The strategies and content in this book are a result of experience and understanding of ITIL® and the refresh of ITIL in July 2011. The evolution of the core principles and practices provided by the framework provides the more holistic guidance needed for an industry that continues to mature and develop at a rapid pace. We recognize, however, that many organizations and individuals who had previously struggled with their adoption of the framework will continue to find challenges in implementing ITIL as part of their approach for governance of IT Service Management practices.

This workbook’s primary purpose is to complement the accredited ITIL Service Operation Program. This book is not a replacement for completing the course.

Each process contains a summarized overview of key knowledge. These overviews are designed to help you to reference the knowledge gained through the course.

We hope you find this book to be a useful tool in your educational library and wish you well in your IT Service Management career.

ITIL® is a registered trade mark of AXELOS Limited, used under permission of AXELOS Limited. All rights reserved.
IT Infrastructure Library® is a registered trade mark of AXELOS Limited, used under permission of AXELOS Limited. All rights reserved.
Notice of Rights

All rights reserved. No part of this book may be reproduced or transmitted in any form by any means, electronic, mechanical, photocopying, recording, or otherwise without the prior written permission of the publisher.

Notice of Liability

The information in this book is distributed on an “As Is” basis without warranty. While every precaution has been taken in the preparation of the book, neither the author nor the publisher shall have any liability to any person or entity with respect to any loss or damage caused or alleged to be caused directly or indirectly by the instructions contained in this book or by the products described in it.

Trademarks

Many of the designations used by manufacturers and sellers to distinguish their products are claimed as trademarks. Where those designations appear in this book, and the publisher was aware of a trademark claim, the designations appear as requested by the owner of the trademark. All other product names and services identified throughout this book are used in editorial fashion only and for the benefit of such companies with no intention of infringement of the trademark. No such use, or the use of any trade name, is intended to convey endorsement or other affiliation with this book.
<table>
<thead>
<tr>
<th>Section</th>
<th>Title</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.1.4</td>
<td>Policies, Principles, and Basic Concepts</td>
<td>97</td>
</tr>
<tr>
<td>10.1.5</td>
<td>Designing for Event Management</td>
<td>99</td>
</tr>
<tr>
<td>10.1.6</td>
<td>Elearning Module 6 &amp; Workbook Review Questions</td>
<td>102</td>
</tr>
<tr>
<td>10.1.7</td>
<td>Process Activities</td>
<td>105</td>
</tr>
<tr>
<td>10.1.8</td>
<td>Triggers, Inputs, and Outputs</td>
<td>107</td>
</tr>
<tr>
<td>10.1.9</td>
<td>Critical Success Factors and Key Performance Indicators</td>
<td>109</td>
</tr>
<tr>
<td>10.1.10</td>
<td>Challenges and Risks</td>
<td>110</td>
</tr>
<tr>
<td>10.1.11</td>
<td>Elearning Module 7 &amp; Workbook Review Questions</td>
<td>111</td>
</tr>
<tr>
<td>10.2</td>
<td>Incident Management</td>
<td>113</td>
</tr>
<tr>
<td>10.2.1</td>
<td>Purpose and Objectives</td>
<td>113</td>
</tr>
<tr>
<td>10.2.2</td>
<td>Scope</td>
<td>114</td>
</tr>
<tr>
<td>10.2.3</td>
<td>Value to Business</td>
<td>115</td>
</tr>
<tr>
<td>10.2.4</td>
<td>Policies, Principles, and Basic Concepts</td>
<td>115</td>
</tr>
<tr>
<td>10.2.5</td>
<td>Elearning Module 8 &amp; Workbook Review Questions</td>
<td>120</td>
</tr>
<tr>
<td>10.2.6</td>
<td>Process Activities</td>
<td>122</td>
</tr>
<tr>
<td>10.2.7</td>
<td>Triggers, Inputs, and Outputs</td>
<td>123</td>
</tr>
<tr>
<td>10.2.8</td>
<td>Critical Success Factors and Key Performance Indicators</td>
<td>125</td>
</tr>
<tr>
<td>10.2.9</td>
<td>Challenges and Risks</td>
<td>126</td>
</tr>
<tr>
<td>10.2.10</td>
<td>Elearning Module 9 &amp; Workbook Review Questions</td>
<td>127</td>
</tr>
</tbody>
</table>
10.4.8  Critical Success Factors and Key Performance Indicators 154

10.4.9  Challenges and Risks 155

10.4.10  Elearning Module 13 & Workbook Review Questions 157

10.5  Access Management 159

10.5.1  Purpose and Objectives 159

10.5.2  Scope 159

10.5.3  Value to Business 160

10.5.4  Policies, Principles, and Basic Concepts 160

10.5.5  Elearning Module 14 & Workbook Review Questions 162

10.5.6  Process Activities 164

10.5.7  Triggers, Inputs, and Outputs 165

10.5.8  Critical Success Factors and Key Performance Indicators 166

10.5.9  Challenges and Risks 167

10.5.10  Elearning Module 15 & Workbook Review Questions 168

11  Service Operation Activities 170

11.1  Monitoring and Control 173

11.1.1  Monitor Control Loop 175

11.1.2  Monitoring Strategies 177

11.1.3  Measurements and Reporting 179
11.1.4 Testing and Audits

11.2 IT Operations
11.2.1 Console Management
11.2.2 Job Scheduling
11.2.3 Backup and Restore
11.2.5 Server and Mainframe Management
11.2.6 Network Management
11.2.7 Storage and Archive
11.2.8 Database Administration
11.2.9 Directory Services Management
11.2.10 Desktop and Mobile Device Support
11.2.11 Middleware Management
11.2.12 Internet Management
11.2.13 Facilities and Data Center Management

11.3 Support from other Lifecycle Stages
11.3.1 Demand Management
11.3.2 Financial Management for IT Services
11.3.3 Capacity Management
11.3.4 Availability Management
11.3.5 IT Service Continuity Management 201
11.3.6 Change Management 201
11.3.7 Release and Deployment Management 204
11.3.8 Service Asset and Configuration Management 206
11.3.9 Knowledge Management 207
11.3.10 Information Security Management 209
11.4 Improving Service Operations 209
11.5 Elearning Module 16 & Workbook Review Questions 210

12 Organizing for Service Operations 213

12.1 Functions 213
12.2 The Service Desk 214
12.2.1 Service Desk Organizational Structures 216
12.2.2 Specialized Service Desk Groups 219
12.2.3 Elearning Module 17 & Workbook Review Questions 221
12.2.4 Service Desk Staffing 223
12.2.5 Measuring Service Desk Performance 225
12.2.6 Customer/User Satisfaction Surveys 226
12.2.7 Elearning Module 18 & Workbook Review Questions 230
12.2.8 Outsourcing the Service Desk 232
<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.2.9 Elearning Module 19 &amp; Workbook Review Questions</td>
<td>233</td>
</tr>
<tr>
<td>12.3 Technical Management</td>
<td>234</td>
</tr>
<tr>
<td>12.3.1 Technical Management Activities</td>
<td>235</td>
</tr>
<tr>
<td>12.3.2 Measuring Technical Management Performance</td>
<td>237</td>
</tr>
<tr>
<td>12.3.3 Elearning Module 20 &amp; Workbook Review Questions</td>
<td>238</td>
</tr>
<tr>
<td>12.4 IT Operations Management</td>
<td>239</td>
</tr>
<tr>
<td>12.4.1 Measuring IT Operations</td>
<td>240</td>
</tr>
<tr>
<td>12.4.2 Elearning Module 21 &amp; Workbook Review Questions</td>
<td>241</td>
</tr>
<tr>
<td>12.5 Application Management</td>
<td>242</td>
</tr>
<tr>
<td>12.5.1 Application Management Lifecycle</td>
<td>244</td>
</tr>
<tr>
<td>12.5.2 Application Management Generic Activities</td>
<td>248</td>
</tr>
<tr>
<td>12.5.3 Measuring Application Management</td>
<td>250</td>
</tr>
<tr>
<td>12.5.4 Elearning Module 22 &amp; Workbook Review Questions</td>
<td>251</td>
</tr>
<tr>
<td>12.6 Organizational Development</td>
<td>252</td>
</tr>
<tr>
<td>12.6.1 Stages of Organizational Development</td>
<td>252</td>
</tr>
<tr>
<td>12.7 Roles and Responsibilities</td>
<td>257</td>
</tr>
<tr>
<td>12.7.1 Service Owner</td>
<td>257</td>
</tr>
<tr>
<td>12.7.2 Process Owner</td>
<td>259</td>
</tr>
<tr>
<td>Section</td>
<td>Page</td>
</tr>
<tr>
<td>------------------------------------------------------------------------</td>
<td>------</td>
</tr>
<tr>
<td>14.4 Operational Support in Other Lifecycle Stages</td>
<td>287</td>
</tr>
<tr>
<td>14.5 Service Management Technologies</td>
<td>288</td>
</tr>
<tr>
<td>14.6 Elearning Module 25 &amp; Workbook Review Questions</td>
<td>289</td>
</tr>
<tr>
<td>15 Challenges, Critical Success Factors, and Risks</td>
<td>290</td>
</tr>
<tr>
<td>15.1 Challenges for Service Operation</td>
<td>290</td>
</tr>
<tr>
<td>15.2 Risks of Service Operation</td>
<td>291</td>
</tr>
<tr>
<td>15.3 Critical Success Factors in Service Operation</td>
<td>292</td>
</tr>
<tr>
<td>16 Answers to Elearning Module &amp; Workbook Review Questions</td>
<td>293</td>
</tr>
<tr>
<td>17 Glossary</td>
<td>296</td>
</tr>
<tr>
<td>18 References</td>
<td>309</td>
</tr>
<tr>
<td>19 Index</td>
<td>310</td>
</tr>
</tbody>
</table>
As this ITIL Intermediate Workbook is designed to help you memorize and understand the official ITIL terminology, in addition to helping you to apply this theory in a practical scenario, many instances of formal definitions and terminology have been quoted from the official core publications.

All gray, italic texts are from the five ITIL official lifecycle books (SS, SD, ST, SO, CSI) Copyright © AXELOS Limited 2011. Reproduced under licence from AXELOS Limited. All rights reserved. ITALIC text is referenced to corresponding book and page number.

All other texts are based on AXELOS material. ITIL® is a registered trade mark of AXELOS Limited, used under permission of AXELOS Limited. All rights reserved.

IT Infrastructure Library® is a registered trade mark of AXELOS Limited, used under permission of AXELOS Limited. All rights reserved.
1 ITIL Certification Pathway

Since July 2007, a new certification path was also released. This new path encompasses all the new Programs, ending in the possible attainment of “Expert Status.” The figure below demonstrates the possible pathways that you could take to achieve the Expert status. The 2011 update to ITIL made no significant changes to the certification path.

To achieve Expert status, you are required to gain a minimum of 22 points by completing various ITIL programs:

- You must complete the Foundation Program (2 points).
- You must complete 15 credits minimum from the Foundation and Intermediate modules. (3–4 points for each module).
- Optional: qualifications from earlier versions of ITIL and complementary qualifications can also earn additional credits (0.5–3.5 points each).
- You must complete the Managing Across the Lifecycle Program (5 points).
- You must process a balanced knowledge base across the ITIL Service Lifecycle.
- (The numbers on each program indicate the point value.)

It is yet to be finalized how the “Advanced Level” can be achieved, but is expected to be based on demonstration of practical experience in ITIL and IT Service Management.
1.1 Exam Specifics

The ITIL Intermediate Qualification Service Operation exam has the following features:

- Multiple-choice exams.
- 90 minutes in length.
- 8 scenario-based questions.
- Passing mark is 70%.
- Closed book exam.
- Scaled Marking system:
  - Most correct answers – 5 marks.
  - Next – 3 marks.
  - Next – 1 mark.
  - 1 answer – 0 marks.

It is possible to do a paper- or a web-based exam. (Please check with your Accredited Examination Center for more information on this.)

1.2 Exam Prerequisites

In order to sit the ITIL Intermediate SO Exam, you MUST have an ITIL V3 or 2011 Foundation Certificate and completion of an accredited program from an ITIL Accredited Training Provider.
1.3 Exam Hints

When it comes time to sit your exam, you need to do this through an accredited Authorized Examination Center. You may have the option to do the exam as web- or paper-based. Either way, you will be given a paper copy of the Scenarios. A good thing! (Especially if you are doing web-based exam—do not waste time opening web versions of the scenario—use the paper ones.)

Do not be fooled by the “only 8 questions” concept. These questions are designed to test you—not only your knowledge, but also your understanding and application of the theory. You have 90 minutes, which means roughly 11 minutes per question. Most questions come with their own case study/scenario. You need to CAREFULLY read the scenario, then the question, then the scenario again.

There are 4 possible answers—1 is totally WRONG! And usually it is obvious to see which that is. If we do our math—you need 28/40 to pass. This means that if the answers are based on a 5/3/1/0 scale—you really cannot afford to get any 0 answers. You MUST get at least 2 × 5 mark answers and the remaining averaging 3s (to get minimum of 28). So you DO need to know your stuff.

THINK Business! Remember, as “Techies,” we tend to get caught up in “our” IT world. The ITIL lifecycle and, in particular, ITSM is customer-centric… THINK THIS WAY when answering questions!

Know your content—know your order. This study guide gives you a solid revision approach to this course—but does not cover ALL content (that’s why you do the course). Make sure you know what makes up a policy/plan and the activities for each process, as well as who does what.
Case Study Hints:

a. Identify main process/concept being tested.
b. Identify the “issue/problem” faced within the scenario—there will always be one—your role is to resolve that issue.
c. Once you have read the associated question, go back and identify/confirm that you are on the right track.

Question Hints:

• The 4 possible answers will appear to be similar—you need to read the possible answers carefully.
• Eliminate the most obvious “wrong answer.” Things to look for:
  o Order of activities.
  o Red herring activities.
  o Wrong processes.
  o Wrong description.
• From the remaining 3 responses, start to identify similarities/differences. This will help you to eliminate the next response generally. The differences will be a hint that one of them is incorrect—you have to decide which one.
• It is probable that the “most correct” response would have the correct order of activities/descriptions and “just that little bit more.”
• DO NOT assume that the longest response is the most correct one.
• Expect a “phase” question. While most questions are obvious with what it is testing for (i.e. process), you could expect to get a “big picture” question asking about Service Transition in general—so make sure you understand your related phases.
2 The Objective Tree

This Objective Tree is a very useful tool for understanding and “tunneling” down into how ITSM can contribute to achieving a corporate objective. This helps us to better understand how the Service Lifecycle can contribute to achieving the Business objectives.
The aim of the Objective Tree is to walk down the tree to understand **HOW** each level of the organization is assisted in achieving their objective by receiving support from the level below.

Once you get to the bottom, you then walk back up the tree, giving an example of **WHY** each would be of benefit to the one above in achieving its objectives.

ITIL contributes in the darker IT aspects in providing quality IT Service Management.

### 2.1 Study Notes

The following study notes are broken down into the following topics:

- Introduction to Service Operation.
- Service Operation Principles.
- Service Operation Processes.
- Managing Personnel.
- Organizing for Service Operation.
- Technology Considerations.
- Implementing Service Operation.
- Challenges, Critical Success Factors, and Risks.

Again, these study notes are not intended to replace an accredited ITIL Foundation or Intermediate Qualification Program. These notes are supplementary and may not include EVERY concept that may be tested.
3 Introduction

While often seen as a stepping stone into higher-level specialist roles in IT, operational support plays a critical part in the quality of IT services being delivered in any organization that is supported by technology. Many factors influence the success being experienced in operational support, including customer expectations, staff turnover, the relative age and complexity of the infrastructure, quality of communication, and knowledge sharing practices, as well as the overall quality of Service Management employed by the IT organization.

In light of this, this workbook aims to develop the reader’s knowledge and appreciation of the practices for IT Service Management with particular focus on those capabilities required for Service Operation (SO) in the modern IT environment. It also seeks to challenge some traditional thinking of the role of IT support, including the measurement of its success. Rather than focusing on a limited set of activities or Service Level Agreement (SLA) targets, organizations are now beginning to focus on the value provided by IT support, specifically its impact on user productivity and business-unit performance.

This comprehensive book is designed to complement the in-depth accredited ITIL Service Operation (SO) eLearning program and, together with your practical experience gained in the field, prepare you for the corresponding examination. Assumptions are made by the authors that readers already have some familiarity with IT and ITIL terminology and have already completed an ITIL Foundation program.
The term “IT Service Management” (ITSM) is used in many ways by different management frameworks and organizations seeking governance and increased maturity of their IT organization. Standard elements for most definitions of ITSM include:

- Description of the processes required to deliver and support IT services for customers.
- The purpose primarily being to deliver and support the technology or products needed by the business to meet key organizational objectives or goals.
- Definition of roles and responsibilities for the people involved including IT staff, customers, and other stakeholders.
- The management of external suppliers (partners) involved in the delivery and support of the technology and products being delivered and supported by IT.

The combination of these elements provides the capabilities required for an IT organization to deliver and support quality IT services that meet specific business needs and requirements.

The official ITIL definition of IT Service Management is found within the Service Design volume on page 16, describing ITSM as “the implementation and management of quality IT services that meet the needs of the business. IT Service Management is performed by IT service providers through an appropriate mix of people, process, and information technology.” These organizational capabilities are influenced by the needs and requirements of customers, the culture that exists within the service organization, and the intangible nature of the output and intermediate products of IT services.
However, IT Service Management comprises more than just these capabilities alone. It is being complemented by an industry of professional practice and wealth of knowledge, experience, and skills. The ITIL framework has developed as a major source of good practice in Service Management and is used by organizations worldwide to establish and improve their ITSM practices.

### 4.1 Benefits of ITSM

While the benefits of applying IT Service Management practices vary depending on the organization’s needs, some typical benefits include:

- Improved quality service provision.
- Cost-justifiable service quality.
- Services that meet business, customer, and user demands.
- Integrated centralized processes.
- Everyone knows their role and knows their responsibilities in service provision.
- Learning from previous experience.
- Demonstrable performance indicators.

It is important to consider the range of stakeholders who can benefit from improved ITSM practices. These stakeholders can come from:

- Senior management.
- Business unit managers.
- Customers.
- End users.
- IT staff.
- Suppliers.
4.2 Business and IT Alignments

A central concept to keep in mind when discussing the benefits of IT Service Management is the goal of business and IT alignment. When staff members of an IT organization have an internal focus on the technology being delivered and supported, they lose sight of the actual purpose and benefit that their efforts deliver to the business. A way in which to communicate how IT supports the business is using Figure 4.A (on page 27) that demonstrates business and IT alignment.

