing disks and lost communications to human error and system “bugs”. To help make some sense of what is happening and later, to help identify the underlying problems causing these Incidents, we categorize recorded Incidents. Identifying the Incident Categories required is not always easy and the categories are likely to evolve over time, especially as new technology is introduced and old technology is removed.

Incident Models
Incident Models pre-define the steps that need to be taken to manage the resolution of specific types (categories) of Incidents. They can also give guidance on timescales required to complete tasks or thresholds for these tasks, communication and escalation procedures and what needs to be done to preserve the evidence of the incident. As these models are often applied to more than one IT Service, they will need to refer to the specific operating information required for the IT Service(s) affected by an Incident. Although this information typically comes from the Service Catalogue, sometimes it is useful to have the Operations part of the

Service Catalogue effectively contain (or refer to) a separate document which contains all the important support information required by SO[12].

Incident Models are useful, not just as guidance but because they often highlight how to improve and even automate the Incident resolution process.

Incident Categorisation and Prioritization
A key part of the process to resolve Incidents is Incident categorisation and prioritization.

By categorising Incidents, especially when they are first recorded, we are able to identify if there is a corresponding Incident Model that we can use to help resolve the Incident as quickly as possible. But Incident categorisation also helps us to identify related Incidents; especially those reported recently that might have the same underlying root cause. Later, the frequency of Incidents in various categories is important input information for Problem Management.

Incident Prioritization is important, especially when the Incident is first reported, because it determines the speed of response required, especially to limit the actual and potential damage done to the organization. Incident Priority is normally calculated by understanding:

- **The Impact of the Incident** on one or more IT Services. The scale of this impact is often, but not always, based on the number of Customers and Users affected by the Incident.
- **The Urgency for Resolution** which is usually based on the actual and potential damage to the organization by the incident and hence how quickly the organization needs resolution.

Overall Approach:

- Provide Incident Management support
- Log and categorize Incidents
- Provide immediate Incident resolution by First Level Support
- Provide Incident resolution by Second and subsequent levels of support
- Manage Major Incidents
- Monitor and escalate Incidents
- Proactively provide information to customers and users
- Close and evaluate Incidents
- Provide Incident Management reports.

[12] I like to think of this document as a "Service Operation Package" for the IT Service, although this is not ITIL® terminology. More will be said about this document later in the EA Publishing Service example.

Request Fulfilment

Key Objective of the Process:
To fulfil Service Requests. In other words, to manage each Service Request over its lifecycle.

Additional Notes:
The ITIL® Definition of a Service Request

A Service Request is a formal request from a user for something to be provided.

"Service Request" is a generic term for all types of tasks requested by customers and users to be performed directly by the IT organization. These are usually a request to perform non-routine tasks, even requests for information. They are not the same as Incidents in that they do not disrupt existing IT Services and no damage is done to the organization. It is important to manage them because they too have a big impact on the workload for IT Operations. Request Fulfilment subsequently provides another very important source of information for managing this workload effectively.

It is useful to look at the key objectives of Request Fulfilment, namely:

- To maintain customer and user satisfaction by providing a professional response to Service Requests
- To provide a single channel for all Service Requests
- To provide IT Service information to customers and users, especially about the availability and procedures for requesting IT Services
- To provide information for improving the management of Service Requests.

From these we can deduce some of the more important benefits of Request Fulfilment:

- Provide quick and easy access to IT Services
- Reduce the bureaucracy in requesting and receiving IT Services (and the cost)
- Increase the level of control over IT Services requested.

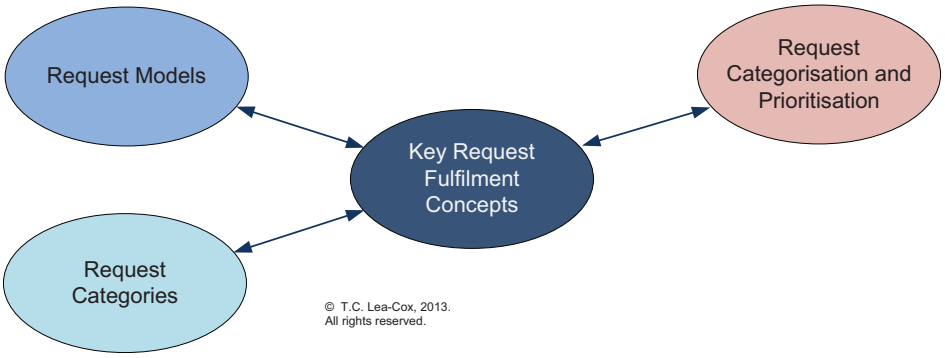

Figure 5: Important concepts used in Request Fulfilment

Request Models
Request Models are very similar in concept to Incident Models but for Service Requests.