Figure 4.A divides an organization into a number of supporting layers that work toward meeting a number of organizational goals. These layers are communicated by the following:

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Organization</td>
<td>What are the key strategic goals and objectives for the organization? These objectives define who we are as an organization and where we want to be in the future.</td>
</tr>
<tr>
<td>CORE Business Processes</td>
<td>These are represented by the repeatable business activities that produce desirable results for the business. Without these results, the organizational objectives defined above would not be supported or achieved.</td>
</tr>
<tr>
<td>IT Service Organization</td>
<td>Defines the IT Services and supporting infrastructure that is required to enable the effective and efficient execution of the business processes above. IT Services are used by the business to facilitate and enhance outcomes, including improved efficiency of operations or ensuring accuracy in the records and information being managed.</td>
</tr>
<tr>
<td>Term</td>
<td>Definition</td>
</tr>
<tr>
<td>-------------------------------</td>
<td>----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>IT Service Management</td>
<td>Made up by the repeatable, managed, and controlled processes used by the IT department that enable quality and efficiency in the delivery and support of the IT Services above.</td>
</tr>
<tr>
<td>IT Technical Activities</td>
<td>The actual technical activities required as part of the execution of the ITSM processes above. ITSM is utilized to ensure that any resources and effort spent performing the technical activities are optimized according to the greatest business need or reward. As these activities are technology specific (e.g. configuring application server), they will not be a focus of this book’s content.</td>
</tr>
</tbody>
</table>

Each layer within this structure is utilized to support the layer(s) above. At the same time, each layer will, in some way, influence the layer below it. For example, a business process that is required to be executed at all times without disruptions (e.g. emergency health services) would result in highly resilient IT services—being implemented and supported by ITSM processes—that reduce the risk and impact of disruptions occurring.
**Example to illustrate business and IT alignment.**

Business: A fashion store.

What are some of your organization’s objectives or strategic goals?

- We want to make a lot of money $$$!
- We want to have a good image and reputation.
What business processes aide in achieving those objectives?

- Retail, marketing, buying, procurement, HR, etc.

What IT services are these business processes dependent on?

- Web site, email, automatic procurement system for buying products, Point of Sale Services.

We have ITSM in order to make sure that the IT services are:

- What we need (Service Level Management, Capacity Management, etc.).
- Available when we need it (Availability Mgt, Incident Mgt, etc.).
- Provisioned cost-effectively (Financial Mgt, Service Level Mgt).

If we do not manage the IT services appropriately, we cannot rely on these services to be available when we need them. If this occurs, we cannot adequately support our business processes effectively and efficiently. And, therefore, we cannot meet or support our overall organization’s objectives.
5 What is ITIL?

ITIL stands for the Information Technology Infrastructure Library. ITIL is the international *de facto* management framework describing best practices for IT Service Management. The ITIL framework evolved from the UK government’s efforts during the 1980s to document how successful organizations approached Service Management. By the early 1990s, they had produced a large collection of books documenting the best practices for IT Service Management. This library was eventually entitled the IT Infrastructure Library.

ITIL has gone through several evolutions and was most recently refreshed with the release of the 2011 edition. Through these evolutions, the scope of practices documented has increased in order to stay current with the continued maturity of the IT industry and meet the needs and requirements of the ITSM professional community.

ITIL is only one of many sources for best practices, including those documented by:

- Public frameworks (ITIL, COBIT, CMMI, etc.).
- Standards (ISO 20000, BS 15000).
- Proprietary knowledge of organizations and individuals.

Generally, best practices are those formalized as a result of being successful in wide-industry use.
Five volumes make up the IT Infrastructure Library:

- Service Strategy.
- Service Design.
- Service Transition.
- Service Operation.
- Continual Service Improvement.

Each volume provides the guidance necessary for an integrated approach and addresses the direct impact of capabilities on a service provider’s performance. The structure of the ITIL framework is that of the service lifecycle. It ensures organizations are able to leverage capabilities in one area for learning and improvements in others. The framework is used to provide structure, stability, and strength to Service Management capabilities with durable principles, methods, and tools. This enables service providers to protect investments and provide the necessary basis for measurement, learning, and improvement.
In addition to the core publications, there is also ITIL Complementary Guidance. This consists of a complementary set of publications with guidance specific to industry sectors, organization types, operating models, and technology architectures.
Critical to our ability to participate with and apply the concepts of the ITIL framework is the need to be able to speak a common language with other IT staff, customers, end users, and other involved stakeholders. This chapter documents the important common terminology that is used throughout the ITIL framework. Most of these concepts and terms will not be new to you, as you will be using them within your workplaces and/or remember them from your foundation level study. This chapter is provided to help you revise the key terms and refresh your memory of the definitions.

A full glossary has also been included at the back of this book for terminology and acronyms that are covered under the ITIL SO syllabus. The following introductory glossary is provided as an introduction to the common terms found within the framework. Throughout the book, relevant terms will be discussed in more detail in the context of their corresponding process and/or lifecycle stage.
<table>
<thead>
<tr>
<th><strong>Terminology</strong></th>
<th><strong>Explanations</strong></th>
</tr>
</thead>
</table>
| **Baselines**   | *(ITIL Continual Service Improvement) (ITIL Service Transition)*  
|                 | A snapshot that is used as a reference point. Many snapshots may be taken and recorded over time but only some will be used as baselines. 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 changes in performance over the lifetime of an IT service.  
|                 | • A configuration baseline can be used as part of a back-out plan to enable the IT infrastructure to be restored to a known configuration if a change or release fails. |
| **Business Case** | A decision support and planning tool that projects the likely consequences of a business action. It provides justification for a significant item of expenditure, includes information about costs, benefits, options, issues, risks, and possible problems. |
| **Capabilities** | The ability of an organization, person, process, application, CI, or IT service to carry out an activity. Capabilities can be described as the functions and processes utilized to manage services. These are intangible assets of an organization that cannot be purchased but must be developed and matured over time.  
<p>|                 | The ITSM set of organizational capabilities aims to enable the effective and efficient delivery of services to customers. |
| <strong>External Service Provider</strong> | Service provider that provides IT services to external customers e.g. providing internet hosting solutions for multiple customers |</p>
<table>
<thead>
<tr>
<th>Terminology</th>
<th>Explanations</th>
</tr>
</thead>
<tbody>
<tr>
<td>Functions</td>
<td>A team or group of people and the tools they use to carry out one or more processes or activities. Functions hold units of an organization responsible for specific outcomes. ITIL Functions covered include:</td>
</tr>
<tr>
<td></td>
<td>• Service Desk.</td>
</tr>
<tr>
<td></td>
<td>• Technical Management.</td>
</tr>
<tr>
<td></td>
<td>• Application Management.</td>
</tr>
<tr>
<td></td>
<td>• IT Operations Management.</td>
</tr>
<tr>
<td>Internal Service Providers</td>
<td>An internal service provider that is embedded within a business unit e.g., one IT organization within each of the business units. The key factor is that the IT services provide a source of competitive advantage in the market space where the business exists.</td>
</tr>
<tr>
<td>IT Service Management</td>
<td>A set of specialized organizational capabilities for providing value to customers in the form of services.</td>
</tr>
<tr>
<td>Process</td>
<td>A set of <em>coordinated activities</em> combining and implementing resources and capabilities in order to produce an outcome and provide value to customers or stakeholders.</td>
</tr>
<tr>
<td></td>
<td>Processes are strategic assets when they create competitive advantage and market differentiation. They may define roles, responsibilities, tools, management controls, policies, standards, guidelines, activities, and work instructions if they are needed.</td>
</tr>
<tr>
<td><strong>Terminology</strong></td>
<td><strong>Explanations</strong></td>
</tr>
<tr>
<td>--------------------------</td>
<td>-----------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Process Owner</td>
<td>The person/role responsible for ensuring that the process is fit for the desired purpose and is accountable for the outputs of that process.</td>
</tr>
<tr>
<td></td>
<td>Example: The owner for the Availability Management Process</td>
</tr>
<tr>
<td>Process Manager</td>
<td>The person/role responsible for the operational management of a process. There may be several managers for the one process. They report to the Process Owner.</td>
</tr>
<tr>
<td>Resources</td>
<td>A generic term that includes IT infrastructure, people, money, or anything else that might help to deliver an IT service. Resources are also considered to be tangible assets of an organization.</td>
</tr>
<tr>
<td>Service</td>
<td>A means of delivering value to customers by facilitating outcomes that customers want to achieve without the ownership of specific costs or risks. The role of the service provider is to manage these costs and risks appropriately, spreading them over multiple customers if possible.</td>
</tr>
<tr>
<td>Service Owner</td>
<td>The person/role accountable for the delivery of a specific IT Service. They are responsible for continual improvement and management of change affecting services under their care.</td>
</tr>
<tr>
<td></td>
<td>Example: The owner of the Payroll Service.</td>
</tr>
<tr>
<td>Shared Service Providers</td>
<td>An internal service provider that provides shared IT service to more than one business unit, e.g., one IT organization to service all businesses in an umbrella organization. IT Services for this provider do not normally provide a source of competitive advantage but, instead, support effective and efficient business processes across an organization.</td>
</tr>
</tbody>
</table>
7 Common Terminology

7.1 What are Services?

The concept of IT services, as opposed to IT components, is central to understanding the Service Lifecycle and IT Service Management principles in general. It requires not just a learned set of skills but also a way of thinking that often challenges the traditional instincts of IT workers to focus on the individual components (typically the applications or hardware under their care) that make up the IT infrastructure. The mind set requires, instead, an alternative outlook to be maintained, with the focus being the service-oriented or end-to-end view of what their organization actually provides to its customers.

The official definition of a service is “a means of delivering value to customers by facilitating outcomes customers want to achieve without the ownership of specific costs or risks” (Service Strategy, page 13). But what does this actually mean? The following analogy explains some of the key concepts in a way that most (food lovers) will understand.

While most people do enjoy cooking, there are often times when they wish to enjoy quality food without the time and effort required to prepare a meal. If they were to cook, they would need to go to a grocery store, buy the ingredients, take these ingredients home, prepare and cook the meal, set the table, and, of course, clean up the kitchen afterward. The alternative is that they can go to a restaurant that delivers a service that provides them with the same outcome (a nice meal) without the time, effort, and general fuss required if they were to cook it themselves.
Now consider how that person would identify the quality and value of that service being provided. It is not just the quality of the food itself that will influence their perceptions, but also:

- The cleanliness of the restaurant.
- The friendliness and customer service skills of the waiters and other staff.
- The ambience of the restaurant (lighting, music, decorations, etc.).
- The time taken to receive the meal (and was it what they asked for?).
- Did they offer a choice of beverages?

If any one of these factors does not meet the person’s expectations, then ultimately, the perceived quality and value delivered to them as a customer is negatively impacted.

Now, relate this to an IT staff member’s role in provisioning an IT Service. If they focus only on the application or hardware elements provided and forget or ignore the importance of the surrounding elements that make up the end-to-end service, just like in the example of the restaurant, the customer experience and perceived quality and value will be negatively impacted.

But if they take a service-oriented perspective, they also ensure that:

- Communication with customers and end users is effectively maintained.
- Appropriate resolution times are maintained for end-user and customer inquiries.
- Transparency and visibility of the IT organization and where money is being spent is maintained.
- The IT organization works proactively to identify potential problems that should be rectified or improvement actions that could be made.

To help clarify the relationship between IT services and the business, we need to look at the concepts of Business Units and Service Units.
7.1.1 Business Units and Service Units

A business unit is a bundle of assets with the purpose of creating value for customers in the form of goods and services. The value received by the customer is paid for by the customer, which, in turn, ensures that an adequate return on investment is obtained for the business unit. The creation of value is dependent on the business unit’s investment of resources to increase their capabilities in delivering services. The function of the service can vary from simply providing resources to the customer to increasing the performance capabilities of the customer’s business processes. The relationship between business unit and customer is symbiotic and beneficial when value is created and returns on investment are generated.
Service units are like business units: a bundle of service assets that specialize in creating value in the form of services. Services define the relationships between business units and service units. Business units (customers) and service units (providers) can be part of the same organization or can be from multiple independent organizations.

This relationship enables business units to focus on the outcomes provided by services, while the service units focus on managing the costs and risks of providing the service, possibly by spreading these costs and risks across more than one customer or business unit.
7.1.2 Creating Service Value

Perhaps, historically, both providers and customers have used price as the focal point for communication and negotiation, but it is this path that ultimately leads to a negative experience for both parties. One of the key mantras that exist for any modern service provider (IT or otherwise) is that it is essential to clearly establish value before you can attach a price to the services offered. This ensures a few key things:

- It avoids an apple-to-orange comparison, which usually occurs with a price focal point.
- It enables the service provider to distinguish their capabilities and differentiation from their competitors.
- It clearly communicates to the customer what they can expect to receive as part of the delivery service.
Providers of IT services need to take special appreciation of the concept of value creation and communication, due to the many misunderstandings about technology on behalf of customers (and poor communication with their IT providers). To support this need, one of the major elements of the Service Strategy lifecycle is the creation of value through services and service packages.

![Figure 7.D – Creating service value](image)

*Figure 7.D – Creating service value*

*Copyright © AXELOS Limited 2011. Reproduced under licence from AXELOS Limited. All rights reserved.*

**Formula:** Service Warranty + Service Utility = Service Value

**Service Utility** describes the positive effect on business processes, activities, objects, and tasks. This could be the removal of constraints that improves performance or some other positive effect that improves the outcomes managed and focused on by the customer and business. This is generally summarized as being fit for purpose.
**Service Warranty**, on the other hand, describes how well these benefits are delivered to the customer. It describes the service’s attributes, such as the availability, capacity, performance, security, and continuity levels to be delivered by the provider. Importantly, the Service Utility potential is only realized when the service is available with sufficient capacity and performance.

By describing both Service Utility and Service Warranty, it enables the provider to clearly establish the value of the service, differentiate themselves from the competition, and, where necessary, attach a meaningful price tag that has relevance to the customer and associated market space.

### 7.1.3 Service Packages and Service Level Packages

To discuss service packages, service level packages, and how they are used to offer choice and value to customers, we are going to use the example of the packages made available by typical Internet Service Providers (ISPs).

As customers, we have a wide range of choice when looking for an ISP to provide broadband internet. So, as a result, ISPs do need to work hard to attract customers by communicating the value that they provide through their offerings. They also need to offer a wide range of choice for customers, who have varying requirements and needs for their broadband internet service.
A service package provides a detailed description of a package of bundled services available to be delivered to customers. The contents of a service package includes:

- The core services provided.
- Any supporting services provided (often the excitement factors).
- The service level package.
Service level packages are effective in developing service packages with levels of utility and warranty appropriate to the customer’s needs and in a cost-effective way.

- Availability and Capacity Levels.
- Continuity Measures.
- Security Levels.
So, for our ISP example, we can define a service package in the following way:

![Service package example (ISP)](image)

**Figure 7.G – Service package example (ISP)**

Most of the components of service packages and service level packages are reusable components of the IT organization (many of which are services). Other components include software, hardware, and other infrastructure elements. By providing service level packages in this way, it reduces the cost and complexity of providing services while maintaining high levels of customer satisfaction. In our example above, the ISP can easily create multiple service packages with varying levels of Utility and Warranty provided in order to offer a wide range of choice to customers and to distinguish themselves from their competition.

The use of service packages and service level packages enables service providers to avoid a one-size-fits-all approach to IT services.
7.1.4 Service Portfolios

A service portfolio describes the provider’s services in terms of business value. They include the complete set of services managed by a service provider. These portfolios are used to articulate business needs and the service provider’s response to those needs. It is possible for a service provider to have multiple service portfolios, depending on the customer groups that they support.

- Includes the complete set of services managed by a service provider.
- Provides the information required to manage the entire lifecycle of all services.

Three categories of services defined in service portfolios:

- Service Pipeline (proposed or in development).
- Service Catalog (live or available for deployment).
- Retired Services (decommissioned services).

Figure 7.H – A service portfolio
Service portfolios have a much larger scope than Service Catalogs and are used to manage the lifecycle of all services in order to maximize the value of IT Service Management to the business.

The portfolio should have the right mix of services in the pipeline and catalog to secure the financial viability of the service provider. Just like a financial portfolio, we need to ensure the balance between risk and benefit provided by the service portfolio.

The service portfolio uses the above information to provide informed responses to the following strategic questions:

1. Why should a customer buy these services?
2. Why should they buy these services from us?
3. What are the pricing or chargeback models?
4. What are our strengths and weaknesses, priorities, and risk?
5. How will resources and capabilities be allocated?

### 7.2 Processes and Functions

#### 7.2.1 Defining Processes

Processes can be defined as “a structured set of activities designed to accomplish a specific objective” (Service Strategy, page 20). The function of a process is to create a defined output from one or more definition. This is accomplished by defining the required actions, sequence of those actions, and dependencies with each other and the defined inputs. When effective, processes can improve the organization's productivity. Some basic characteristics exist for each process including:

- **Measurability**: The process is measured to monitor performance relative to cost, quality, duration, and productivity.
• **Specific results:** A process’ purpose is in delivering a specific result as defined output or outcome of using the process, which must be clearly identifiable.

• **Customers:** The primary results of the process are defined and delivered to customers and stakeholders, whether they are internal or external to the organization. Within this context, the process and its results must meet the expectations of the customer.

• **Responsiveness to specific triggers:** Every process is invoked by a specific trigger. This is the case whether the process is iterative like incident management or ongoing like event management.

The process is managed and executed by three generic roles:

• **Process Owner** – ensures the process is fit for purpose. The role takes on the strategic and tactical aspects of the process and ensures the process is aligned with the objectives of Service Management and the customer.

• **Process Manager** – manages the operational aspects of the process on a daily basis. The process manager role may be fulfilled by the same person fulfilling the process owner. In larger organizations, a different process manager may be assigned to different business units or customers.

• **Process Practitioner** – primary responsibilities include:
  - Carrying out one or more activities of a process.
  - Understanding how their role contributes to the overall delivery of service and creation of value for the business.
  - Working with other stakeholders, such as their manager, co-workers, users, and customers, to ensure that their contributions are effective.
  - Ensuring that inputs, outputs, and interfaces for their activities are correct.
  - Creating or updating records to show that activities have been carried out correctly ([Service Strategy, page 332](#)).
Figure 7.1 – Generic process elements

Copyright © AXELOS Limited 2011. Reproduced under licence from AXELOS Limited. All rights reserved.
The figure above describes the physical components of processes, which are tangible and, therefore, typically get the most attention. The behavioral component, which is intangible, is an underlying pattern so deeply embedded and recurrent that it is displayed by most members of the organization and includes decision-making, communication, and learning processes. Behavioral components have no independent existence apart from the work processes in which they appear, but, at the same time, they greatly affect and impact the form, substance, and character of activities and subsequent outputs by shaping how they are carried out. So, when defining and designing processes, it is important to consider both the physical and behavioral aspects that exist.

The ITIL processes covered within the Service Operation capability are:

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

### 7.2.2 Defining Functions

Functions refer to the logical grouping of roles and automated measures that execute a defined process, an activity, or combination of both. The functions within Service Operation are needed to manage the steady state operation IT environment. Just like in sports where each player will have a specific role to play in the overall team strategy, IT functions define the different roles and responsibilities required for the overall service delivery and support of IT services.
The ITIL functions covered within the ITSM capability are:

- Service Desk.
- Technical Management.
- IT Operations Management.
- Applications Management.

**Figure 7.J – The ITIL functions from service operation**

Copyright © AXELOS Limited 2011. Reproduced under licence from AXELOS Limited. All rights reserved.

NOTE: These are logical functions and do not necessarily have to be performed by equivalent organizational structure. This means that Technical and Application Management can be organized in any combination and into any number of departments. The lower groupings (e.g. Mainframe, Server) are examples of activities performed by Technical Management and are not a suggested organizational structure.
7.2.3 Connecting Processes and Functions

It is often said that processes are perfect.....until people get involved. This saying comes from failure when executing processes due to misunderstandings of the people involved and a lack of clarity regarding the roles and responsibilities that exist.

A useful tool to assist the definition of the roles and responsibilities when designing processes is the RACI Model. RACI stands for:

- **R**—Responsibility (actually does the work for that activity but reports to the function or position that has an “A” against it).

- **A**—Accountability (is made accountable for ensuring that the action takes place, even if they might not do it themselves). This role implies ownership.

- **C**—Consult (advice/guidance/information can be gained from this function or position prior to the action taking place).

- **I**—Inform (the function or position that is told about the event after it has happened).
A RACI Model is used to define the roles and responsibilities of the various functions in relation to the activities of Incident Management.

General rules that exist:

- Only 1 “A” per row can be defined (ensures accountability, more than one “A” would confuse this).
- At least 1 “R” per row must be defined (shows that actions are taking place), with more than one being appropriate where there is shared responsibility.

In the example RACI model given, the service desk is both responsible and accountable for ensuring that incidents are logged and classified, but not responsible for the subsequent investigation, which, in this case, will be performed by other functional teams.
For the service lifecycle to be successful, an organization will need to clearly define the roles and responsibilities required to undertake the processes and activities involved in each lifecycle stage. These roles will need to be assigned to individuals, and an appropriate organizational structure of teams, groups, or functions will need to be established and managed. These are defined as follows:

- **Group:** A group is a set of people who share some common theme or interest, such as performing the same activities regardless of the technology used or who they perform the work for. These people may not even work in the same functional unit. For instance, insurance agents from different companies can be a group. Groups are not used to define a formal organizational structure, but can be used to logically contain people who must follow a common process.

- **Team:** A team is a special type of group who share a common objective or purpose. They may not be part of the same organization structure, but they are typically working together and will build relationships with each other. Teams are useful in collaborating between organizational structures or dealing with a temporary situation, such as a project or major incident.

- **Department:** Formal organizational structures designed to perform several defined activities on an ongoing basis. Departments will employ hierarchy involving managers responsible for the execution of activities by department members, as well as the day-to-day management of those department members.

- **Division:** A self-contained entity consisting of multiple departments grouped together by a shared theme, such as geography
8 Introduction to Service Operation

8.1 Relationship to Service Lifecycle

Service Operation is the fourth stage of the ITIL Service Lifecycle. The other stages of the service lifecycle are:

- Service Strategy.
- Service Design.
- Service Transition.
- Continual Service Improvement.

Service Strategy is considered the hub of the service lifecycle, with design, transition, and operation acting as spokes to the outer support ring of Service Design; however, Service Operation is the fulfillment of strategic objectives and design initiatives.

Each stage of the service lifecycle will influence and depend on the effectiveness of the stages; thus creating an environment of checks and balances between the different aspects of ITSM and ensure services provide value to the customer.
8.2 Purpose and Objectives of Service Operation

Service Operation is responsible for coordinating and performing the processes and activities required to deliver and manage services to the business and customers at agreed service levels, as well as the ongoing management of the technology used to deliver and support those services. Service Operation is the day-to-day operation of IT activities, including performance monitoring, assessment of metrics, and gathering operational data.

While the tendency of IT personnel may be to focus on managing the individual components they are responsible, such as hardware or software, the ideal perspective for service operation is to have an overall view of Service Operation and delivery. This enables the organization to identify the impact caused by the individual components to the larger environment as well as the threats and opportunities in the environment on the individual components. Since services can be delivered, in part or as a whole from supplier organizations, an end-to-end view of service delivery and support ensures that all components are used effectively to achieve business objectives.

The objectives of Service Operation are:

- Using effective and efficient delivery and support of agreed IT services to maintain business satisfaction and confidence.
- Minimize the impact of service outages on day-to-day business activities.
- Ensure that only authorized personnel have access to and receive agreed IT services.
8.3 Scope of Service Operations

The scope of service operation covers the ongoing activities and components required to deliver and support services day-to-day. These components include

- Agreed IT Services.
- Service Management processes.
- Technology.
- People.

8.4 Business Value of Service Operation

The value to the business from Service Operation is dependent on adopting and implementing standard and consistent practices for Service Operation. Such an approach will provide the following benefits:

- Unplanned labor and costs for the business and IT are reduced through optimizing the handling of service outages and identifying their root causes.
- The duration and frequency of service outages are reduced to enable the business leverage the full value of the services they receive.
- Provide operational results and data to be used by other serviced management processes to improve services continually and provide justification for investing in ongoing service improvement activities and supporting technologies.
- Ensuring IT services will be accessed only by those authorized to use them in order to meet the goals and objectives of the organization’s security policy.
- Provide quick and effective access to standard services
- Support automation of operations to increase efficiencies and allowing expensive human resources to be used to lead innovation.
8.5 Context of Service Operations to Other Lifecycle Stages

As mentioned before, Service Operation will realize the requirements from Service Strategy, developed in Service Design, and tested and deployed in Service Transition. Most users will experience the efforts of serviced operation over all other lifecycle stages.

8.5.1 Service Strategy

Strategy is the center of the service lifecycle because it creates the rules, policies, and plans which all other Service Management processes align. While the service lifecycle can be seen as a sequence or cycle of activities, in reality it neither linear nor cyclical, but meshed. In this context, Service Strategy has an impact on all other lifecycle stages and how these stages are engaged by the service provider will have a profound effect on meeting the objectives of Service Strategy.

Service Strategy is focused on the creation of value and begins the process by understanding the opportunities and constraints associated with organizational objectives and customer requirements. The developed strategy will provide the boundaries regarding the services and the systems managing those services. It is within this context the Service Design operates, by establishing how the services and management systems will develop and operate for the purpose of fulfilling strategic objectives and customer outcomes.

8.5.2 Service Design

Design activities focus on the development of a comprehensive solution and how it will fit into the existing environment in order to meet the requirements of the business defined in Service Strategy. The design approach is holistic; that is, it considers more than the service solution itself, namely the architectures, management systems, processes and measurements used to ensure the delivery and support of the service solution. The end result of Service Design is the Service Design package,
which includes a high-level plan for Service Transition and Service Operation.

### 8.5.3 Service Transition

Service Transition is responsible for introducing new or changes services into the production environment: this includes providing the necessary guidance for developing and improving capabilities to support such introductions. Service Transition focuses on managing the “state” of a service, while controlling the risks associated with its introduction to the production environment. The lifecycle stage ensures the value identified in Service Strategy and encoded in Service Design can be realized in Service Operation.

Service Strategy will provide rules, policies and standards that must be honored within the services flowing through transition, but also for how Service Transition proceeds. Service Design will “encode” these rules, policies and standards into the necessary service assets and plans for transition. Most Service Transitions will be in the form of projects; and it will be necessary to design a program and project management function which consistently meets its objectives across all projects regardless of type, size, or purpose.

The Service Knowledge Management System is introduced in Service Transition and serves to identify, gather, and disseminate information necessary to be effective in all service lifecycle stages and decisions made in those stages. The design of the SKMS and its operation is a product of the Service Design stage, but more importantly, the SKMS serves as a means of capturing and disseminating information from Service Design to the other lifecycle stages as well as making information from those stages to Service Design for purposes of understanding the real world opportunities and struggles related to the design of services and management systems.
8.5.4 Service Operation

Service Operation is responsible for managing services in a production state. This lifecycle stage fulfills this responsibility according to how the service is designed, as well as how the underlying management system is designed. The responsibility involves:

- Providing guidance on achieving and improving service effectiveness and efficiency.
- Providing support of services to deliver expected value to the customer, users, and the service provider.

The design created within the Service Design stage has an opportunity to create the expected value within the Service Operation stage. But to do this effectively, the current environment must “build up” the resources and capabilities available to the service provider. This “build up” is the focus of Service Transition and enables the Service Operation stage to fully realize the value of the services.

8.5.5 Continual Service Improvement

Continual Service Improvement provides guidance on the creation and maintenance of value through better capabilities in Service Strategy, Design, Transition, and Operations. Continual Service Improvement leverages the knowledge and best practices of quality management, Change Management, and capability improvement.

In theory, the better the organization is on creating and communicating strategy, the more mature and competitive the organization will be. Likewise, the better the organization is in designing, developing, deploying, and managing services, the more likely the organization will fulfill their strategic objectives. Both these situations are made possible through continual improvement.
Continual Service Improvement can be used to achieve incremental and large-scale improvements to:

- Service quality.
- Operational efficiency.
- Business continuity.
- Investment return.

Continual Service Improvement provides guidance on:

- The improvement of services.
- The improvement of capabilities and resources to each of the service lifecycle stages.

### 8.6 Fundamental Concepts of Service Operations

The tendency for many people will be to focus on the day-to-day activities of service operation; however, the responsibilities of this lifecycle stage requires careful consideration of the whole service environment, the value it provides as of present and in the future. Some of these responsibilities include:

- Optimizing the cost and quality of services.
- Enabling the business to meet objectives.
- Effectively supporting services through proper operation of service components.
- Manage and deliver services through proper execution of operation control activities.
- Delivering services efficiently.
- Delivering services within prescribed service levels.
- Maintaining user satisfaction.
8.6.1 Areas of Concern

Every service lifecycle stage should provide value to the business and customer; however, Service Operation is where most of that value will be realized from the strategic model, to the Service Design, to the build and testing of service testing, and ongoing improvements. Beyond the day-to-day procedures and activities required to continually deliver and support the services, the personnel working within the Service Operation stage must be mindful of the various threats to the value they generate, including:

- Budget and ROI targets are supposed to be met by designed and tested services, but rarely do organizations plan effectively for ongoing Service Management. Cost estimates are easier to develop for projects, than for ongoing operations over a period of three to five years.
- The ability to obtain funding for design flaws or unforeseen requirements is difficult since it is not part of the original value proposition. Unfortunately, these flaws are often only seen over time and most organizations do not have a formal mechanism in place to review the design and value of operational services.
- Improving the efficiency of Service Operation may be difficult because funding for these tools or actions, including training, is either not directly linked to the functionality of the service or the customer already believes the costs of improvements should be built into the current price.
- Operational services which have been in place for some time will become the norm in terms of what the customer expects from the service provider. Unless the service has been problematic, the service provider may have some difficulty attempting to optimize the service or use new technology: the customer essentially believes the service provider is trying “to fix something that is not broken.”
An effective service provider will strive to optimize service operation performance whenever possible. This effort is typically focused on driving down costs of operation, guaranteeing the service's ability to meet service levels and/or demand, or reducing reaction time to operational issues or events. Optimization of service operation will usually take two paths:

- Long-term incremental improvements are performed after evaluating the performance and output of the Service Management processes over time and consists of fundamental changes to the process or technology. A new tool would be an example of this type of change.
- Short-term ongoing improvements are made to the working practices of the processes, functions and technologies underpinning Service Operation. They are typically smaller in scope and do not change the process or technology fundamentally. Training and tuning are examples of this type of change.

The processes of Service Operation are:

- Event Management – the ongoing operations of a service will be filled with events, both positive and negative; and this process is designed to coordinate activities to detect these events, determine what they mean, and determine how to respond to those events.
- Incident Management – incidents are any unexpected degradation or disruption of services to the user, and this process is designed to correct the situation as quickly as possible.
- Problem Management – unlike Incident Management, this process is focused on the root cause of the incident in order to correct it permanently or with minimal impact.
- Request Fulfillment – service requests allow users to formally request something from the service provider, such as access to an application, facilities move, or password reset. They are often standard changes, which are managed though this process, rather than Change Management.
- Access Management – this process manages the activities for granting authorized users the rights to use a service.
The processes of Service Operation are typically not separated organizational, but are processes to be performed by all IT personnel, sometimes simultaneously. For instance, many organizations will not have a formal Problem Management department which handles all problems identified. However, the service provider organization may be divided into several functions which provide different levels of process support. These functions include:

- **Service Desk** – the single point of contact for the user and responsible for addressing incidents, problems, and service requests with the user, and coordinating the efforts of other IT groups and processes to resolve the user’s concern.

- **IT Operations Management** – will execute the daily operational activities required to manage and support the IT services. This function will centralize at least some activity and staff for processes like Event Management and Access Management. The function consists of two unique sub-functions, IT Operations Control and Facilities Management, and will leverage the skills and resources from Technical Management and Application Management.

- **IT Operational Control** – ensures routine operational tasks are performed, including centralized monitoring and control of services.

- **Facilities Management** – manages the physical aspects of the IT environment, such as space, power, cooling and other concerns relevant to the management of a data center or computer room(s).

- **Technical management** – the technical skills and resources required to support ongoing management and operations of the services. Technical management will typically be involved throughout the entire lifecycle of a service and will assist the service desk with incidents and requests they cannot address themselves, usually because the service desk lacks the skill or resources.

- **Application Management** – will manage applications throughout their lifecycle, including design, development, testing, and improvement of applications. While application development may be viewed as a separate entity, application management is a broader view of what is required to support applications in all stages of the lifecycle.
8.7 Elearning Module 3 & Workbook Review Questions

1. Which of the following is not an objective of Service Operation?
   a. Provide effective and efficient delivery of agreed IT services in order to maintain business satisfaction and confidence in IT
   b. Ensure that the impact of service outages on day-to-day business activities is minimal
   c. Review and analyze service level achievement
   d. Ensure that only authorized personnel are given access to agreed IT services

2. The scope of Service Operation includes all of the following components except?
   a. Actual services
   b. Strategies
   c. Service Management processes
   d. Technology

3. Which of the following is not a value provided by service operation?
   a. Reduce the duration and frequency of service outages
   b. Ensure IT services will be accessed by those authorized to use them
   c. Provide the basis for automated operations
   d. Ensure IT services remain continuously aligned to business requirements

4. Improvements are a means of optimizing Service Operation; which of the following is an example of long-term incremental improvement?
   a. Incident Management tool set
   b. Performance tuning
   c. Workload balancing
   d. Personnel redeployment
5. Which of the following is not a Service Operation process?
   a. Incident Management
   b. Problem management
   c. Request fulfillment
   d. Change Management

6. Which of the following processes does the Service Desk have little responsibility?
   a. Incident Management
   b. Event Management
   c. Problem management
   d. Request fulfillment
Chapter 9

9 Principles of Service Operation

While the concept of Service Operation is simple, its actual execution can be intricate and complex. Service Operation provides more to the service lifecycle and Service Management capabilities of the service provider than the basic move from conceptual (Service Design) to actual (Service Operation); it provides the means for understanding the service environment and controlling. Its three primary processes provide systems which are used extensively throughout the entire service lifecycle, namely:

• Service Knowledge Management System.
• Configuration Management System.
• Change Management Process.

9.1 The Dynamics of Service Operation

If a person thinks that Service Operation is simply a set of repetitive procedures and activities, they would be incorrect. While Service Operation does have to deliver and support services as designed in order to meet a specified and agreed level of service, they have to do so in an environment that is constantly changing. As a result, the activities which may work at the moment may have to be adjusted to be effective in the next. In this sense, Service Operation has to maintain the status quo while adapting to change.
There are four key areas while Service Operation has to manage potential conflict in a dynamically changing environment:

- Internal IT and External business perspectives.
- Stability versus responsiveness.
- Quality versus cost of service.
- Reactive versus proactive.

9.1.1 Internal and External Perspectives

The core conflict in an IT environment is the perspective one has on the environment, specifically internally with IT personnel and externally with business personnel. Consider the perspective most people will have their automobile. Ordinary drivers are chiefly concerned that the automobile fulfills its function—it delivers the person to their destination in the desired time frame. If the car breaks down, they will quickly start blaming the car. However, car enthusiasts, professional drivers, and mechanics, as well as car manufacturers, understand automobiles to be delicate and interactive machines.

IT services have similar perspectives. The customer simply wants what the service promises to deliver and they don’t care about how the service is delivered or any underlying problems preventing delivery. IT personnel, however, care about the components of the service, which are often managed across several departments who specialize in different technologies and methods. The conflict ensures when what is delivered becomes more important than how it is delivered, or vice versa. Services should be structured to support the customer, but without compromising the quality of service by not considering the proper components are in place. Focusing on the services being delivered over how those services are delivered, the service provider can potentially promise to deliver something they do not have the resources or capabilities to deliver. However, focusing on the service components over the value those components deliver will potentially lead to expensive services with little value being generated.
When an organization is focused entirely from an internal perspective, they are more concerned with the performance and management of IT infrastructure devices, systems and staff without being greatly concerned with the end result of the service. As a result, the metrics will consist of technical performance and not the quality of the service output. Generally, the delivery of the service will be highly consistent, usually focusing on a standard set of services used by all business units, but will not provide everything the business needs. Adopting new technology, architectures, or techniques is difficult as the goal is to establish and maintain standard operations. Cost reductions are typically obtained when consolidating technology or optimizing operational procedures and resources, while some benefits may be seen immediately, the larger impact of cost cutting will take significant time to understand. Training is performed as an apprenticeship because a high level of specialization occurs in the environment. Training that will concentrate on “what to do” is given greater priority over “why to do it.” The general assumption from personnel is that good customer service is only available through good technical achievement.

If an organization is focused from an external perspective, performance (typically to service level agreements) is the driving force rather than technical capabilities and achievements. Metrics will report on outcomes, but will not show how those outcomes were achieved. Internal metrics may exist, but they must be devised and obtained by staff internally. As a result of not measuring technical capabilities, the level of consistency in service delivery is generally poor and staff are “reacting” to operational needs. Typically, the organization is comprised of multiple delivery teams and multiple technologies. While services may be more customizable for the customer, adopting new technology, architectures, and techniques will create new teams within the organization. Additionally, priority is given to the customer who has the most need and is willing to pay for the service. Training is performed from project to project and standard training courses are not generally seen. General knowledge is encouraged and specialist skills are typically consolidated within the organization.
To properly balance the internal and external perspectives to services, the service provider must ensure that the following concerns are addressed:

- Knowledge of the services used by the business and their justification.
- Knowledge of the relative importance and impact of services on the business.
- Knowledge of how technology is used to provide those services.
- CSI project involvement of service operation to identify opportunities to deliver more, increase quality of service and decrease cost of service.
- Creation of procedures and manuals related to the management of technology and delivery of IT services.
- Establishing a set of differentiated metrics to report the achievement of service objectives to the business, and the effectiveness and efficiency of Service Operation to IT management.
- Knowledge across the entire IT organization on how technology performance can affect the delivery of IT services, the business and business goals.
- Standard operating procedures which can meet requirements for both standard services delivered consistently to all business units and non-standard services delivered to specific business units.
- Balancing the requirements of different business units with the cost savings provided through optimization of existing technology or investments in new technology, encapsulated in a single-cost strategy
- The establishment of a value-based ROI strategy over a cost-based strategy.
- The use of CSI as input and feedback to identify areas of imbalance and means of enforcing improvements.
- A clear communication and training plan for the business.