Request Categorisation and Prioritization
Categorisation and Prioritization are similar in principle to Incident Management. However, it is likely that there will be some different categories and there may be different prioritization rules.

Overall Approach:

- Provide Request Fulfilment management support
- Log, categorize and prioritize Service Requests
- Fulfil a Service Request (using an appropriate Service Request Model)
- Close and evaluate Service Requests
- Monitor and escalate Service Requests as required
- Provide Request Fulfilment management reports.

Problem Management

Key Objective of the Process:
To manage the lifecycle of all Problems. Also to prevent Incidents from happening and to minimize the impact of Incidents that cannot be prevented.

Additional Notes:
The ITIL® Definition of a Problem

A cause of one or more Incidents.

Note the causal relationship with Incidents and that an Incident may have more than one cause and hence, related Problem.

In essence, Problem Management aims to minimize the impact of underlying errors and defects in the IT Service Infrastructure by:

- Diagnosing and identifying the root cause of Incidents logged
- Documenting and communicating the details of known errors and defects (referred to collectively as “Known Errors”)
- Providing temporary fixes or “Workarounds” to remedy Known Errors until they can be removed from the IT Service Infrastructure
- Then initiating action to improve or correct the faulty infrastructure.

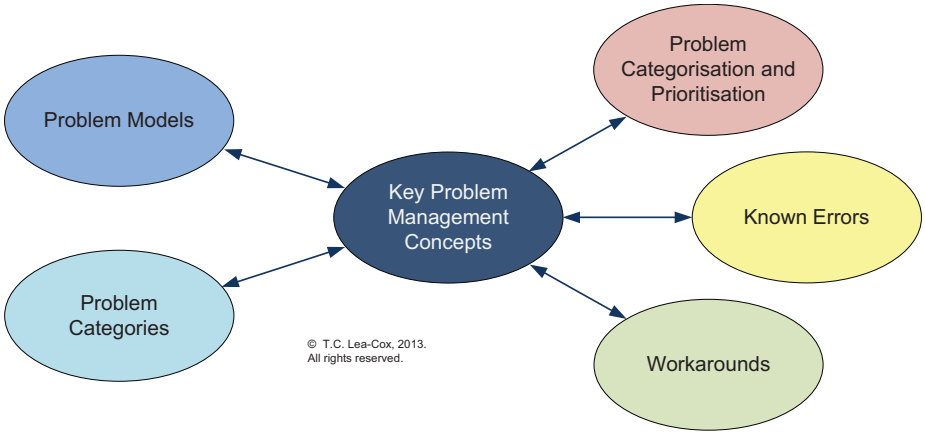

Figure 6: Important concepts used in Problem Management

Problem Categories

Incident and Problem Management are closely related so it is highly likely that they will be most effective if they use similar categorisation and prioritization coding structures.

Problem Models

Different types of Problems require different approaches to help identify and remove their root causes. Problem Models help to establish efficient and coordinated approaches to do so for similar categories of Problems.

Known Errors

When the root cause of a Problem cannot be resolved immediately, a Known Error is created in the Known Error Database (KEDB), together with details of any Workarounds identified. The KEDB is an important facility used by Incident Management to help resolve Incidents expeditiously.

Workarounds

A Workaround is a temporary resolution to a Known Error implemented to restore an IT Service quickly for its users. The most important thing to remember is that when the root cause is removed, some (types of) Workarounds also have to be reversed.

Proactive Problem Management

There are two types of Problem Management; Reactive and Proactive.

- Reactive Problem Management responds to triggers from Incident Management.
- Proactive Problem Management is triggered by activities seeking to improve IT Services using tools such as Trend Analysis and Correlation.

Overall Approach:

- Provide Problem Management support
- Proactively identify Problems
- Categorize and prioritize Problems
- Diagnose and resolve Problems
- Monitor and escalate Problems
- Close and evaluate Problems
- Perform Major Problem Reviews when required
- Provide Problem Management reports.

Access Management

Key Objective of the Process:
To grant authorised users the right to use an IT Service whilst preventing access to users that are not authorised.

Additional Notes:
Access Management effectively implements the policies of Information Security Management (that help to manage the confidentiality, availability and integrity of the organization's data and information). In doing so, Access Management ensure that staff have controlled access to IT Services and ensures compliance with regulatory and legislative requirements, contracts and approved standards.

Access Management usually uses role-based techniques to control access. These make it easy to assign or withdraw security profiles to individual or groups of users. But it is important to remember that there are two key verification perspectives to every access rights request:

- Check the user requesting new or changed access rights are who they say they are
- Check that the user has a legitimate requirement for access to an IT Service or system.

Overall Approach:

- Provide Access Rights management support
- Maintain a catalogue of user roles, user groups and access profiles.
- Process user access rights requests
- Provide Access Rights Management reports (to authorised managers).