### 9.1.2 Stability and Responsiveness

Beyond the different perspectives from internal and external stakeholders and groups, Service Operation is already dealing with a critical struggle between ensuring the stability of the services delivered and responding effectively and quickly to changes affecting that stability. Stabilization takes time and effort in many cases, as service components are tuned to find the best configuration
for the demand on the service, people become more familiar with the functionality and levels of service, and historical data can demonstrate consistency in performance.

While some changes may be evolutionary, happening over long periods of time as the functionality, performance, and architecture of the service or service components change, many of the changes experienced in an IT environment will come about rapidly and with great pressure to implement. Being able to respond appropriately to both types without impacting other services has its inherent challenges. Evolutionary changes allow the service provider to plan on how to stabilize the environment, but the rate of change may be too slow in order to deal with the immediate concerns of the customer. The more immediate changes will satisfy the customer, but will cause greater upheaval in the environment.

The primary focus of stabilization is on the technology: developing and refining IT management techniques and processes. The organization will choose to demonstrate compliance to standard operating procedures and agreements, even when alignment to business requirements is clearly missing. Growth occurs as a result of analyzing demand on existing systems: new services or systems are typically a product of “rogue” efforts within business units. New technology, architectures and methodologies are resisted and new or changed services must operate within existing parameters to be accepted.

The primary focus of responsiveness is the output of the business. As a result, changes may be agreed to before understanding what it will take to satisfy the change. Routine tasks are not typically defined, documented or even executed because the staff is busy with new services or new projects. Capital spending is justified for every new business requirement and existing technologies and solutions may be used for similar services which have slightly different business requirements. Usually, the service provider will over-provision technology and forecasts are based on future demand on services without considering current workloads.
A balance between stabilization and responsiveness can be achieved by addressing the following concerns:

- Adopt an adaptive strategy, rather than rigid, to investing in technologies and processes.
- Establish a solid foundation for service level management, which ensures involvement throughout the entire service lifecycle from Service Design to Service Design.
- Encourage complete mapping of business requirements to IT operational activities and components by ensuring integration between service level management and other Service Design processes.
- Initiate changes at the earliest possible stage in the service lifecycle to ensure functional and management requirements can be assessed, built, tested, and changed together.
- Ensure early involvement of IT in business changes occurs as soon as possible to ensure IT services are scalable, consistent and achievable to support the change.
- Rely heavily on service level management to avoid “rogue” informal agreements among business, IT managers, and staff.

9.1.3 Quality and Cost of Service

There is typically a direct correlation between the quality of service and the cost of service: as the quality of service increases, so does the cost of service. However, the correlation is not always proportional: an improvement in service availability from 50% to 75% may be less expensive than an improvement from 98% to 99.9%. Ironically, most service provider organizations are expected to increase the quality of service while reducing the costs of service. This demand on service provider can be achieved within what is called a “range or optimization” for the service. Understanding where that range is can be difficult because it will be different from each service and there is no standard or template for calculating that range.

Establishing an appropriate balance between cost and quality needs to be done within the Service Strategy and design stages; though many organizations will leave it to Service Operation, who typically will not have the perspective, knowledge, or authority to be effective in achieving the
desired balance. It is possible for organizations to spend massive amounts of money without improving the quality of a service: usually because they are not analyzing the situation to find the source of the inefficiency. Blatant cost cutting without considering the long-term effects to quality should not be performed, but occurs commonly in IT organizations because of business pressures.

Unfortunately, the impact of cost-cutting initiatives is not always seen immediately and may grow unnoticed like a snow ball down a hill. Consider a common initiative of reducing staff. At first, a slight increase in the number of incidents may be noticed, as well as more time needed to resolve incidents. This is primarily due to less people being able to monitor the systems and proactively correct any noticeable problems. After the staff cuts, less people are now doing more to resolve incidents which are typically reactive. The more incidents being worked, the less proactive the staff will be; as the number of incidents increase, the more hours staff would usually have to work, leading to fatigue, apathy, and lower productivity. Eventually, the quality of service has dropped significantly and the investment needed to return to its former state will be greater than the cost savings achieved through the initiative.

This does not mean that cost-cutting initiatives should be avoided, just that they should carefully consider what costs are being cut and what the long-term impact will be. In the example given, the reduction in staff did not consider the level of proactivity being performed: efforts which are not easily seen or justified until they are not being made. Think in terms of war where staff is actively holding back the invaders. Reduce the number of defenders and a breach is imminent. A possible solution is to automate what the staff is doing proactively, but this may require additional spending if the level of automation currently supported is too low. Another solution is to reduce the number of systems that the staff is supporting, which is often the focus of consolidation efforts: less systems supported, the less staff required to support those systems. However, the number of systems available needs to be able to support the demand for the services.

Ideally, the most effective means of balancing quality and costs are through proper management and use of service level requirements, as well as understanding the business purpose and associated
risks of those requirements. Effective management of these requirements will ensure that a service properly “sized”—the correct number of IT resources is identified and maintained to provide the right level of service quality. In support of these requirements, the financial management process and tools are able to account for and cost of providing IT services and model alternative methods of delivering services at different cost projections. Additionally, managers with appropriate authority are making decisions regarding cost versus quality at the strategy and design stages of the service lifecycle. IT operational managers should only make financial decisions regarding the achievement of operational efficiencies.

9.1.4 Reactive and Proactive

The concepts of a reactive or proactive organization are related to that organization’s relationship to external factors or forces. When an organization takes action when influenced by an external force, it is said to be reactive; but when an organization takes action to influence the external force, it is said to be proactive. In truth, an organization must do both, be reactive and proactive. An organization which is more reactive in design will often experience greater effort and cost in its activities and has a higher risk to the stability and consistency of service delivery. While being proactive is seen as positive, an organization that embraces this side of the scale will tend to have higher costs and ignore the existing and current issues a customer may have.

The ability of an organization to balance the reactive and proactive needs of the ITSM requires understanding:

- The organization’s maturity – maturity relates to the organization’s experience and commitment to delivering a consistent set of IT services, which can result in developing an understanding about the relationships among the business, IT, IT infrastructure and IT services.
- The organization’s culture – where the organization’s belief and value system(s) directs them will influence how things are done: a culture of innovation tends to be more proactive, while a culture of maintaining the status quo will be more reactive.
- IT’s role and mandate – the involvement IT has in developing business strategy and tactics is
a key factor as IT organizations who are more involved will tend to be more proactive.

- Level of integration for management processes and tools – greater integration leads to increased recognition of opportunities to explore proactively.
- Knowledge management’s maturity and scope – storing, organizing and analyzing historical data increasing the organization’s ability to recognize opportunities.

Maturity will likely be a major topic for service operation, as many use the term to describe an organization’s effectiveness in a variety of different areas. Maturity assessments have been adopted to measure organizational maturity, process maturity, service maturity and software maturity. These assessments simply measure where the organization falls within a prescribed set of characteristics or best practices. Generally speaking, the less mature an organization is, the more reactive its efforts will be: therefore, the desire is to be more proactive, or mature. This doesn’t disregard the need for an organization to be reactive, but they are doing so according to a set of predefined policies, processes, and understanding of responsibilities and consequences. Below are some basic observations about maturity:

- New IT services and technologies will be introduced at a lower maturity because the organization’s experience, knowledge and understanding will be low. Over time and with a commitment to generate and share knowledge, the maturity will increase for the organization.
- Less mature organizations tend to be more reactive, simply because they are not exposed to all the variables of a particular situation.
- Newer IT organizations will usually hire IT staff members who are “generalists,” knowledge across a broad spectrum of IT technologies or methodologies: this is because the organization will not fully understand the competencies and skills required to deliver specific aspects of the services.
- The level of unpredictability surrounding incidents and problems will increase for newer services and/or organization as they stabilize.
- Maturity is a by-product of more knowledge, information, data and reporting which can be used to identify patterns, workflows and trends.
- Maturity is also a by-product of creating and maintaining good relationships among IT staff,
business staff, customers, and suppliers.

To balance the organization’s effectiveness to be both proactive and reactive, the following recommendations should be addressed:

- Problem management and Incident Management should be formalized and integrated between service operation and continual service improvement.
- Both technical faults and business demands need to be prioritized and supported though appropriate incident categorization systems, escalation procedures and impact assessments for change.
- Service Asset and Configuration Management should be able to provide the necessary data needed to make informed and timely decisions across the organization.
- Service level management should be actively involved in Service Operation.

### 9.2 What is Good Service?

“Good service” has some basic characteristics. At the forefront, the service meets the customer’s needs, but it does so in a timely, courteous and professional manner. Think in terms of a mail service, such as the US postal Service, UPS, or Federal Express. As a customer, you use the service to send or receive a package: ultimately the point of the service is to ensure the package arrives at its destination. However, the service may be perceived as poor if the package is delayed or arrives late, the package is damaged, or the delivery person is rude or unpresentable. In this situation, the customer was “served,” but the service would not be considered “good.”

To correct the problem, the mail service may implement tracking controls which ensure that the package is delivered on time, will improve handling procedures, and provide additional training and performance incentives to its delivery staff. As long as the core objective, delivering the package, is achieved, all other concerns can be addressed appropriately. However, organizations need to understand that meeting objectives and how those objectives are met are distinctly different ideas to be developed.
9.3 Early Lifecycle Involvement of Operation Staff

For most IT organizations, there are two distinct groups of people—operational personnel and non-operational personnel. Operational personnel are generally responsible for the day-to-day management and maintenance of the IT infrastructure, applications and services. Non-operational personnel are comprised of administrators, designers, managers, and other persons responsible for the strategic and tactical thinking and decision-making required to grow the business and support the customer. Unfortunately, the separation between these two groups is extensive in most organizations. The usual result of such a split will have managers making decisions that the operational staff cannot implement or operational staff who are performing without any real guidance.

ITSM practices will ensure proper alignment between service performance and business need. However, a mature organization will improve its success by involving operational personnel as early as possible in the service lifecycle.

Operational personnel can support Service Strategy through the following actions:

- Identify and communication current capabilities in the operating environment, workload levels and staff skills against developing IT strategies.
- Gather and identify IT operational costs.
- Identify high-level impact of IT strategies.
- Identify operational risks for developing IT strategies.
Effective Service Operation is a result of good Service Design, specifically:

- Definition of IT service objectives and performance criteria.
- Mapping IT service specifications to the performance of the IT infrastructure.
- Definition of operational performance requirements.
- Mapping services and technology.
- Modelling the effects of changes to technology and changes to business requirements.
- Providing appropriate cost models.

For most organizations, Service Design is not an independent function of the service provider separated from service operation; in fact, most people involved in Service Design will be operational staff. This is because operational staff is considered the subject matter experts in the different aspects of IT delivery and support, services, applications and infrastructure.

Operational staff is also involved in Service Transition to ensure consistency and build experience and knowledge necessary for the ongoing Service Operation. Specific activities in Service Transition performed by Service Operation include:

- Training on new or changed services.
- Participation and review of operational acceptance tests.
- Participation in transition planning to identify impact on current operational activities.
- Participation in transition project activities, particularly deployment.
- Providing early life support for new services or major changes and releases.
- Participation in quality assurance.
Service providers should always strive for improving service delivery and support, which will typically mean improving service operation. As a result, service operation should be involved in supporting and identifying opportunities for improvement, specifically:

- Ensuring operational data is available for use in improvement efforts.
- Validating accuracy of operational data used to identify opportunities for improvements.
- Assessing the impact of proposed improvements on existing operations.
- Executing operational tasks to support monitoring, measuring and reporting.
- Identify and promote operational issues and concerns to CSI staff.
- Identifying and proposing improvements to enhance performance and quality of IT services.
9.4 Elearning Module 4 & Workbook Review Questions

1. Achieving balance in Service Operation is a factor of success for an IT organization, but which of the following balancing acts is not a function of service operation?
   a. Cost of service versus quality of service
   b. Functionality versus time and resources
   c. Reactive versus proactive
   d. Stability versus responsiveness

2. Which statement best describes the external view of IT:
   a. The way IT services are experienced by its users and customer
   b. The way IT components and systems are managed to deliver the services
   c. The way IT services are packaged by the service organization
   d. The way IT components and systems are delivered by third-party suppliers

3. Which of the following is a potential risk of focusing on stability over responsiveness?
   a. Overprovisioning of resources
   b. New services are not leveraging existing infrastructure
   c. Existing workloads are not relevant or considered
   d. Business units may take ownership of systems to get access to new services

4. Which of the following is a problem experienced by focusing on cost of service over quality of service?
   a. Escalating budgets
   b. Escalating demands for higher-quality services
   c. Escalation from business to get more service from IT
   d. IT services deliver more than required
5. What is the disadvantage to being proactive?
   a. Over-planning of IT recovery options
   b. Similar incidents occur repeatedly
   c. Staff turnover is high
   d. Morale is generally low

6. What is the critical element of being a proficient service provider?
   a. Placing emphasis on recruiting and training staff to development competency in technologies and IT tools
   b. Placing emphasis on providing timely, professional and courteous service to allow the business to conduct its own activities
   c. Training staff on how to delivery and support IT services, as well as the manner in which services should be provided
   d. Placing emphasis on recruiting and training staff to develop competency in dealing with and management customer relationships and interactions

7. Which of the following activities does operation staff perform to support Service Strategy?
   a. Link IT service specifications to the performance of the IT infrastructure
   b. Identify and communicate current operational capabilities, workforce levels and operational staff skills
   c. Provide a mapping of services and technology
   d. Participate in quality assurance activities
8. What is the advantage of using operations staff in Service Design activities?
   a. Ensures operational tasks are executed to support service monitoring, measurement and reporting activities
   b. Ensures consistency and the achievement of stated business and manageability requirements
   c. Ensures continuity between business requirements and technology design and operation
   d. Identifies high-level impacts of chosen IT decisions on current operational activities
9.5 Achieving Operational Health

What is operational health? The best explanation is relating a human being’s body to a machine where vital statistics can be monitored to identify optimal performance levels. When those optimal levels are reached, the subject is considered healthy; and when the levels are not reached, the subject is considered unhealthy. The same can be applied to Service Management, where optimal performance levels can be identified and monitored.

What interesting about managing the health of a human being is that vital statistics will focus on a few operating premises and not the entire body. When a person goes in for a routine check-up, the doctor will concentrate on the person’s heart, lungs, blood, and the senses. Any further examination will be based on the patient’s medical history or complaint’s they have. Within an IT service environment, not every service component has to be monitored unless there is a suspicion of a problem.

This does not mean that service components are ignored forever. As with medical exams, certain examinations are recommended from time-to-time. These examinations are more thorough than a routine spot-check. In an IT environment, every system should have a thorough examination from time-to-time and most organizations will ensure this is done at least once a year, if not quarterly. As with a human being, the need for these extra exams may be based on the subject’s age, activity and recent performance.

As with health care, the primary reason for a routine check or monitoring is preventive: to identify and correct any incidents or problems which prevent the subject from performing at optimal levels. Advances in operational health have led to the development of self-healing systems: systems designed to resist severe operating conditions and detect, diagnose, and correct from more incidents and known errors.
The major characteristics of a self-healing system are:

- Hardware, software, data and operating system resilience are designed and built into the system.
- Processing can be shifted from one physical device to another without disrupting the service.
- Built-in monitoring utilities can detect events and compare against normal operating conditions.
- A correlation engine can determine the significance of each event and identify an appropriate predefined response to the event.
- Diagnostic tools can detect errors in system operations and determine an appropriate response.
- Manual intervention can be called upon through alerts.

### 9.6 Communication Requirements for Service Operations

In previous exam guides and sections of this guide, the importance of communication between Service Operation and other stages of the service lifecycle have been highlighted; however, communication between the different functions within Service Operation is equally important and vital for the effectiveness of Service Operation. As with any communication, communications within Service Operation should have an intent or desired result within a determined audience. The different topics of communication will typically fall into one of these general categories:

- Routine operational communications.
- Communication between shifts.
- Performance reports.
- Project communication.
- Communication related to changes.
- Communications related to exceptions (incidents and problems).
- Communications related to emergencies.
• Training.
• Communication from strategy, design and transition.

Methods of communication in Service Operation can include the following tools:

• Email.
• Social media.
• Web-based internal relay chat.
• Short message service messages
• Pagers.
• Instant messaging or texting.
• Web-based chat rooms.
• Voice over Internet Protocol (VoIP) utilities.
• Teleconference utilities.
• Video-conference utilities.
• Document-sharing utilities.

9.6.1 Meetings

One of the primary avenues of communication for a service organization is meetings: which can also be abused and misused. The purpose of any meeting is to communicate effectively to a group of people about a common set of objectives or activities. They need to be controlled and brief, with the intent to facilitate action. Some tips for effective meetings:

• Establish and communicate a clear agenda in advance to allow participants to prepare and meet meeting objectives.
• Ensure the rules of conduct in meetings are understood and enforced.
• Create notes of issues not relevant to the meeting.
• Establish guidelines for minutes of the meeting and how those minutes will be used.
• Encourage the appropriate level of participation from everyone.
Generally speaking, service operation will have three general categories of meetings:

- **Operational meetings** – typically attended by managers at the beginning of a business day or week, the purpose of these meetings are designed to communicate issues which may impact the operational state of the service. Operational meetings allow the organization to “sync.”

- **Team meetings** – managers will typically take information from the operational meeting and communicate to their respective departments, groups and teams the relevant points. Team meetings are also an opportunity to discuss in detail the incidents, problems and changes which are still open and allow communication of:
  - Progress or status.
  - Confirmation of immediate actions to be taken.
  - Estimated completion times.
  - Requests for resources.
  - Raising of potential problems or issues.
  - Staff availability.
  - Confirmation of holiday or vacation schedules.

- **Customer meetings** – communication with the customer will generally be required after a major incident which impacted business operations, to discuss areas of common concerns, or review of service quality and performance. In most cases, meetings with the customer will be scheduled and conducted in cooperation with business relationship management and service level management.
9.7 Documentation Requirements for Service Operations

Consistent operations of services, processes, and services will require some level of knowledge sharing, not only across the organization, but over time and across the entire service lifecycle. Rather than trying to ensure all the relevant and interested persons are meetings, the best approach for sharing data, information and knowledge is through rigorous and accurate documentation. Service operation is a major source of all data and information used by the service provider and business: every function is involved in creating and maintaining a variety of documents and records stored within the service knowledge management system.