Service Operation Functions

Earlier we saw that the Technology Infrastructure used to deliver IT Services is managed by a number of key operating functions, namely:

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

These operating functions support and use the SO Processes to ensure the IT Services are delivered on an efficient and effective basis. This section will summarise the contribution of these functions.

Service Desk Function

The Service Desk is the primary interface with, and often the single point of contact for, IT Service customers and users. It communicates with them using a variety of media but typically these are e-mail, telephone (including Voice over Data), text messages and through the organization's website. In some companies, social media provides another important channel for communications.

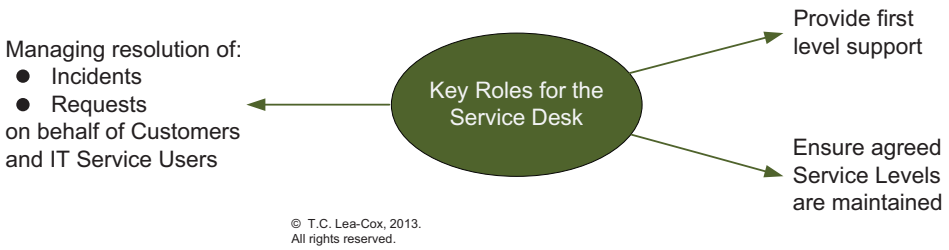

Figure 7: Important Roles of the Service Desk

The Service Desk handles a wide variety of tasks, mainly the management of:

- Incidents
- Requests
- Asset and configuration updates (usually these are approved, standard changes for customers and users)
- Monitoring and expediting outstanding issues on behalf of customers and users.

The number, type, size and location of the Service Desks depend on a number of key factors, typically:

- The complexity of IT Services and the (IS and) IT Infrastructures.
- The timing and size of the demand for IT Services provided by the Service Desk
- The level of knowledge of Service Desk operators.

Managing the staffing and performance of a Service Desk can be very challenging. Not only can demand be volatile and relatively unpredictable, but the content of the job can become very repetitive and / or stressful. Monitoring workload statistics for the Service Desk and corresponding user and customer satisfaction is a prerequisite to getting this situation right.

An effective Service Desk is very valuable as it can compensate for deficiencies elsewhere in the organization. But a poor Service Desk creates a poor impression of what may otherwise be a very effective IT organization.

Technical Management Function

These are the groups, departments or teams that provide the knowledge and technical expertise to manage and maintain the IT Infrastructure. It is not normally provided by a single department or group as each IT organization usually will have a number of areas of technology that require specific skills to manage and operate the technology. For example;

- Server Team
- Desktop team
- Storage team
- Networking team
- Virtualization team
- Database team
- Middleware team
- Directory Services team
- Messaging team

And more!

Figure 8: Important Roles of the Technical Management Function

These teams have an important dual role:

- To be the custodian of the technical knowledge and expertise for the area of technology for which they are responsible and to ensure this technical knowledge and expertise is developed further and maintained.
- To provide the skilled resources required by the organization to manage, develop and operate their area of the technology.

Application Management Function

Application Management are responsible for managing applications throughout their lifecycle. Note that this is not the same as Application Development as it addresses the whole life of an application, including requirements specification, design, development and testing, operations, maintenance and support and decommissioning at the end of its life.

Application Management is to the Information Systems infrastructure, what Technical Management is to the IT infrastructure, whether an application is purchased or developed in-house.

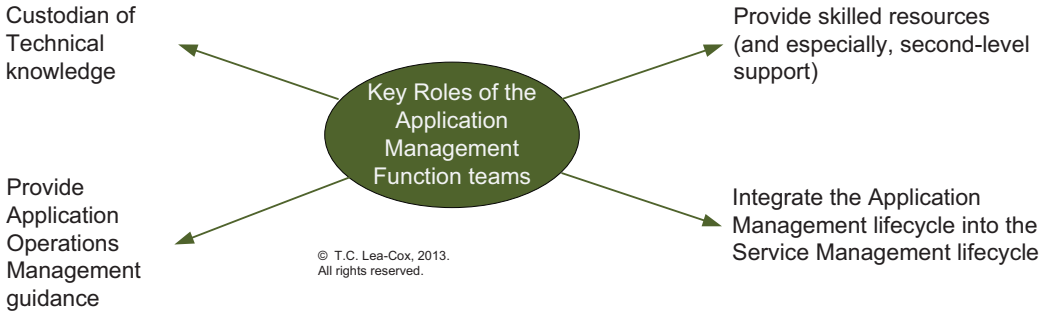

Figure 9: Important Roles of the Application Management Function

Like Technical Management, Application Management is custodian of the knowledge and expertise required to manage, develop and integrate applications for the organization and they also to provide the actual resources to do this. A key objective in this respect is to balance the skills required against the cost of these resources. But they have two further specific roles:

- To provide the guidance to IT Operations about how to manage the applications from an operating perspective
- To manage the integration of the Application Management lifecycle into the Service Management lifecycle.