Documentation activities in Service Operation include:

- Defining and maintaining process manuals for all processes a person is involved in, including all Service Management processes across the entire service lifecycle.
- Creating and maintaining technical procedures.
- Creating and maintaining planning documentation.
- Creating and maintaining the content in the service portfolio.
- Defining and maintaining work instructions for Service Management tool(s).

9.8 Inputs and Outputs of Service Operation

The inputs to Service Operation from other service lifecycle stages include:

- Service Strategy:
  - Vision and mission.
  - Service Portfolio.
  - Policies.
  - Strategies and plans.
- Priorities.
- Financial information and budgets.
- Demand forecasts and strategies.
- Strategic risks.

- Service Design:
  - Service catalog.
  - Service Design packages, including:
    - Utility and warranty details.
    - Operation plans and procedures
    - Recovery procedures.
  - Knowledge and information in the SKMS.
  - Vital business functions.
  - Hardware and software maintenance requirements.
  - Process and procedures designs for Service Operation.
  - SLAs, OLAs, and underpinning contracts.
  - Security policies.

- Service Transition:
  - New or changed services.
  - Known errors.
  - Standard changes.
  - Knowledge and information in the SKMS.
  - Change schedule.

- Continual Service Improvement:
  - Customer and user satisfaction survey results.
  - Service reports and dashboards.
  - Data required for metrics, KPIs and CSFs.
  - Requests for change for implementing improvements.
The outputs from Service Operation to other service lifecycle stages include:

- **Service Strategy:**
  - Operating risks.
  - Operating cost information on calculating TCO.
  - Actual performance data.
- **Service Design:**
  - Operational requirements.
  - Actual performance data.
  - RFCs to resolve operational issues.
  - Historical incident and problem records.
- **Service Transition:**
  - RFCs to resolve operational issues.
  - Feedback on quality of Service Transition.
  - Input to operational testing.
  - Actual performance information.
  - Input to change evaluation and CAB meetings.
- **Continual Service Improvement:**
  - Operational performance data and service records.
  - Proposed problem resolutions and proactive measures.
  - Knowledge and information found in SKMS and CMS.
  - Achievements against metrics, KPIs, and CSFs.
  - Logged improvement opportunities.
9.9 Elearning Module 5 & Workbook Review Questions

1. What predefined information is important for determining the best measurements to use to monitor operational health?
   a. Vital Business Functions
   b. Critical Services
   c. Functionality
   d. Design constraints

2. The criteria used to determine operational health is developed in what service lifecycle stage?
   a. Service Strategy
   b. Service Design
   c. Service Transition
   d. Service Operation

3. Which of the following tool solutions are not perceived as self-healing systems?
   a. Automatic systems
   b. Clustered nodes
   c. Adaptive systems
   d. Dynamic systems

4. What is the most important principle in communications?
   a. An audience for the communication must be clearly defined
   b. The audience has a say in what is being communicated
   c. Communication must have an intended purpose or resultant action
   d. Frequency, location and type of medium used for communication must be documented in a policy
5. Proposed problem resolutions and proactive measures are outputs of Service Operation to what service lifecycle stage
   a. Service Strategy
   b. Service Design
   c. Service Transition
   d. Continual Service Improvement
10 Processes of Service Operation

The processes of Service Operation include:

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

One of the unique characteristics of these processes is their cross-functionality: that is, every function, department, group, and team will have some role in their success, usually at different levels of involvement. For instance, it may be asserted that Incident Management and request fulfillment are designed for the Service Desk, but they are not exclusive to the Service Desk. In fact, these processes may be owned by the Service Desk to ensure their objectives are met, but used by other functions in the organization. For example, most service agreements require a certain number of incidents to be resolved at the Service Desk, usually around 75-80%. However, the remaining incidents are expected to be resolved by an appropriate team within the service organization either because it requires manually touching the impacted system or the Service Desk does not have the competency to resolve the incident. When second level support is called in to resolve the incident, they are still using the same Incident Management process the Service Desk is using. The same is true for the Request Fulfillment process.

Another characteristic of the Service Operation processes is their application to service lifecycle activities and Service Management systems. For instance, access to the service portfolio will be
managed in the same way that access to a customer application will be managed. Problems occurring as part of Service Design and transition will utilize the Problem Management process to identify the root cause. Event Management can monitor the performance of the lifecycle stages just as easily as it can monitor customer delivered services and supporting components.

10.1 Event Management

An event is any change of state that has a significant impact on the management of the configuration item or IT service. While some changes of state are induced as part of Change Management; other state changes are the result of unexpected, unintended or unpredicted conditions within the service environment. A corollary may be the closing of a road: sometimes the road is closed because of infrastructure repairs and other times because the weather will make the road too difficult to drive. While Event Management will communicate all events (closings), it is primarily concerned with those random, unplanned events.

The activities of event monitoring will focus on monitoring the IT environment, services and service components. For Event Management to be effective, it requires two components. The first is a solid understanding of what normal operation of the environment, service and components looks like: this allows Event Management to compare the results of monitoring to identify any significant deviations from the norm. The second is a good set of monitoring and control systems: if the service cannot be monitored according to design, then Event Management has no real value to the business or IT.
The monitoring and control systems are categorized into two types of tools:

- Active monitoring tools will regularly poll, ping, or request information from key configuration items to determine their status and availability.
- Passive monitoring tools will detect and correlate operational alerts or communications from configuration items.

The difference between these two types of tools can be associated with active interviewing and observation. For instance, a political pollster will get a sense of the political landscape for an election by engaging the public through surveys – this can be correlated to active monitoring. However, a political analyst may draw up conclusions through observing the behaviors and trends within the voting population – this correlates to passive monitoring. Both can provide significant information about the political state and both can be used independently from each other or together for a larger picture of the situation.

10.1.1 Purpose and Objectives

While monitoring may be the significant activity of Event Management, the end goal is not to simply monitor, but to allow the service provider to manage events through their lifecycle, which consists of:

- Detection.
- Understanding.
- Response.

Operational monitoring and control relies heavily on the capabilities of Event Management. If the three stages of the event lifecycle can be programmed with appropriate data, then Event Management becomes the basis for automating many routine operational tasks. While automation may not be the goal of Event Management, its effectiveness allows automation to be successful.
The objectives of Event Management include:

- Detect all changes of state with a significant impact on the management of a configuration item or IT service.
- Determine the appropriate action to control events and ensure these events and actions are communicated to the responsible functions.
- Trigger the execution of many Service Operation processes and operations management activities.
- Compare actual operating performance and behavior against design standards and service level agreements.
- Support service assurance and reporting and continual service improvement.

10.1.2 Scope

Let’s take an event in the life of a child from a parent’s perspective. The event is detected and can be physical (a fall), emotional (child is sad), mental (trouble reading), social (child is sitting alone), or a myriad of other events in a child’s life. Once the event is detected, the parent will attempt to understand the circumstances and impact of the event as quickly as possible. If the child falls, they determine if the child is hurt: do they have a broken bone or a cut. In practice, the parent will encourage the child to “return to normal.” If the child is hurt, they attempt to determine the reason behind the injury: were they pushed, from what height did they fall, or other circumstances they can catalog as evidence. This evidence can be used to determine an appropriate response. Can the child walk it off or do they need a doctor?

The role of Event Management is similar to the role of a parent, where the IT services are the children. This analogy is appropriate because the question which begs an answer is “what is the scope of Event Management?” In other words, how far should a parent go to protect their child? The extent of protecting a child is not in question here; however, it provides a good basis for asking what events a parent should be watchful. In a high crime area, a parent may need to protect their child from severe events like drive-by shootings. A well-to-do parent or celebrity may be more concerned with abductions. Poor schools may be hot beds for drugs or alcohol.
While many events a parent may monitor have negative overtones, positive events should also be monitored and managed. A good grade should be encouraged and a parent may need to tutor the child. Scheduled events like games, recitals and other events are places where good behavior can be reinforced.

The scope of Event Management is dependent on what the organization considers an event, both positive and negative. Essentially, the process is applicable for any aspect of Service Management that needs to be controlled. This can include any of the following:

- Configuration items which need to remain in a constant state and events identify when the CI moves out of the desired state.
- Configuration items which need to change states frequently and events that ensure these state changes are triggered automatically or on schedule.
- Environmental conditions such as temperature, water pressure for cooling systems, or fire and smoke detection systems.
- Software licensing management to ensure optimal and legal usage of licenses.
- Security threats, intrusion and detection systems.
- Normal or predicted utilization or performance of individual components.

10.1.3 Value to Business

The value Event Management provides the business is indirect, because it is largely hidden from the customer. However, the benefits that come from this process allow other customer-facing processes to be effective and satisfy the customer in various ways.

- Incident Management – Event Management has mechanisms in place to detect incidents early which can be resolved before an actual service outage occurs or impact to user(s) felt.
- Availability Management – downtime can be reduced by monitoring some types of automated activities by exception: these mechanisms are also less expensive and require fewer resources to operate.
- All Service Management processes – Event Management can identify and alert when status changes or exceptions to the process occur which can allow a person to respond quickly
and improve the performance of the process: the result is often a Service Management solution which is more effective and efficient.

- Resource management – as a basis for automated operations, Event Management can increase efficiencies and enable the organization to assign human resources to more innovative work or focus on service improvement.
- Business Relationship Management – Event Management can have a direct impact on customer satisfaction and service delivery by monitoring key aspects of a business service and alert the appropriate person; thus improving responsiveness.

10.1.4 Policies, Principles, and Basic Concepts

Not every event monitored is the same and different types of events will provide a different set of information and require a different response. In general, there are three categories of events:

- Informational events are used to alert when a significant event has occurred, but will not require a response. The information is typically used as evidence for planning or response to incident or problem. User logins and logouts are examples of informational events.
- Warning events will identify unusually, but not exceptional, performance and is usually based meeting a pre-defined threshold which is being monitored: for example, the processing resources for a server are at 85% utilization. The alert provided by a warning allows the organization to monitor the situation much closely than they normally would.
- Exception events identify exceptions in Service Operation. Exceptions are typically pre-defined and indicate a problem with service delivery and support operations which require immediate response.

What events will be monitored and what they mean is determined by the service provider. An event can be informational, a warning or an exception based on the organization's understanding and relationship to the event. For example, user logins may be informational, but a warning may be initiated if the number of user logins to a service reaches a defined threshold, or an attempt to login with an incorrect username/password combination may be seen as an exception.
Events are communications in the form of event notifications: meaning they require some form or sending and receiving messages along the network. This is important to understand because messages will utilize IT resources which could be used to support the services. While resource utilization is low for individual events, a large number of monitored or actual events can use a significant portion of those resources at any given time. Therefore, Event Management requires planning to determine how events are defined, generated and captured.

Understanding the different types of events is a prelude to understanding the different policies an organization may adopt for Event Management, such as:

- Event notifications can only be sent to those persons or systems responsible for handling further actions or decisions to avoid unwarranted or unwanted communications.
- Event Management and monitoring should be a centralized function to avoid organizational conflicts in managing events.
- A common set of messaging and logging standards and protocols should be used for all application events to enable consistent handling of events.
- Automation of event handling activities is preferred over the possibility of human error resulting in incident.
- A common handling and escalation process should be referenced by a standard classification scheme to support consistency in handling events in a manner that supports operational and service level objectives.
- All events should be captured and logged as evidence used in the analysis for incidents, problems and trends.

As mentioned, not every event will have the same meeting across different organizations and, in a single organization, not every event needs to be monitored or responded to equally. To highlight those events of importance, the organization will introduce a mechanism to filter the events. This enables the organization to focus management and control efforts on those events of particular significance to the organization.
To obtain the proper level of filtering, one or more of the following strategies may be adopted:

- **Integration** – Event Management is integrated into all Service Management process. For instance, warnings identifying that a resolution SLA may be breached in Incident Management is a form of integration.
- **Design** – Event Management is a major consideration when designing new or changed services.
- **Trial and error** – a formal process is introduced to evaluate the effectiveness of filtering and adapt accordingly to achieve optimal results.
- **Planning** – project-based efforts to introduce Event Management software into the IT environment with realistic time frames and adequate resources allocated.

10.1.5 Designing for Event Management

Event Management is not an activity that simply happens; it must be designed. Since the core activity of Event Management is monitoring the performance and availability of a service, targets and mechanisms for monitoring are key inputs from the capacity management and availability management processes. Designed event mechanisms need to be tested and evaluated within Service Transition. Event mechanisms are key components of a successful deployment of service because they may provide demonstrative proof of the value the service provides to the customer.

Because Event Management is a major activity of Service Operation, which manages an ever-changing environment, the design of Event Management cannot be done in isolation by remote system developers; nor should Event Management become static because the design is developed and agreed. Day-to-day operations will need to define different priorities, alerts and other improvements that will influence Event Management design.
When designing Event Management, the following questions are pertinent:

- What needs to be monitored?
- What type of monitoring is required?
- What will an event be generated?
- What type of information needs to be communicated in the event?
- Who are the messages from the event for?
- Who will be responsible for recognizing, communicating, escalating and taking action on events?

The specific design areas related to Event Management include:

- Instrumentation.
- Error messaging.
- Event detection and alert mechanisms.

The instrumentation is about defining what can be monitored about individual configuration items and how their behaviors can be controlled. Design efforts will go into what decisions need to be made and what mechanisms must be in place to execute those decisions. Specific mechanisms include:

- How events are generated?
- How events are classified?
- How events are communicated and escalated?
- Is a standard feature of the monitored configuration item an event generation mechanism which can be leveraged and/or customized?
- What data will populate the event record?
- Where will events be logged and stored?
- How will supplementary data be gathered?
The design of IT components (hardware, software, network etc.) should support Event Management through the development of meaningful error messages and/or codes which clearly identify specific points of failure and likely causes. Current technologies provide basic tools for building appropriate solutions for managing and monitoring IT components and eliminate or reduce the need to include error messaging within the code.

Event Management design will also cover the tools used to filter, correlate and escalate events. Correlation engines allow the development of event rule sets: rules defining how the event messages will be processed and evaluated. Event detection and alert mechanism design will require the following knowledge:

- Business processes being managed through Event Management.
- Service level requirements of the service between supported by each configuration item.
- Who supports the configuration item(s).
- What constitutes normal and abnormal operation of the configuration item.
- Significance of multiple similar events on the same configuration item or several configuration items.
- What is required to support a configuration item effectively.
- Information needed to aid diagnosis of configuration item problems.
- Incident prioritization and categorization codes used to create incident records.
- Relationships between configuration items.
10.1.6 Elearning Module 6 & Workbook Review Questions

1. What Service Operation process is responsible for monitoring of normal operations and will detect and escalate abnormal behavior in service performance?
   a. Event Management
   b. Incident Management
   c. Problem Management
   d. Access Management

2. What does Event Management fundamentally allow the service provider to do?
   a. Resolve problems quickly and with minimal impact to the business
   b. Perform monitoring and control activities
   c. Demonstrate achievement of service level agreements
   d. Identify opportunities for improvement

3. Which of the following statements is not an objective of Event Management?
   a. Detect changes of state
   b. Determine appropriate control actions
   c. Increase visibility and communication of incidents
   d. Provides a means of comparing actual performance against designed performance

4. Which of the following is not typically monitored through Event Management?
   a. Data center temperature
   b. Security breaches
   c. State changes for configuration items
   d. Changes in Service Design
5. A scheduled workload has completed is what type of event?
   a. Informational
   b. Warning
   c. Exception
   d. Continuity

6. The utilization of a server’s disk drive is has reached 81% of capacity is what type of event?
   a. Informational
   b. Warning
   c. Exception
   d. Continuity

7. The existence of an unauthorized software install is what type of event?
   a. Informational
   b. Warning
   c. Exception
   d. Continuity

8. A formal process to evaluate the effectiveness of filtering is a key characteristic of what filtering strategy?
   a. Integration
   b. Design
   c. Trial and error
   d. Planning
9. Defining how to monitor and control the IT infrastructure and services is called what?
   a. Improvement
   b. Planning and design
   c. Service Management
   d. Instrumentation

10. Correlation engines are used for what purpose?
   a. To match relationships between configuration items and plausible events
   b. To match subsequent actions with certain types of events based on predefined rules and criteria
   c. To identify events from basic information provided through alerts and event rule sets
   d. To detect events and issue appropriate alerts to responsible persons as notification
10.1.7 Process Activities

Events occur all the time, but only those which are detected and registered will trigger Event Management. The determination of what events are detected or not is based on input from everyone involved in the design, development, management, and support of IT service.

Once an event occurs, some form of notification will be issued. While some notifications may be proprietary to the tool used to monitor the IT system, most configuration items will generate generic event notifications using an open standard like SNMP. Notifications can be initiated using two methods:

- A management tool polls a configuration item for targeted data.
- A configuration item generates a notification when certain pre-defined conditions are met.

The notification is a means of detecting the event; if the notification is not created, the event will not be detected. The notification also provides sufficient data to understand what the event is. The event and its details are then logged. An event record could be created in an Event Management tool or as an entry in the system log of the configuration item generating the event. If the latter method is used, those logs need to be regularly checked.

The first decision point of the Event Management process provides initial event correlation and filtering to determine if the event should be ignored or communicated to a management tool. An ignored event simply means that no additional action is required to respond to the event other than recording in the configuration item's log. One of the reasons for this initial step is that the event notification capabilities of a configuration item cannot typically be turned off; so a number of insignificant notifications may be received. Correlation engines residing on or connected to the configuration item will determine if the event notification pertains to an informational, warning or exception event.
If the event is informational, no more is required from Event Management. If the event is a warning, a second decision must be made regarding further action. If no further action is required, the Event Management process will end. If further action is required, five possible outcomes may exist:

- Automated response, such as performance tuning or system reboot.
- An alert to engage human intervention, such as close monitoring of the situation.
- Initiating Incident Management.
- Initiating Problem Management.
- Initiating Change Management.

From a process perspective, a review of events should occur to ensure the response to the event was sufficient and handled appropriately. Not all events need a formal review and most events can be reviewed automatically; for instance, polling a rebooted server to ensure the service is functioning properly. Additionally, reviews of events do not need to supersede or replace reviews initiated as part of incident, problem and Change Management processes, such as the post-implementation review.

At the end of the process, the event should be closed. In truth, events simply exist and are not “opened” or “closed.” So the concept of closing an event refers to closing the lifecycle loop of an event or any record of the event in an Event Management tool. If the event caused a record of an incident, problem or change to be opened, the closing of those records should automatically close the event record, if the response was appropriate as determined by the review.
10.1.8 Triggers, Inputs, and Outputs

Event Management will be triggered by the following events:

- Exceptions to performance of configuration items as defined in design specifications, operational level agreements, and standard operating procedures.
- Exceptions to automated procedures or processes.
- Exceptions to a business process being monitored by Event Management.
- Completion of any automated task or job.
- Any status change attributed to a service or database configuration item.
- User accessing an application or database (or access by automated procedure or job).
- A predefined performance threshold has been reached for any monitored device, database or application.