IT Operations Management Function

The IT Operations function are the groups, departments or teams of people responsible for the day-to-day operations activities, comparable to running a production line in a manufacturing environment. They perform the work required to deliver the organization's IT Services, including the day-to-day running of the IT Infrastructure to ensure that IT Services are delivered to meet agreed service levels.

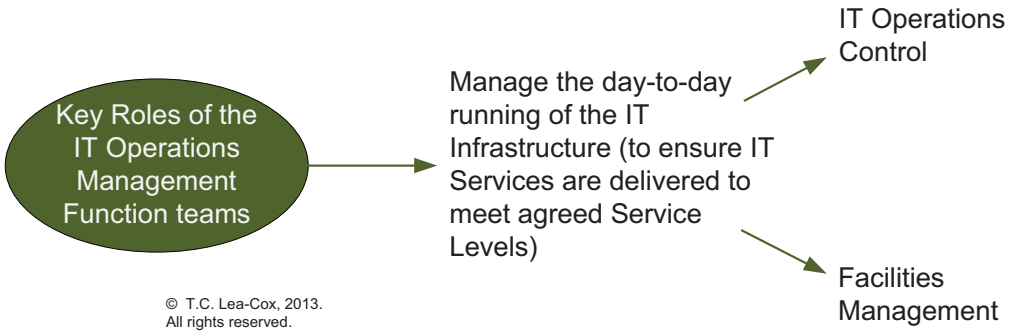

Figure 10: Important Roles of the IT Operations Management Function

These activities fall into two main categories:

IT Operations Control which oversees the performance and monitoring of operational activities and the events in the IT Infrastructure often achieved using an "Operations Bridge" or "Operations Centre". In addition to the executing routine tasks in all the technical areas, IT Operations Control also performs the following:

- Defining and implementing central observation and monitoring consoles and then using these consoles to manage operating events.
- Job scheduling
- "Batch" tasks such as backing up and restoring the organization's data and information.
- Managing shared and centralized technology.

Facilities Management:

- This is the management of the physical environments for IT, usually data centres and operations rooms requiring special equipment for, for example, power, air conditioning, fire protection and physical access security.
- They will also manage any facilities, for example a data centre that has been outsourced.

Applying Service Operation principles to a small EA department

Enterprise Architecture Publishing Service (EA Publishing Service)

In Service Strategy we identified two services that would help to meet the requirements of the department's customers and we selected the EA Publishing Service to expand as an example. Now we will review the impact of the SO processes on our EA Publishing Service.

Some catching up in the context of Service Operation

We also learned in Service Strategy that our organization has implemented the following SO processes:

- Request Fulfilment
- Incident Management
- Problem Management.

In other words these processes need to be updated formally to account for our new EA Publishing Service.

Now that we have covered the key components of SO, again we have some catching up to do. The first area is to clarify the Operating Functions in our organization. Even though they may not be formalized in the way explained in ITIL®, it is certain that the following functions will be present in some form:

- Technology Management
- Applications Management
- IT Operations Management.

It is also likely it will have an IT Service Desk, especially if Request Fulfilment, Incident and Problem Management have been established and we will assume as much.

Many of the actual changes made during Release and Deployment Management in Service Transition will have been made, or at least coordinated by the Technology, Application and IT Operations Management teams. In fact, because our EA Publishing Service will largely use the existing IT systems and infrastructure, most of the changes will have happened at the application systems level and to manual procedures.

The Service Catalogue would have been updated at this stage too showing the EA Publishing Service first as “ready for deployment” and then as “in service”. The main implication of this is that it is now a formally managed IT Service within SO.

We can also explain better the operating aspect of “Measurements, Metrics and Methods” in Service Design. Much of the information for the EA Publishing Service will be collected by the application systems used, for example, the number of times a specific diagram (page) is accessed (used) on the intranet. However, some event-based information may also need to be collected, for example, any attempts to access confidential diagrams by unauthorised users. To do this the intranet system may have to be updated to provide a warning or an alert when this happens. However, note that many of the more common alerts and warnings required will be produced from monitoring software already used by IT Operations, for example, for monitoring disk and network usage.

You may have noticed in Service Transition that there was a lot of activity in the Service Asset and Configuration Management process. Some of the more important of these activities were:

- Maintaining the Configuration Management System (CMS) as the EA Publishing Service components were built and added.
- Updating the Configuration Model (for any new types of Configuration Items added). For example, Architecture Views and Diagrams may not have previously been part of the Configuration Model.
- Establishing new Configuration standards and controls required.
- Baselining newly released components of the EA Publishing Service and adding these to the Definitive Media Library where appropriate to do so.

All the service components and the information about them in the CMS will subsequently be used in SO.