The inputs and outputs of design coordination are summarized in the following table:

<table>
<thead>
<tr>
<th>Inputs</th>
<th>Outputs</th>
</tr>
</thead>
<tbody>
<tr>
<td>Operational and service level agreements associated with events</td>
<td>Events communicated and escalated to those responsible for further action</td>
</tr>
<tr>
<td>Alarms, alerts and thresholds for recognizing events</td>
<td>Event logs</td>
</tr>
<tr>
<td>Correlation tables, rules, event codes and automated response solutions</td>
<td>Events initiating Incident Management</td>
</tr>
<tr>
<td>Roles and responsibility regarding who identifies and communicates events to those who handle responses to events</td>
<td>Events indicating a potential breach of an SLA or OLA</td>
</tr>
<tr>
<td>Operating procedures for recognizing, logging, escalating and communicating events</td>
<td>Events and alerts indicating completion status of monitored events</td>
</tr>
<tr>
<td></td>
<td>Event information and history recorded in SKMS</td>
</tr>
</tbody>
</table>
Event Management will interface with all Service Management processes to ensure they are monitored and controlled appropriately, especially those processes which do not require real-time monitoring, but require some intervention following an event or group of events, like IT Service Continuity Management. However, particular interfaces need to be established to ensure the smooth and effective execution of the Event Management process, including:

- Service Level Management – Event Management provides the necessary monitoring and communications to ensure any potential impact on SLAs are identified as soon as possible.
- Information Security Management – Event Management will monitor business applications and/or processes for abnormal activity which may indicate a potential security threat.
- Capacity Management – will define what events are significant, thresholds to monitor, and appropriate responses to events; Event Management will provide sufficient data and alerts to ensure improvement of the process’ capabilities to support IT services.
- Availability Management – will define what events are significant, thresholds to monitor, and appropriate responses to events; Event Management will provide sufficient data and alerts to ensure improvement of the process’ capabilities to support IT services.
- Service Asset and Configuration Management – Event Management can provide data regarding the current status of any configuration item, as well as any unauthorized changes in the environment.
- Knowledge Management – Event Management is a rich source of information.
- Change Management – Event Management can identify conditions which may require activity within the process.
- Incident Management – Event Management can identify conditions which may require activity within the process.
- Problem Management – Event Management can identify conditions which may require activity within the process.
- Access Management – Event Management can be used to identify unauthorized access attempts or security breaches.
10.1.9 Critical Success Factors and Key Performance Indicators

The following critical success factors and key performance indicators are samples related to Event Management. Each critical success factor has at least one key performance indicator which is used to demonstrate achievement of the CSF.

- All changes of state which are significant to the management of configuration items and IT services are detected:
  - Number and ratio of events against the number of incidents.
  - Number and percentage of events, by type, platform, or application versus the number of platforms and applications supporting IT services.
- All events are communicated to the appropriate functions who need to be informed or have a responsibility in taking any further action:
  - Number and percentage of events requiring human intervention and receiving it.
  - Number of incidents occurred and percentage of incidents triggered without a corresponding event.
- Effectively triggering the execution of Service Operation processes or operational management procedures:
  - Number and percentage of events requiring human intervention and receiving it.
- Establishing the means to compare actual operating performance behaviors against predicted standards from design specifications and service level agreements:
  - Number and percentage of incidents resolved without impact to business.
  - Number and percentage of events resulting in incident or change.
  - Number and percentage of events caused by existing problem or known errors.
  - Number or percentage of events identifying performance issues.
  - Number and percentage of events identifying potential availability issues.
- Establish the basis for service assurance, reporting and improvement:
  - Number and percentage of repeated or duplicated events.
  - Number of events/alerts generated within actual degradation of service/functionality (false positives).
10.1.10 Challenges and Risks

The challenges facing Event Management include:

- Obtaining sufficient funding for necessary tools and resources.
- Setting the correct level of filtering.
- Deploying monitoring agents across the entire IT infrastructure.
- Negative impact on network capacity levels, specifically from automated monitoring activities.
- Acquiring the necessary skills.
- Event Management tools deployed without appropriate processes to deploy, operate or adjust them.

Risks to Event Management include:

- Failure to obtain sufficient funding.
- Ensuring the right correct level of filtering.
- Failure to maintain momentum when deploying monitoring agents.
10.1.11 Elearning Module 7 & Workbook Review Questions

1. What Service Operation process is not typically invoked by Event Management?
   a. Incident Management
   b. Problem management
   c. Request fulfillment
   d. Access Management

2. What will trigger Event Management?
   a. Service request
   b. Request for change
   c. Change in state
   d. Opportunity for improvement

3. Which of the following is an output of Event Management?
   a. Roles and responsibilities for recognizing events and communicating them
   b. Document of event information and history in the SKMS
   c. Operational procedures for recognizing, logging, escalating and communicating events
   d. Operational and service level requirements associated with events

4. Why does Event Management interface with service level management?
   a. To ensure early detection of potential SLA breaches and failures which can be resolved with minimal impact to service targets
   b. To identify conditions that may need a response or action
   c. To detect unauthorized access attempts and security breaches
   d. To define what events are significant, the appropriate thresholds to monitor, and the correct responses when thresholds are met
5. What is an appropriate key performance indicator to demonstrate that all events are communicated to appropriate functions for further action?
   a. Number and percentage of incidents resolved without impact to the business
   b. Number and percentage of repeated or duplicated events
   c. Number and percentage of events that required human intervention and whether intervention was performed
   d. Number and ratio of events compared with the number of incidents

6. What is the primary disadvantage to automated monitoring?
   a. Influx of relatively insignificant events
   b. Negative impact on planned capacity levels of the network
   c. Acquiring the necessary skills to respond adequately to events
   d. Incomplete or missing processes can reduce the value of effort

7. Which of the following is not a risk for Event Management?
   a. Failure to obtain adequate funding
   b. Failure to obtain the correct level for filtering
   c. Failure to maintain momentum in deploying monitoring agents
   d. Failure to obtain necessary skills
10.2 Incident Management

An incident is defined as “an unplanned interruption to an IT service or reduction in the quality of an IT service or a failure of a configuration item that has not yet impacted as IT service” (Service Operation, page 72). In essence, an incident is any abnormal operation which prevents or could prevent the delivery or support of an IT service.

The process for Incident Management is designed to manage an incident through its lifecycle, starting with detecting and ending with a return to “normal” operation. Incident Management is distinguishable from Problem Management: Incident Management is concerned with returning the service to working order, while Problem Management is concerned with the root cause. The common scenario of a flat tire is a good analogy for the distinction: Incident Management would focus on replacing the flat tire with a good tire, while Problem Management would focus on what caused the tire to go flat in order to prevent another incident.

10.2.1 Purpose and Objectives

The purpose of Incident Management is two-fold:

- Return the service to normal working condition.
- Minimize any adverse impact from the incident on the business.

Normal working conditions, or Service Operation, refers to how the service should perform according to design and within the services agreed service and operational levels.
The objectives of Incident Management are:

- Standardize the methods and procedures used to respond, analyze, document, manage and report incidents efficiently and quickly.
- Increase visibility and communication of incidents to IT support staff and the customer/business.
- Provide a professional approach to managing and communicating incidents which enhances the customer/user’s perception of IT.
- Align Incident Management activities and priorities with the business.
- Maintain user satisfaction with the quality of IT services.

10.2.2 Scope

Any event which disrupts or could disrupt a service will invoke the Incident Management process. The process could be triggered by an alert from the Event Management process; but not all events are incidents. The most perceptive aspect of Incident Management occurs when users call the Service Desk to report an incident that they are experiencing; however, the Service Desk will also handle service requests which are not incidents. Technical staff may identify and report an incident; either by logging the incident themselves or contacting the Service Desk, based on the organization’s policy.

While most organizations recognize the need for Incident Management to manage disruptions to IT services delivered to the customer, the process can be used to record and manage any incident within the service lifecycle. For instance, if service testing during the transition is impacted because of a faulty component in the test environment, this can be logged as an incident. If during a change, a reconfigured system shuts down for no apparent reason, an incident has occurred. The scope of Incident Management needs to be determined by the organization.
10.2.3 Value to Business

What is the value of Incident Management to the business? Luckily, this process has often been highly visible to the business and therefore, its value is easily demonstrated. Because of this visibility, it is usually one of the first Service Management processes to be implemented, but it also provides the means of highlighting problem areas in other parts of Service Management. Unfortunately, Incident Management is sometimes seen as solely a process of the Service Desk and some of the hidden aspects of the process can be more difficult to justify.

In general, Incident Management allows the service provider and business to:

- Increase serviced availability by detecting and resolving incidents resulting in reducing downtime.
- Reduce unplanned labor and costs used to manage incidents.
- Align IT activity to real-time business priorities.
- Identify potential improvements to services.
- Identify additional service or training requirements.

10.2.4 Policies, Principles, and Basic Concepts

There are several pertinent concepts introduced through the Incident Management process. Because of its purpose and visibility to the customer, the process is one of the most controlled processes in ITSM. This is demonstrated most in the agreed response and resolution targets associated with incidents. Briefly, the time allocated to resolving an incident is typically based on the potential impact of the incident on the service environment and the criticality of the service being affected. Usually described as the severity of the incident, a disruption to a critical application during the peak for the business day would warrant a higher severity than a non-critical web page on the weekend. A higher severity simply means the incident must be resolved faster.
These time scales are often broken down into smaller agreed targets. Here are some common targets related to Incident Management:

- Response time to user call to Service Desk – 15 seconds.
- First call resolution of incidents/service requests by Service Desk – 80%.
- Average call time (for Service Desk) – 8-15 minutes.
- Response to escalated or queue incident – 10 minutes to 2 hours, based on severity.
- Resolution and closure of severity 1 incident – 2 hours.
- Resolution and closure of severity 4 incident – 24 hours.

Consider the following math for every 100 incidents. If every incident was a severity 4 incident, the allocated time to resolution would total 2,400 hours or just short of 14 weeks (if only one person was working incidents). If every incident was a severity 1 incident, the allocated time would be 1 ½ weeks. However, higher severity places more pressure on the organization, increases the potential mistakes made and will require more resources over time. The Service Desk alleviates much of this pressure, because with these targets it must resolve 80% of the incidents without escalation. Using the maximum average call time for the Service Desk, 80 incidents would be resolved in 20 hours with the remaining 20 incidents resolved within 40 hours.

The point of the calculations above is to demonstrate that Incident Management can take significant amounts of time and resources for service operation. The problem with the calculations above is the assumption that incidents occur linearly: the fact is, several unrelated incidents may occur simultaneously and sometimes at the most inconvenient times. Additionally, the calculations assume the work is being done by a single person; when in truth, Incident Management may be worked on by every person in the service organization, so it’s possible that 100 different people can take a single incident and all the work is done fairly quickly. For a small service provider, the total number of incidents identified in a single day may reach well over 1,000.

The underlying problem with Incident Management being the responsibility of multiple people in the organization is the level of consistency given to any given situation. Without any level of
standardization, two people work the same incident conditions will likely arrive at a different resolution, with diverse results over different time frames. One way to create more consistency in handling incidents is by introducing incident models.

For most of IT, incidents are rarely unique. This means that the conditions underlying a particular incident may be similar to a previously experienced incident and will likely occur again in the future: for instance, an application freezing when running a process. Incident models can predefine the steps to be taken when certain conditions are experienced. Below is a brief, common model for monitors that are not working:

- Check the light on the monitor.
  - a. If no light appears, the monitor has no power. Check power cords to ensure connection.
  - b. If the orange light appears, the monitor is not communicating with compute. Check connection to a computer.
  - c. If green light appears, the monitor has power and is connected to the computer; likely solution is replacing the monitor.

While this incident model is basic, it can be applied to most monitors, even across different manufacturers; though some manufacturers may have additional steps to suggest.

An incident model will include:

- The steps to be taken to handle the incident.
- The order of the steps, usually chronologically.
- Who should perform what steps?
- Any precautions to take before performing steps, such as backing up data.
- Expected time scales and thresholds for completing of actions.
- Escalation procedures (both horizontal and vertical escalation).
- Any evidence-preservation activities to take, particularly for security- or capacity-related incidents.
One particular type of incident model relates to major incidents: incidents which usually have the highest allocated severity. The definition of what constitutes a major incident must be agreed by the service provider and the customer, because major incidents are usually managed using a separate procedure from the normal Incident Management process. The most significant difference is the establishment of an incident manager and a major incident team, which is responsible for managing the incident to closure. A team is formed to ensure all aspects and concerns about the incident and its impact are addressed immediately. In some cases, the resolution to the incident requires understanding the root cause, so Problem Management may be executed simultaneously. To confuse matters even more, the resolution may require a significant change, so the Change Management process may be invoked. Because a major incident will have a significant impact on the business, a higher severity is assigned which means that the team has a shorter time to do all this work, usually 2 hours. The higher impact potential also requires a high level of communication between the team and the stakeholders affected.

Every incident has a lifecycle and the lifecycle is the same for every incident. Some incidents may move through their lifecycle much faster than others. Tracking an incident through its lifecycle means applying and reporting status of the incident within the incident record. The most common status codes used in Incident Management are:

- **Open** – incident has been identified and logged but has not been assigned to a support resource for resolution
- **In progress** – the incident is actively being investigated and resolved
- **Resolved** – a resolution has been applied by normal operation of the service has not be verified by the business or user
- **Closed** – normal Service Operation has been verified by the business or user and incident record has been closed
Understanding the above concepts, the following policies may be developed for Incident Management:

- The existence and status of incidents must be communicated to appropriate stakeholders in a timely and effective manner
- Resolution of incidents must be within time frames agreed between the service provider and business; and documented in appropriate SLAs, OLAs and underpinning contracts
- Customer satisfaction must be maintained at all times
- Processing and handling of incidents should be aligned with overall service levels and objectives
- All incidents are to be stored and managed in a single management system
- A standard classification schema will be applied to all incident and be consistent with the business enterprise
- Incident records are to be audited on a regular basis to ensure accuracy and appropriateness when handling incidents
- A common format and set of information fields should be used in all incident records
- A common and agreed set of criteria for prioritizing and escalating incidents should be established
10.2.5 Elearning Module 8 & Workbook Review Questions

1. What is the purpose of Incident Management?
   a. Ensure normal Service Operation is monitored appropriately and correct response is made when abnormal operation or failure occurs
   b. Ensure normal Service Operation is restored at the earliest possible point and minimize any negative impact on business operations
   c. Minimize the adverse impact of incidents on the business that are caused by underlying errors within the IT infrastructure
   d. Minimize the costs of responding to multiple incidents by ensuring first-line support has appropriate skills and knowledge to resolve incidents

2. What function is typically seen as the single point of contract for all incidents?
   a. Service Desk
   b. Operations Bridge
   c. Technical Teams
   d. Application Teams

3. Why is the demonstration of value from Incident Management so much easier than with other processes?
   a. Because Incident Management will minimize the impact of disruptions to the business
   b. Because Incident Management can be leveraged to identify opportunities for business improvement
   c. Because Incident Management is a highly visible process to the business
   d. Because Incident Management is usually the first process to be implemented
4. Which of the following is not typically a factor for determining how much time the organization is given to resolve an incident?
   a. Impact
   b. Priority
   c. Classification
   d. Location

5. Which of the following is not necessary to complete an adequate incident model?
   a. Steps to handle the incident
   b. Priorities and impact codes
   c. Time scales for completing actions
   d. Escalation procedures

6. Which of the following properly defines what a major incident is?
   a. An incident which will adversely impact a large number of people
   b. An incident which will adversely impact a critical business process or vital business function
   c. An incident with predefined criteria agreed by the customer and the service provider
   d. An incident which requires a collaborative effort from multiple technical teams to find an appropriate workaround

7. An incident that has been identified but not assigned to a support resource for resolution is considered in what state?
   a. Open
   b. In progress
   c. Resolved
   d. Closed
10.2.6 Process Activities

Incidents may be reported from a variety of sources, such as Event Management or the customer through mechanisms like a phone call or the web. One of the first steps when an incident is reported, is to validate whether the incident is truly an incident or not. It is possible that the report is really a service request or a change proposal. For instance, a user may complain that they cannot access an application and the reason is because they have been locked out and/or they need to reset their password. While this may be seen as a disruption to the person's day, it is not a disruption to the service and a password reset is a service request, not an incident. If the customer still cannot access the application after resetting the password, an incident may be identified.

Once an incident has been identified, it will be logged in the Incident Management tool; sometimes called a call tracking or call management tool. When creating a record, the incident will be categorized using a standard schema and prioritized according to agreed service requirements. At this point, the incident will either be considered a major incident or not: if it is, the major incident procedure is invoked immediately. This procedure may include similar steps as a normal incident, but executed at a much faster pace.

A normal incident will continue with an initial diagnosis. This will lead to three potential options:

- Functional (horizontal) escalation – the incident is passed on to a person or a group of people with the expertise and responsibility to resolve the incident, usually based on categorization.
- Hierarchical (vertical) escalation – the incident is passed on to management to become involved in the resolution, usually focusing on user satisfaction with the process.
- Resolution – a resolution is identified and sometimes tested.

Whether the person escalates the incident or attempts to find a resolution themselves, the resolution option will always be applied. If a resolution cannot be found for the incident, further escalation may be necessary until one is found. Once an appropriate resolution is found, it is applied and any recovery activities performed, such as recovery of data.
The next step is to seek verification from the business or user that the applied resolution was effective in returning the service to normal operations and closing the incident.

### 10.2.7 Triggers, Inputs, and Outputs

Incident Management will be triggered by the following events:

- Disruption in service identified and reported
- Potential disruption to service identified and reported

The inputs and outputs of Incident Management are summarized in the following table:

<table>
<thead>
<tr>
<th><strong>Inputs</strong></th>
<th><strong>Outputs</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Information and status on configuration items</td>
<td>Actions taken to achieve resolution and resolved incidents</td>
</tr>
<tr>
<td>Information on known errors and workarounds</td>
<td>Undated Incident Management records</td>
</tr>
<tr>
<td>Communication and feedback on incidents and symptoms</td>
<td>Updated classification of incidents to support Problem Management efforts</td>
</tr>
<tr>
<td>Communication and feedback on requests for change and releases to be implemented</td>
<td>Raising of problem records</td>
</tr>
<tr>
<td>Communication of events</td>
<td>Validation on non-recurrence of incidents where root cause have been found</td>
</tr>
<tr>
<td>Operational and service level objectives</td>
<td>Feedback on incidents related to changes and releases</td>
</tr>
<tr>
<td>Customer feedback on incident resolution activities</td>
<td>Identification of configuration items associated with or impacted by incidents</td>
</tr>
<tr>
<td>Agreed criteria for prioritizing and escalating incidents</td>
<td>Feedback from customers regarding satisfaction</td>
</tr>
</tbody>
</table>
## Inputs

<table>
<thead>
<tr>
<th>Feedback on level and quality of monitoring technologies</th>
</tr>
</thead>
</table>

## Outputs

| Incident and resolution history data used in identifying overall service quality |

The major interfaces for Incident Management are:

- **Service Level Management** – Incident Management plays a major role in achieving service targets and service level agreements by responding quickly to events that threaten that achievement, and even providing pertinent data for use in deciding relevant service improvements. SLM will define acceptable levels of work from which Incident Management operates, such as response times, impact definitions, and resolution times.