In broader terms in Knowledge Management, all the information derived during mainly Service Design and Transition, about for example;

- Roles and responsibilities (cf. RACI diagrams)
- Operating standards and controls required
- Operating procedures
- Service Architecture

needs to be documented, stored and made available to those involved in the operation of the EA Publishing Service. This documentation will be used mainly to train new staff, investigate problems and assess EA Publishing Service performance and to help improve service quality[13].

Event Management

Event Management is not formally managed in our example organization. Nevertheless it is an important process area and it is likely that some events pertaining to our EA Publishing Service are already monitored within the current technology environment, for example, disk usage and network usage.

However, it is likely with any new IT Service that new events will need to be logged and monitored. For example, in our EA Publishing Service, details of the usage of the architecture diagrams will need to be logged and monitored. The sort of information that might be logged is for example:

- Date and time of access request
- Id of the diagram requested
- Id of the user requesting access
- Whether the access was successful or not and if not, the reason.

[13] This is effectively the "Service Operation Package" for the EA Publishing Service, which is part of the Service Catalogue.

Facilities to log this sort of information may already be available in the organization's Intranet system as this type of requirement is common. If it is not, submit a change request (RFC) requesting and justifying a system upgrade.

Figure 11 summarises the most important information input to and output from Event Management:

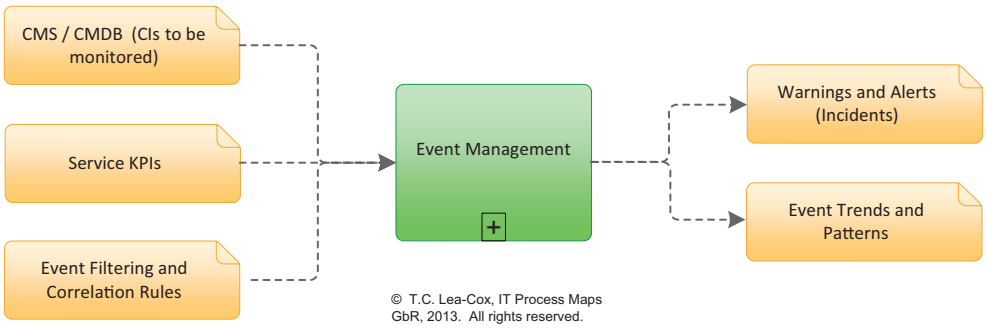

Figure 11: Key Information input into and output from Event Management

Incident Management

Incident Management is being managed on a formal basis. As a result we have a number of actions to set up the Incident Management system to help manage our EA Publishing Service. As one might expect, having a system available to do this makes the process relatively easy once the system has been set up.

Earlier we mentioned a number of "key concepts". These (amongst other requirements depending on the sophistication of your Service Management System) determine the key input required to set up the Incident Management system for use in SO.

For example:

- Incident Categories: Update the Incident Categories to provide one or more categories for EA Publishing Service Incidents. For example:
  - EA Directory-related incidents
  - EA Diagram-related incidents.
- Incident Model: We are likely to be able to use an existing (or standard) Incident Model for our EA Publishing Service. The "EA Publishing Service Operations Package" will contain all the key information required by IT Operations, including the Service Desk, to incorporate the EA Publishing Service into the existing Incident Model.

- Incident Prioritization and Escalation rules: As the EA Publishing Service is not exceptional, it is likely that the organization's generic SLA / OLA terms will be sufficient. In other words we can use the standard prioritization and escalation rules already established within the Incident Management system.
- Known Errors and Workarounds: If any known errors exist for the EA Publishing Service then the KEDB will be updated together with a corresponding Workaround if one is known and available.
- Key Contact Information: Naturally, a further important category of information to the Incident Management system is the contact information required in the event of an Incident (from the Service Operations Package). Normally this information will be used to complete the tasks defined in the Incident Model.

Once IT Service Continuity is established, there is an important additional component to add as input to Incident Management which is one or more major incident response or recovery plans, or in ITIL®, an "IT Service Continuity Plan" for the EA Publishing Service. In practice, this is such an important issue in many organizations that even if there is no formal requirement, it is prudent to establish such plans when Incident Management is formalized, especially when a new IT Service is introduced. These plans describe what needs to be done and by whom in the event of a major incident so that the IT Service is restored as quickly as possible for its customers and users. They will also make provision for emergency access to key architectural diagrams during a technology failure (or "outage"). If this is a requirement and it has not been done previously, we would prepare a (general) Major Incident Recovery Plan or IT Service Continuity Plan for the EA Publishing Service now.

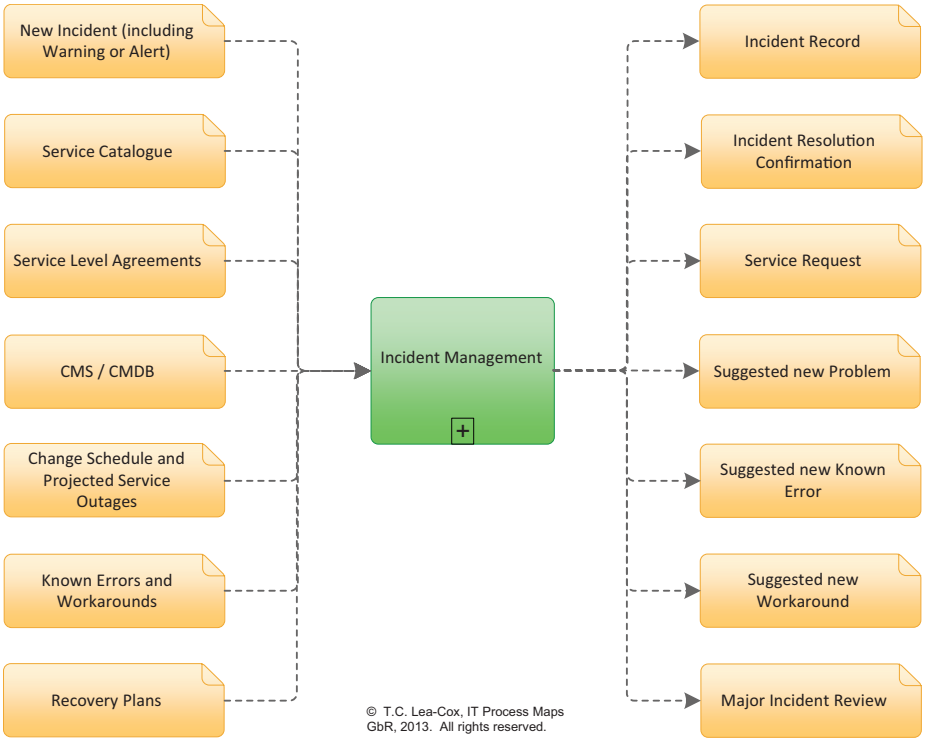

Figure 12: Key Information input into and output from Incident Management

Note also that as Service Asset and Configuration Management and Change Management are also formally managed process areas, there are some important inputs from these processes into Incident Management, for example:

- The CMS to look up which CIs are affected by the Incident and their current status.
- The Change Schedule
- The Projected Service Outages report.
- However, all of these are likely to have been set up already for Incident Management in the organization.

Request Fulfilment

Request Fulfilment is also being managed on a formal basis in our organization and once again as there is likely to be a system that has been established for managing Requests, configuring the system for the EA Publishing Service will be easy.

The key concepts for Request Fulfilment once again indicate key input requirements to set up the system for use in SO:

- Request Categories: Update the Request Categories to provide one or more categories for the EA Publishing Service. There are several different types of requests possible for our EA Publishing Service which will determine the Request Categories required, for example:
  - A "New User" Request to access the EA Publishing Service
  - A Request to access a new Architecture Domain or View
  - A Request to update a set of diagrams on the Intranet.
- Request Model: We are likely to be able to use a standard Request Model for our EA Publishing Service. Once again the "EA Publishing Service Operations Package" will provide the key information required to complete the specific information required for this model, including the key contact information.
- Request Prioritization and Escalation rules: Once again it is highly likely that we can use the standard prioritization and escalation rules already established within the Request Fulfilment system.

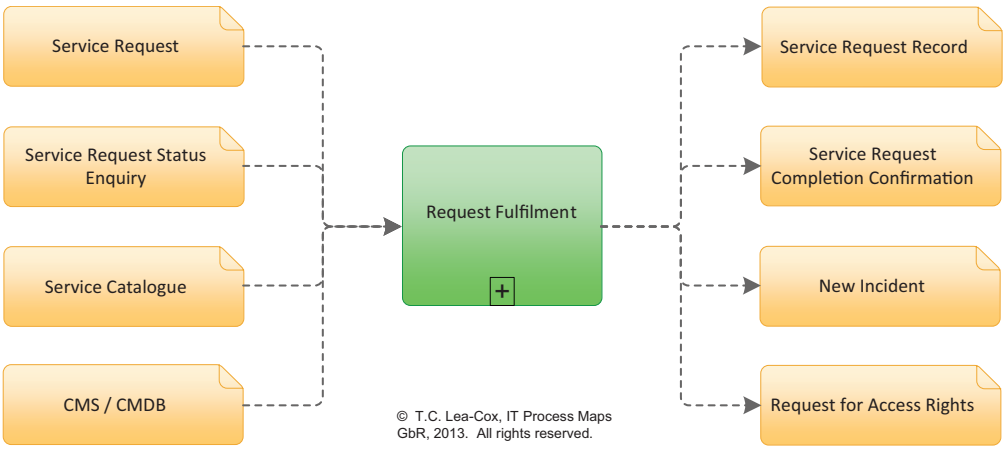

Figure 13: Key Information input into and output from Request Fulfilment

Problem Management

As Problem Management is also formally managed, one of the first things to note is that certain output from Incident Management is important input for Problem Management and that this will be automatically set up if the systems to automate these areas come from the same family of systems. Examples of these inputs from Incident Management are:

- Suggested new Problems
- Suggested new Known Errors
- Suggested new Workarounds.