- **Information Security Management** – Incident Management provides an overall picture of the effectiveness of ISM through the data generated around security-related incidents.

- **Capacity Management** – Incident Management provides a trigger for performance monitoring; in turn, capacity management will develop workarounds for capacity and performance-related incidents.

- **Availability Management** – utilizes data from Incident Management to determine the availability of IT services.

- **Service Asset and Configuration Management** – provides data pertinent for identifying incidents and managing progress to resolution.

- **Change Management** – manages requests for change which are required to implement a workaround or resolution for an incident.

- **Problem Management** - will be invoked to identify the root cause of incidents, particularly those with a major impact, recurring, or with little information.

- **Access Management** – attempts to access without authorization or security breaches are considered incidents to be managed and data from these incidents are used for forensic investigations.
10.2.8 Critical Success Factors and Key Performance Indicators

The following critical success factors and key performance indicators are samples related to Incident Management. Each critical success factor has at least one key performance indicator which is used to demonstrate achievement of the CSF.

- Minimizing the impact of incidents to the business by resolving them as quickly as possible:
  - Mean elapsed time (per impact code) to achieve incident resolution or workaround.
  - Breakdown of incidents at each stage of the process.
  - Percentage of incidents closed by the service desk (commonly called First Call Resolution).
  - Number and percentage of incidents resolved remotely, without visit.
  - Number of incidents resolved without impact to the business (tied to the effectiveness of Event Management).

- Maintain IT service quality:
  - Total number of incidents (control measure).
  - Size of current incident backlog for each IT service.
  - Number and percentage of major incidents for each IT service.

- Maintain user satisfaction with IT service:
  - Average score on user/customer survey.
  - Percentage of satisfaction surveys answered versus number of surveys sent.

- Increase visibility and communication of incidents to business and IT staff:
  - Average number of contacts (service desk calls) from business users of incidents already reports
  - Number of business user complaints or issues regarding the content and quality of incident communications.

- Align Incident Management activities and priorities with the business:
  - Percentage of incidents handled within the agreed response time.
  - Average cost per incident.

- Increase business confidence in IT capabilities by using standardized methods and procedures for efficient and prompt response, analysis, documentation, ongoing management and reporting of incidents:
- Number and percentage of incidents incorrectly assigned.
- Number of percentage of incidents incorrectly categorized.
- Number and percentage of incidents processed per service desk agent.
- Number and percentage of incidents related to changes and releases.

**10.2.9 Challenges and Risks**

The challenges facing Incident Management are:

- The ability to detect incidents as early as possible.
- Convincing all staff (internal and external) that all incidents must be logged.
- Encouraging the use of self-help web-based capabilities.
- Insufficient availability in information about problems and known errors.
- Integration with a configuration management system to determine relationships between configuration items and obtain historical information about configuration items.
- Integration into the service level management process to correctly assess the impact and priority of incidents.

The risks associated with Incident Management include:

- Inability to handle incidents within acceptable time scales due to the lack of availability or properly trained resources.
- Unintended backlog of incidents due to inadequate support tools to raise alerts and encourage progress.
- Lack of adequate and/or timely information sources.
- Mismatches in objectives or actions because of poorly aligned or non-existent OLAs or underpinning contracts.
10.2.10 Elearning Module 9 & Workbook Review Questions

1. After what activity step is the major incident procedure engaged?
   a. Incident logging
   b. Incident categorization
   c. Incident prioritization
   d. Initial diagnosis

2. What is a primary rule of Incident Management?
   a. Every incident must be logged
   b. Every incident must be resolved
   c. Every incident must be closed
   d. Every incident must be prioritized

3. What is the most common route for triggering Incident Management?
   a. Event detected through IT Operations
   b. User call to the service desk
   c. Technical staff identifies abnormal behavior
   d. Suppliers notifies service provider of incident

4. Which of the following is an input to Incident Management?
   a. Raising of problem record
   b. Customer satisfaction survey
   c. Resolved incident or action to resolution
   d. Operational and service level objectives
5. Recurring incidents not resolved thoroughly by Incident Management would be handled by what Service Management process?
   a. Service level management
   b. Change Management
   c. Problem management
   d. Design coordination

6. What is a control measure for Incident Management?
   a. Total number of incidents
   b. Total number of closed incidents
   c. Number of incidents closed within agreed time frames
   d. Number of incidents closed satisfactorily
10.3 Request Fulfilment

In addition to responding to and resolving incidents, Service Desks are also capable of responding to user requests for services, or service requests. The variety of service requests from users is extreme and can include requests for information, access to a system, password resets, application installs, new hardware, and facility moves, to name a few. Like Incident Management, some of these requests can be fulfilled by the Service Desk, while others must be performed by a second-level support team: for this reason, it is dangerous to assume that Request Fulfillment is a Service Desk process.

At the same time, service requests are actually changing to how services are delivered and supported, but these changes are usually pre-defined and have very specific instructions for fulfilling the request. These are typically seen as standard changes, but not all standard changes will go through request fulfillment; however, some level of integration is required between Change Management and request fulfillment to ensure all changes are tracked appropriately.

10.3.1 Purpose and Objectives

The purpose of request fulfillment is to manage the lifecycle of all service requests from the user. The objectives of request fulfillment include:

- Through efficient and professional handling of service requests, maintain user and customer satisfaction.
- Provide a means for users to request and receive standard services which have a predefined authorization and qualification process.
- Provide information to users and customers about the availability of services and procedures for obtaining those services.
- Source and deliver the components of requests standard services.
- Assist with general information, complaints and comments.
10.3.2 Scope

The scope and handling of request fulfillment can vary from one organization to the next. First of all, the processes used to fulfill a particular request can vary based on what requests are accepted. When multiple request types are allowed, it is best to create request models for each type and store them in the service knowledge management system. Secondly, some organizations will use the same tool for request fulfillment and Incident Management and treat service requests as a type of “incident.” While there may be infrastructure advantages to this setup, incidents are unplanned events, whereas service requests can be and should be planned. Finally, the use of self-help web-based tools to handle user service requests has grown significantly and can impact how the organization performs request fulfillment structurally.

In some arrangements with the customer, request fulfillment may be extended to encompass non-IT service requests, such as photocopier repairs, procurement of office furniture, or even facility maintenance, such as electrical or plumbing problems. In these cases, the Service Desk will typically log the request and have appropriate OLAs in place with a customer-run support team outside of the IT department.

10.3.3 Value to Business

Request fulfillment provides value to the business in the following ways:

- Ability to provide quick and effective access to standard services use by the business to improve productivity or quality of business services and products.
- Ability to effectively reduce bureaucracy attributed to requesting and receiving access to new or existing services; which reduces the cost of providing those services.
- Ability to increase the level of control over requested services through the centralization of the fulfillment process, thus reducing the costs of providing services.
10.3.4 Policies, Principles, and Basic Concepts

Service requests will happen often: unlike Incident Management where it is desirable to decrease the number of incidents occurring, organizations are typically encouraged with increases in service requests. Like Incident Management, building confidence and consistency in handling user requests requires some standardization to be implemented. Request models allow the service provider to predetermine and document how different service requests will be handled. Luckily for the service provider, the type of service requests to be handled by the organization will typically be obvious and predefined in the Service Design stage and the models created as part of transitioning a new or changed service. For example, the deployment of a new application will always require request models for:

- Installing the application software.
- Access network resources for the application.
- Obtaining a username and password for service components.
- Password resets.
- Revoking access rights.
- Performing backup of application data.
- Uninstalling application software.

The growth and acceptance of the Internet have enabled the introduction of self-help tools and practices. While self-help tools can be leveraged for most of the Service Operation processes, they are highly effective for allowing users to make service requests. “Menu selection” is commonly used to describe what request options are available to users through these self-help tools. The methodology simply guides the user in requesting and providing details about the service requests by providing a series of predefined menus in the request form. This guided request process enables the service provider to control the request process and estimate the number of resources, time frames, and other IT concerns better.
Consider a service provider who has multiple customers in the form of business units. The support structure for customers has several shared services and a few custom services for individual business units. When using a self-help tool for user requests, the service provider needs to manage licenses and access to custom services, so they may need to control which options are seen by the user or provide a warning alert when the user attempts to request services they are not authorized or are unavailable to them. These restrictions may be based on the lack of licenses, the user’s location, business unit, or role/job in the organization.

Once a service request has been submitted, the next concern for the request fulfillment process is tracking the progress of the service request. Unlike an incident, a service request will typically have a few more stages to go through as indicated by different status codes, such as:

- Draft – request has been recorded but not submitted by the user at this time.
- Waiting authorization – the service request has been submitted for authorization: management, financial, etc.
- Rejected – the request has not been authorized and therefore rejected.
- In review – request has been authorized and currently under review by person or by group authorized to fulfill the request.
- Suspended – request fulfillment has been suspended, usually because of some level of coordination with other projects, plans, or service requests.
- Cancelled - the request is no longer required by the user.
- In progress – the request is being fulfilled.
- Completed - the request has been fulfilled but not verified with the user/requestor.
- Closed – user has agreed that the service request has been fulfilled and the request record has been closed.

The prioritization of service requests can utilize the same impact/urgency schema adopted in Incident Management. Service requests can also be escalated in a similar manner for both functional and hierarchical purposes.
Unlike incidents, service requests will typically require approval before moving forward with fulfillment, sometimes several approvals depending on the policies and the type of request. There are typically two types of approval a service request will be subjected:

- **Financial** – this approval simply acknowledges that the costs for providing the service will be covered as part of the agreement between the service provider and customer. For instance, the contract may stipulate a limited number of software licenses or facility moves to be provided per calendar period; if the number of service requests exceeds this contractual amount, the customer must agree to the additional costs to them. This step also supports the accounting activities managed in financial management for IT services.

- **Compliance** – also seen as business or management approval, this step will validate whether the user has the appropriate rights to the service(s) requests.

One of the decisions an organization may need to determine is the nature of service requests allowed. For instance, when a new employee is hired, will a single-service request be sufficient to ensure they have the appropriate IT resources or are several service requests required, each for a different service; or will the organization allow parent/child relationships between different requests. This is especially important where different parts of the request are fulfilled by different teams in the organization. Even with a simple application installed, the desktop team may be responsible for installing the application (or the user can pull from the self-help tool) and the service desk may need to setup the access rights to the application. In a facility move, some organizations will have very strict requirements on responsibilities, such as only IT personnel can move IT equipment, while non-IT equipment must be moved by a third-party moving company.

While the service desk is sometimes the defacto function for receiving service requests, if they are also involved in Incident Management, they may not be the appropriate people to coordinate fulfillment activities. In some organizations, a small section of the service desk function may be dedicated to request fulfillment: if so, they would perform the appropriate coordination. This “fulfillment desk” may not be part of the service desk function in some organizations.
Understanding these concepts will facilitate the organization’s ability to formulate policies regarding request fulfillment, such as:

- Fulfillment of requests must follow a predefined process flow (model) which identified the steps to take, responsible parties for fulfillment, target time scales and escalation paths.
- Ownership of service requests will reside with a centralized function which monitors, escalates, dispatches, and often fulfills the service request.
- Service requests that impact configuration items should be satisfied by implementing a standard change.
- All requests should be logged, controlled, coordinated, promoted and management though a single system.
- All requests must be authorized before they are fulfilled.
- Request fulfillment should proceed under an agreed set of criteria for determining priority which is aligned with overall service levels and objectives.
- Clear communications regarding requesting services and determining status of service request must be in place.
10.3.5 Elearning Module 10 & Workbook Review Questions

1. Which of the following is not an objective of the request fulfillment process?
   a. Assist with general information, complaints and comments
   b. Maintain user and customer satisfaction through efficient and professional handling of incidents
   c. Provide a channel for users to request and receive standard services
   d. Source and deliver the components of requests standard services

2. Requests models should be stored in what tool?
   a. Configuration management system
   b. Known error database
   c. Service knowledge management system
   d. Service catalog

3. What function will usually own and coordinate fulfillment of service requests?
   a. Service Desk
   b. IT Operations
   c. Technical Teams
   d. Application Teams

4. Self-help tools are primary mean of making service requests; what is a key consideration for the design of such tools to ensure users can provide consistent and accurate details about the request?
   a. Status tracking
   b. Escalation
   c. Request models
   d. Menu selection
5. What status code would be used to show that the user has communicated they no longer need access to a service?
   a. Suspended
   b. Cancelled
   c. Closed
   d. Rejected
10.3.6 Process Activities

The request fulfillment process is similar to the Incident Management process, largely because the Service Desk is typically responsible for both. Service requests will generally come from the user, either by contacting the service desk directly or submitting the request through a self-help tool or other predefined method (submitting a form). Once the request is received by the centralized function, the first question to ask is if the service request is really a request: it could be an incident, a change proposal, or a request that is not fulfilled by this process based on policy.

The received and accepted service request will then be logged into the appropriate management system and validated. Most efforts in validation simply ensure all the information in the request is complete and accurate. If the information is not, the request must be sent back to the user and the request placed on hold or suspended. When the information is completed and accurate, the request can be categorized and prioritized appropriately. This completes the logging of the request record.

From here, any approvals for the request are obtained. This typically requires the request to pass through the financial management and Access Management processes, who will update the record appropriately. If the request is not approved, it is considered rejected and sent back to the user. If the request is approved, the request goes to the person or group responsible for fulfilling the request, who will review the request and escalate if necessary. In some cases, one group may fulfill a part of the request and escalate to the next group per the instructions in the request model.

Fulfillment of the request will proceed according to the request model. If a configuration item will be impacted by the service request, the Change Management process must become involved, usually in the form of a standard change. This invocation of Change Management is largely dependent on how the organization defines “configuration item” and what configuration items are under the control of Change Management. For instance, are the access tables to an application or database managed as a configuration item? They might be if they are part of a critical and confidential system.
In some cases, the request may not be fulfilled: this is especially true if the request will have an adverse effect on the configuration item. At this point, the request will be sent back to the user or requestor. If the request has been fulfilled, the user should be contacted to confirm the fulfillment of their requests. At this point, the request record can be closed; however to complete the accounting process for financial management, a notification of fulfillment may need to be sent to the financial management process, which will initiate any charging appropriate to the requested service.

10.3.7 Triggers, Inputs, and Outputs

Request Fulfillment will be triggered by the following events:

- Request from user, either by calling the service desk or submitting request through a self-help tool or other predefined path.

The inputs and outputs of Request Fulfillment coordination are summarized in the following table:

<table>
<thead>
<tr>
<th>Inputs</th>
<th>Outputs</th>
</tr>
</thead>
<tbody>
<tr>
<td>Work requests</td>
<td>Authorized service requests</td>
</tr>
<tr>
<td>Authorization forms</td>
<td>Rejected service requests</td>
</tr>
<tr>
<td>Service requests</td>
<td>Request fulfillment status reports</td>
</tr>
<tr>
<td>Requests for change</td>
<td>Fulfilled service requests</td>
</tr>
<tr>
<td>Requests from various sources (phone calls, web interfaces, or email)</td>
<td>Incidents (rerouted)</td>
</tr>
<tr>
<td>Requests for information</td>
<td>Requests for change/standard changes</td>
</tr>
<tr>
<td></td>
<td>Updates to assets or configuration items</td>
</tr>
<tr>
<td></td>
<td>Updated request records</td>
</tr>
<tr>
<td></td>
<td>Closed service requests</td>
</tr>
<tr>
<td></td>
<td>Cancelled service requests</td>
</tr>
</tbody>
</table>
The major interfaces for Request Fulfillment are:

- Financial Management for IT Service – provides approval for service request should costs need to be reported and recovered.
- Service Catalog Management – ensures available service requests are well communicated to users and linked to services found in the service catalog.
- Release and Deployment Management – enables release packages to be predefined, built and tested for automatic deployment based on service requests.
- Service Asset and Configuration Management – will update configuration items to reflect changes made as part of fulfillment activities, as well as provides instructions for labelling and naming assets impacted by service requests, such as moves, adds and changes.
- Change Management – involved in service requests where a configuration item will be changed in order to fulfill the request.
- Incident and Problem Management – in addition to being performed in conjunction with Incident Management, request fulfilment must be invoked because of an incident or problem occurring in the environment and require the appropriate connections to be made.
- Access Management – validates the authority of those making service requests and those receiving services as part of a service request.

10.3.8 Critical Success Factors and Key Performance Indicators

The following critical success factors and key performance indicators are samples related to Request Fulfillment. Each critical success factor has at least one key performance indicator, which is used to demonstrate achievement of the CSF.

- Requests are fulfilled in an efficient and timely manner which is aligned with agreed service level targets for each type of request:
  - The mean elapsed time for handling requests for each service request type.
  - The number and percentage of service requests completed within agreed target times.
  - Breakdown of service quests at each stage.
  - Percentage of service requests closed by service desk without any additional escalation (known as First Call Resolution).
  - Number and percentage of service requests fulfilled remotely or through automated
methods.
  o Total number of resources (control measure).
  o The average cost per type of service requests.
• Only authorized requests are fulfilled:
  o Percentage of service requests fulfilled that were authorized appropriately.
  o Number of incidents related to security threats from request fulfillment activities.
• User satisfaction is maintained:
  o Satisfaction scores related to the handling of service requests.
  o Total number of incidents related to request fulfillment activities.
  o Size of current backlog of outstanding service requests.