Other key types of information required to set up Problem Management to include our EA Publishing Service are:

- Problem Categories: The same categories as used for Incident Management are likely to be used for Problem Management. In other words, the following categories need to be added:
  - EA Directory-related problems
  - EA Diagram-related problems.
- Problem Model: Although a standard Problem Model is likely to apply to the EA Publishing Service and much of the information for this required will come from the "EA Publishing Service Operations Package", in practice most of the information required to resolve problems will come from the most up-to-date status information about our EA Publishing Service, especially from the CMS, the Event Management logs and details of changes recently made.
- Problem Prioritization and Escalation rules: Problem prioritization and escalation rules will be driven by those in Incident Management, especially when there is no adequate workaround to resolve an Incident (or set of related incidents). If there is an adequate workaround established, prioritization and escalation will be driven more by commercial expediency.
- Known Errors and Workarounds: If any known errors exist for the EA Publishing Service then the KEDB will be updated together with a corresponding Workaround if one is known and available. Problem Management staff are responsible for validating any new entries in this respect.

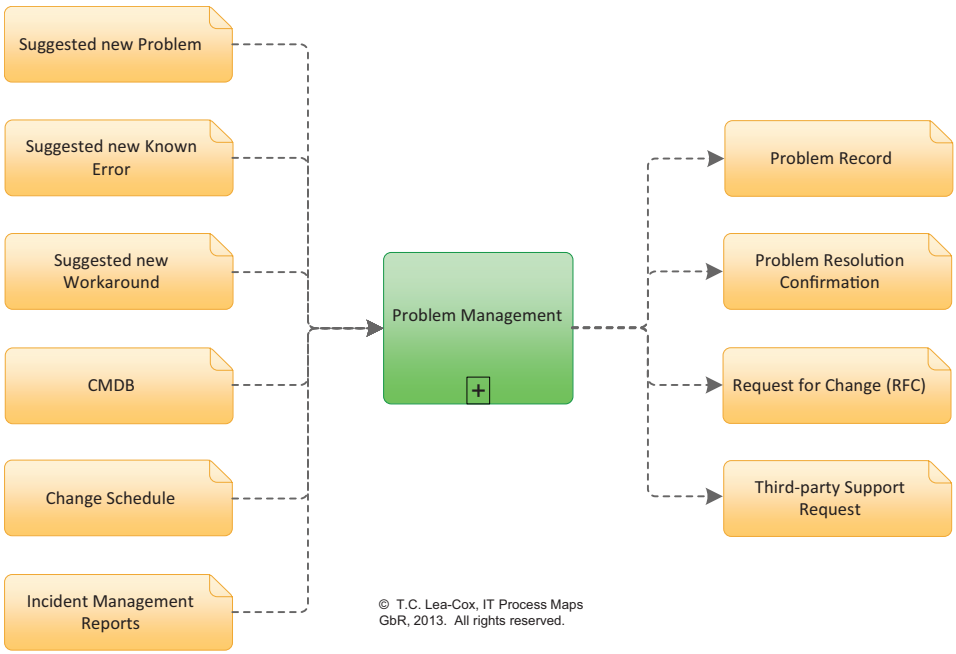

Figure 14: Key Information input into and output from Problem Management

Access Management

Access Management has not been formally established in our example organization. However, it is likely that:

- The EA Management system will have access security implemented.
- The Intranet (including the Content Management System and / or Document Management system behind the Intranet, if any) will have access security implemented.

If this is the case, the information for updating the access security in these systems will come from the "EA Publishing Service Operation Package" but they will have to be updated and maintained independently. Subsequently, a number of checks need to be identified and implemented to ensure that any updates to access security are synchronised correctly across all systems involved.

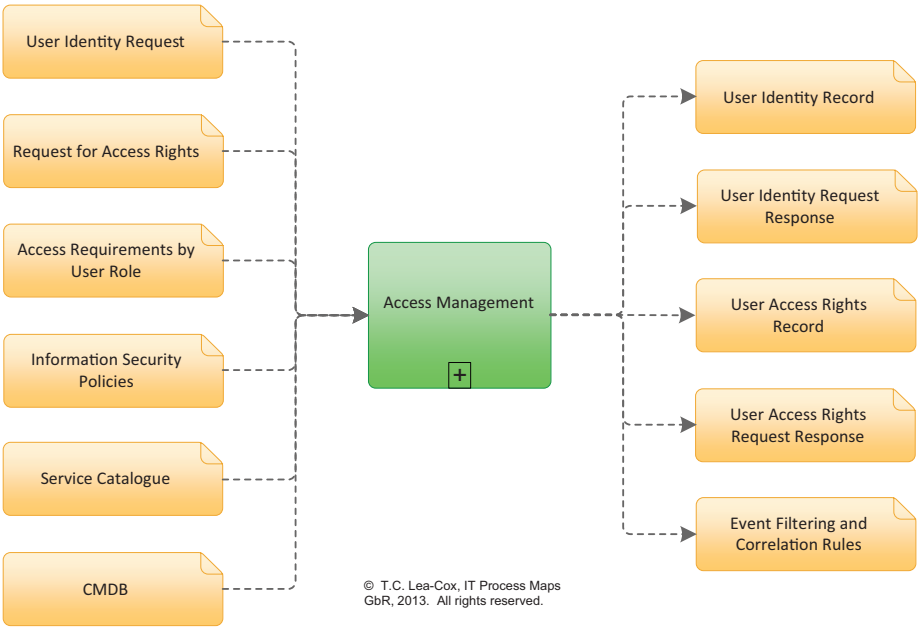

Figure 15: Key Information input into and output from Access Management

Key IT Operating Functions

Apart from the SO processes, the introduction of the EA Publishing Service potentially affects the key IT Operating Functions, especially the Service Desk and the IT Operations Management functions.

Service Desk:
The Service Desk team will need to be briefed (and where appropriate, trained) on the new EA Publishing Service, especially:

- Its function and business context
- Requests that can be expected and how to manage them
- Scripts on how to identify EA Publishing Service Incidents and how to process these Incidents
- Contact details for key customers, users and support staff.

This information should be available in the EA Publishing Service Operating Package.

IT Operations Management Function:
The most important tasks of IT Operations Management are:

- To perform the routine and non-routine tasks that ensure the EA Publishing Service meets agreed service levels. Note that the Architecture Administrators would be considered part of the IT Operations in this respect; in other words, part of the EA Publishing Service team.
- To collect information on the usage and performance of the EA Publishing Service and to report this to IT Management. Although these tasks are relatively standard, they need to be built into the EA Publishing Service standard operating procedures.
- All IT Operations staff involved in the EA Publishing Service need to be briefed and where appropriate, trained, not only when the EA Publishing Service goes live, but subsequently whenever there is a change of staff.

In Conclusion

Service Operation is where an IT Service is delivered and value is created for its customers and users. We have explored briefly how the IT Operations function uses the Service Operation processes to manage IT Services and ensure that they meet agreed service levels.

However, the business context for IT Services frequently changes and hence their value deteriorates. The final Service Management stage, Continual Service Improvement, highlights the main processes and techniques that are require to continually improve the quality and performance of IT Services. This is the subject of the next and final white paper in this series.

Appendix A: Summary of the Processes at each ITIL® Service Lifecycle Stage

ITIL® Service Lifecycle Stage	ITIL® Process
Service Strategy	Strategy Management for IT Services Service Portfolio Management Financial Management for IT Services Demand Management Business Relationship Management
Service Design	Design Coordination Service Catalogue Management Service Level Management Availability Management Capacity Management IT Service Continuity Management Information Security Management Supplier Management
Service Transition	Transition Planning and Support Change Management Service Asset and Configuration Management Release and Deployment Management Service Validation and Testing Change Evaluation Knowledge Management
Service Operation	Event Management Incident Management Request Fulfilment Problem Management Access Management
Continual Service Improvement	Seven-step Improvement Process

Appendix B: Summary of acronyms used and their meaning

Acronym used	Meaning
CI	Configuration Item
CIO	Chief Information Officer
CMDB	Configuration Management Database
CMS	Configuration Management System
COTS	Commercial, Off-the Shelf (usually applied to information systems)
DML	Definitive Media Library
EA	Enterprise Architecture
IT	Information Technology
ITIL®	IT Infrastructure Library
ITSCM	IT Service Continuity Management
IS	Information Systems
KPI	Key Performance Indicator
KEDB	Known Error Database
LAN	Local Area Network
OLA	Operating Level Agreement
PAAS	Platform as a Service
PIR	Post Implementation Management
RFC	Request for Change
SAAS	Software as a Service
SACM	Service Asset and Configuration Management
Scrum	Scrum is not an acronym but the name given to an agile software development method.
SD	Service Design
SDP	Service Design Package
SKMS	Service Knowledge Management System
SLA	Service Level Agreement
SM	Service Management
SMS	Service Management System
SS	Service Strategy
ST	Service Transition
SOA	Service Oriented Architecture
TOGAF	The Open Group Architecture Framework
VM	Virtual Machine
WOA	Web Oriented Architecture

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

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

orbus software