10.3.9 Challenges and Risks

The challenges facing Request Fulfillment include:

• Defining and documenting clearly the type of requests handled by the request fulfillment process.
• Allowing users to interface successfully with the request fulfillment process using self-help front-end capabilities.
• Establishing clear service level targets for each type of request.
• Obtaining agreement for costs related to request fulfillment of each type of service requests.
• Standardizing services and who will be authorized to request them.
• Ensuring information about requests is available and easily accessible.
• Following a predefined standard fulfillment procedure for each type of request.
• Managing request fulfillment to ensure a high level of user satisfaction is maintained.
The risks commonly associated with Request Fulfillment include:

- Poorly defined scope where people are unsure what the process can or should handle.
- Poorly designed or implemented user interfaces.
- Badly designed or operated back-end fulfillment processes incapable of handling the volume or nature of the requests.
- Inadequate monitoring capabilities.
10.3.10 Elearning Module 11 & Workbook Review Questions

1. Which of the following conditions is not required to ensure a request is authorized?
   a. The person requesting is authorized to make requests
   b. The service being requested is appropriate for the user based on job responsibilities
   c. The request has appropriate financial and management approvals
   d. Request specifically asks for access and rights to a service

2. Who is most likely to initiate a service request?
   a. User
   b. Service Desk
   c. Technical team
   d. Supplier

3. Which of the following is not a valid source of service requests?
   a. Work requests
   b. Problem records
   c. Requests for change
   d. Requests for information

4. Request fulfillment will have similarities with what Service Management process in terms of how the process is executed?
   a. Change Management
   b. Access Management
   c. Release and Deployment Management
   d. Incident Management
5. What key performance indicator is sometimes referred to as first point of contact measurement or first call resolution?
   a. Number and percentage of service requests completed within agreed target times
   b. Percentage of service requests closed by the service desk without reference to other levels of support
   c. Total number of service requests
   d. Number and percentage of service requests resolved remotely or through automation
10.4 Problem Management

A problem is “the underlying cause of one or more incidents” (Service Operation, page 97). While Incident Management is designed to prevent any impact from an incident, Problem Management serves to understand this underlying cause and prevent the incident itself, or at least provide the best possible response. Though most problems will be related to an incident, Incident Management will not initiate Problem Management in all cases. For example, a process owner may utilize Problem Management as a means of discovering why a process is inefficient.

10.4.1 Purpose and Objectives

The purpose of Problem Management is to manage the lifecycle of a problem from initial identification to eventual resolution of the problem. Problem management seeks to minimize the adverse impact of incidents and problems on the business and to proactively prevent the recurrence of incidents related to the underlying errors in the IT environment.

The objectives of Problem Management are:

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

10.4.2 Scope

The activities of Problem Management will be to diagnose the root cause of incidents and determine the resolution to problems. The process will document and communicate those resolutions in the form of a known error database, which can be used in the environment to respond to recurring incidents which were not eliminated. While Incident Management and Problem Management are separate processes, they may utilize the same management tools, categories, priorities, and impact coding system.
The process for Problem Management can be used reactively or proactively.

- Reactive Problem Management will solve problems related to one or more incidents.
- Proactive Problem Management will identify and solve problems and known errors before related incidents can occur.
- Proactive Problem Management will be conducted as part of improving the overall availability and user satisfaction with IT services.
- The question, “How can recurrence be prevented” in a major incident review can trigger Problem Management as the answer requires an understanding of the underlying cause.
- Problems may be identified as part of conducting scheduled reviews of operational logs and maintenance records identifying patterns and trends of activities or event logs to identify patterns and trends of warning and exception events.
- Problems may be identified through conducting brainstorming sessions to identify trends.
- Detection of problems can be supported by using check sheets to collect data on service or operational quality issues.

10.4.3 Value to Business

Problem management provides value to the business by reducing the number and duration of incidents that service may incur, thus increasing service availability. Productivity can also be affected as the unplanned labor associated with incidents can be greatly reduced, primarily by eliminating the root cause or creating a resolution plan for recurring incidents. Problem management can reduce costs by ensuring workarounds or resolutions to problems truly work or though establish solid instructions for handling incidents generically or based on incident type.

10.4.4 Policies, Principles, and Basic Concepts

Like with many of the processes in the Service Operation stage, Problem Management encourages the creation of problem models which are standardized approaches to handling different problems. Unlike the other processes, the creation of the problem models is actually part of the process; the workarounds and resolutions to known errors discovered in Problem Management and documented within the Known Error Database are problem models. The Known Error Database is essential for the
effectiveness of Service Operation and Incident Management as it provides valuable information for handling known errors.

Problem models are different from incident models, though they may be used as part of the incident model to quickly diagnose and resolve an incident. However, the focus of Incident Management is to mitigate the impact of an incident on the business, whereas Problem Management seeks to find the root cause and eliminate it. A traffic cop will mitigate the impact of an accident by directing traffic, but a detective will be called upon to identify the cause of the accident. Everyone has their role.

In practice, incidents will often initiate Problem Management, though the rules for initiating the process can vary and are at the discretion of the organization. Some general reasons for invoking Problem Management include:

- An incident cannot be matched to an existing problem or known error.
- Trend analysis of several incidents indicates a possible root cause.
- An occurrence of a major incident where a root cause must be identified.
- A problem condition has been identified by another IT function.
- A resolved incident has not clear cause and the likelihood of recurrence is high.
- Analysis on an individual incident identifies the possibility of an underlying cause.
- Supplier has notified the service provider that a problem which needs to be resolved exists.

The methodology of problem analysis, diagnosis and resolution has a number of tools and techniques available; some are used with great success in an organization and others are ignored.
The use of these tools are at the discretion of the organization, individual preferences, and the intended outcome of the effort they are applied. These techniques include:

- **Chronological Analysis** – all events related to the problem are documented in chronological order to easily determine what happened and when.

- **Pain Value Analysis** – an in-depth analysis of the impact on the business, from the incident or problem, in order to clearly understand the problem. Results may include the number of people affected, the duration of the downtime, and the cost to the business.

- **Kepner and Tregoe** – a systematic method of analysis to determine deeply rooted causes of problems and incidents. The technique involves the following steps:
  
  1. Define problem.
  2. Describe problem in terms of identity, location, time and size.
  3. Establish possible cause.
  4. Test most probable cause.
  5. Verify true cause.

- **Brainstorming** – a group effort where possible causes are identified without editorializing; the technique can be very constructive and innovative when done properly.

- **5-WHYs** – a simple approach to finding the root cause which requires the analyst to question their own conclusion with some form of “why” question: the approach suggests that an average of five iterations of questions are required to reach a valid conclusion.

- **Fault Isolation** – this technique recreates the events of the problem in order to identify where the problem is located. This technique is especially helpful when the problem impacts a known value chain.

- **Affinity Mapping** – the technique will organize large amounts of data into groups with common characteristics.

- **Hypothesis Testing** – a list of possible root causes is generated based on educated guests and are tested individually to determine if they are the actual cause.

- **Technical Observation Post** – for incidents which recur intermittently, a group of technical specialists may be formed to monitor events in real-time to determine and identify the specific situation where the problem occurs and identify possible causes.

- **Ishiwaka Diagrams, or Fishbone Diagrams** – a means of documented causes and effects used in quality control to identify where problems may exist and be improved.
• Pareto Analysis – a method of organizing potential causes of failures based on probability: also called the 80/20 method.
• As with most processes, Problem Management has several policy concerns to be addressed by the organization, including:
  • Problems should be tracked separately from incidents.
  • All problems should be stored and managed in a single management system.
  • All problems should subscribe to a standard classification schema consistent with the business enterprise, particularly Incident Management.

One point of clarification: not all problems will be resolved. Identifying a resolution and implementing a resolution is a major step for organizations. In some cases, the resolution for the problem may cost more than the loss experienced by the business by the problem. In this situation, the business may decide to absorb the risk and not put a resolution in place: however, they will usually establish an agreeable workaround and monitor the situation closely in the future to ensure the problem does not grow.
10.4.5 Elearning Module 12 & Workbook Review Questions

1. Which of the following statements is not an objective of Problem Management?
   a. Prevent problems and resulting incidents from happening
   b. Eliminate recurring incidents
   c. Minimize the impact of incidents that cannot be prevented
   d. Maintain user satisfaction with the quality of IT services

2. Which of the following activities is an example of reactive Problem Management?
   a. Identifying and solving problems and known errors before further incidents occur again
   b. Solving problems in response to one or more incidents
   c. Improve the overall availability and end user satisfaction with IT services
   d. Conducting periodic schedule reviews of operational logs and maintenance records

3. Which of the following is not a value provided by Problem Management to the business?
   a. Ensure IT services remain continuously aligned to business requirements
   b. Higher service availability by reducing the number and duration of incidents
   c. Higher productivity of IT staff by reducing unplanned labor
   d. Reduced costs of implementing workarounds or resolutions that do not work

4. From a policy perspective, what should Problem Management share with Incident Management to drive consistency in service delivery?
   a. Record management technology
   b. Staffing resources
   c. Standard classification schema
   d. Process ownership
5. Which of the following is not a trigger for proactive Problem Management?
   a. Incidents
   b. Incident reports
   c. Trending
   d. SLA reviews

6. Problem models are most likely to be documented in what Service Management convention?
   a. Configuration Management System
   b. Service Catalog
   c. Information Security Management System
   d. Known Error Database
10.4.6 Process Activities

Problem management can be initiated through Incident Management and the Service Desk, or by a supplier or Event Management; many of the Service Management processes may identify a potential problem as part of their proactive efforts. Once a problem has been detected, it will be documented or logged in the appropriate system. When creating the problem record, the problem will be categorized and prioritized based on a standard schema developed by the organization.

From this point, the investigation and diagnosis of the problem can proceed. Any of the techniques identified in the previous section can be used and the effort can be done by an individual or a group. Information from the configuration management system is vital at this step because the data provide current and historical context to the problem. The end of this step is the identification of the problem’s root cause.

In some instances, a workaround is still required by Incident Management; particularly if Problem Management was invoked in the middle of a major incident. If a workaround is required, Problem Management will provide one. Remember that workarounds allow the business to continually operate while the problem is still persistent. For some incidents, a workaround is the best option given the time frame, costs, and priorities of the business regarding the business.

A vital step to Problem Management is raising a known error record. A known error documents the findings from the investigation and diagnosis of the problem and communicates the agreed workaround and potential resolutions to the problem. This information is used to support planning initiatives, service improvements, and Incident Management.

The actual resolution of a problem may require a change to a configuration item and this requires a request for change. Therefore, the implementation of the problem resolution is managed by Change Management, but the problem record needs to remain open until the change has completed and the effectiveness of the resolution has been verified. If the problem has not been resolved by the
change, further investigation and diagnosis is required and the process is repeated. However, because some effort has already been made, the priority assigned to the problem may change based on the organization’s guidelines. For instance, a lower priority may justify a single investigator into the problem while a high priority demands the efforts of a group.

If a resolution has been implemented and verified, the problem record may be closed, but the Problem Management process may still continue. The organization’s priority system will identify major problems and a review of those problems may be initiated to determine any lessons learned, specifically:

• What was done correctly?
• What was done incorrectly?
• What can be done better?
• How can recurrence be prevented?
• Who was responsible for what?
• What follow-up actions are required?

These questions can be applied to the Problem Management process or the process from which the problem occurred. The intention is to learn more and identify any opportunities for improvement in the service environment.

10.4.7 Triggers, Inputs, and Outputs

Problem Management will be triggered by the following events:

• In reaction to one or more incidents.
• Suppliers communicating potential faults or known deficiencies in their products or services.
• Identification of patterns or trends pertinent to managing individual Service Management processes and services.
The inputs and outputs of Problem Management are summarized in the following table:

<table>
<thead>
<tr>
<th>Inputs</th>
<th>Outputs</th>
</tr>
</thead>
<tbody>
<tr>
<td>Incidents records</td>
<td>Resolved problems and actions taken to achieve resolutions</td>
</tr>
<tr>
<td>Incident reports and histories</td>
<td>Updated Problem Management records</td>
</tr>
<tr>
<td>Configuration item information and status</td>
<td>Requests for change to remove infrastructure errors</td>
</tr>
<tr>
<td>Communication and feedback about incidents and their symptoms</td>
<td>Workarounds for incidents</td>
</tr>
<tr>
<td>Communication and feedback about requests for services and releases</td>
<td>Known error records</td>
</tr>
<tr>
<td>Communication of triggered events</td>
<td>Problem management reports</td>
</tr>
<tr>
<td>Operational and service level objectives</td>
<td>Output from major problem reviews</td>
</tr>
<tr>
<td>Customer feedback on success of problem resolutions and overall quality of Problem Management activities</td>
<td>Improvement recommendations</td>
</tr>
<tr>
<td>Agreed criteria for prioritizing and escalating problems</td>
<td></td>
</tr>
<tr>
<td>Risk management and risk assessment outputs</td>
<td></td>
</tr>
</tbody>
</table>

The major interfaces for Problem Management are:

- Incident Management – primary process interface as discussed in detail above.
- Financial Management for IT Services – assess the impact of proposed resolutions and workarounds from a financial perspective, as well as contribute to pain value analysis.
- Availability Management – responsible for determining how to reduce downtime and increase uptime, which requires leveraging the Problem Management process.
- Capability Management – capacity management teams and techniques are usually leveraged by Problem Management during investigations and assessing proactive measures.
• IT Service Continuity Management – may be invoked by Problem Management should a significant problem not be resolved before it starts to have a major impact on the business.
• Service Level Management – Problem Management contributes to improvement in service levels and will provide pertinent information for use in SLA reviews.
• Change Management – will utilize Problem Management to resolve problems caused by failed changes and Problem Management will use Change Management to ensure that any workaround or resolution impacting a configuration items will be implemented through a request for change.
• Service Asset and Configuration Management – identifies faulty configuration items and information regarding the potential impact of problems and resolutions.
• Release and Deployment Management – responsible for deploying problem fixes into the live environment and assists in the development and submission of known errors associated with new or changed services.
• Knowledge Management – the Known Error Database may be a component of the service knowledge management system.
• Continual Service Improvement – incidents and problems are the basis for identifying opportunities for improvement and adding to the CIS register.

10.4.8 Critical Success Factors and Key Performance Indicators

The following critical success factors and key performance indicators are samples related to Problem Management. Each critical success factor has at least one key performance indicators which is used to demonstrate achievement of the CSF.

• Incidents which cannot be prevented will have their impact of the business minimized:
  o The number of known errors added to the known error database.
  o The percentage accuracy of the known error database.
  o Percentage of incidents closed by the service desk without further escalation.
  o Average resolution time for incidents linked to problem records.
• IT service quality will be maintained through the elimination of recurring incidents:
  o Total number of problems (control measure).
  o Size of current problem backlog for each IT service.
Number of repeat incidents for each IT service.

- Business confidence in IT capabilities is maintained through the overall quality and professionalism of handling problems:
  - The number of major problems (in each stage, including closed).
  - Percentage of major problem reviews successfully performed.
  - Percentage of major problem reviews completed successfully and on time.
  - Number and percentage of problems incorrectly assigned.
  - Number and percentage of problems incorrectly categorized.
  - Backlog of outstanding problems and trends.
  - Number and percentage of problems exceeding target resolution times.
  - Percentage of problems resoled within SLA targets.
  - Average cost per problem.

### 10.4.9 Challenges and Risks

The challenges facing Problem Management are:

- Effective Incident Management process and tools.
- Skills and capabilities of problem resolution staff to identify the true root cause of incidents.
- Ability to relate incidents to problems, particularly when using different systems.
- Ability to integrate Problem Management activities with the configuration management system.
- Ensuring all knowledge and Service Asset and Configuration Management resources available are used to investigate and resolve problems.
- Ensuring ongoing training of technical staff.
- Good working relationship between all lines of support staff.
- Ensuring that business impact is understood by those people developing problem resolutions.
The risks associated with Problem Management include:

- Lack of available or properly trained resources to handle influx of problems.
- Inadequate support tools for the investigation, preventing progress in the problem process
- Lack of adequate or timely information sources.
- Improper training of problem support staff.
- Poorly aligned or non-existent OLAs and underpinning contracts.
10.4.10 Elearning Module 13 & Workbook Review Questions

1. What step in Problem Management does the configuration management system support?
   a. Problem detection
   b. Problem prioritization
   c. Problem investigation and diagnosis
   d. Problem resolution

2. Which of the following is an output of Problem Management?
   a. Known errors
   b. Operational and service level objectives
   c. Incident records
   d. Configuration item information

3. What process is responsible for implementing problem fixes into the live environment?
   a. Problem management
   b. Change Management
   c. Service-step improvement process
   d. Release and Deployment Management

4. How is the accuracy of the known Error Database determined?
   a. Usefulness of the records
   b. Audits performed on the database
   c. Editorial reviews by subject matter experts
   d. The percentage of incidents prevented
5. The effectiveness of Problem Management is highly dependent on what being implemented?
   a. Effective Incident Management process and tools
   b. Skills and capabilities of problem resolution staff
   c. Effective Change Management process and tools
   d. Integration of Problem Management with CMS
10.5 Access Management

Access Management is sometimes referred to as Rights Management or Identity Management.

10.5.1 Purpose and Objectives

Access Management is seen as the executor of the information security management policies. The process’s sole purpose is to ensure those people who have the right to use a service or group of service have the appropriate access to those services.

The objectives of Access Management are:

- Manage access to services based on policies and actions defined in information security management.
- Respond to requests for granting, changing, restricting or revoking access to services.
- Monitor service access to ensure rights are not improperly used.

10.5.2 Scope

Access Management is performed by all functions within the service environment, though the Service Desk may provide a single point of coordination. Access Management can be initiated by a service request. The process is essentially the execution of the information security policies.
10.5.3 Value to Business

The value provided by Access Management includes:

- Controlled access to services, which in turn maintains effective confidentiality of information for the business.
- Ensures employees have the right level of access to be productive in their assigned jobs.
- Reduces errors in data entry or use of critical service by persons not skilled or familiar with the systems.
- Enables auditing of service user and trace abuse of services.
- Provides capabilities to revoke access rights in a timely manner.
- Provides and demonstrates compliance with regulatory requirements.

10.5.4 Policies, Principles, and Basic Concepts

The policies found with Access Management may include:

- The information security policy-defined policies and controls will guide and direct Access Management administrative activities.
- Access to services should be logged and tracked to ensure rights provided are used appropriately.
- Access to services should be maintained in alignment with changes in personnel, including transfers and terminations.
- Access Management should maintain a historical record of who has accessed, or attempted to access, services.
- The handling, escalating and communicating of service events should be clearly defined and documented as procedure(s) in accordance with the information security policy.

The services from which Access Management is responsible for providing and managing access are those services found in the service catalog. Access refers to the level and extent of the functionality, or data of the service for which a user is entitled. Access is based on the user’s identity, which distinguishes as an individual and verifies their status in the organization.
A user may have different rights, or privileges, from their contemporaries. Rights define different levels of access and are usually associated with read, write, execute, change and delete privileges. Most users are not restricted to one service and a group of users may require access and the same rights to a particular service. Therefore, organizations may organize services and users into defined administrative groups: this allows the organization to provide access by associating the user with the appropriate group(s).

Directory services are specific types of tools used to manage access and rights for services and users.
10.5.5 Elearning Module 14 & Workbook Review Questions

1. Access Management is closely tied to what Service Management process in terms of fulfilling policy requirements?
   a. Information security management
   b. Request fulfillment
   c. Incident Management
   d. Change Management

2. Which of the following is not an objective of Access Management?
   a. Manage access to services passed on security policies
   b. Information is observed by or disclosed to only those people who have the right to know
   c. Respond to requests for granting access of changing access rights
   d. Oversee access to services and ensure proper use of that access

3. Access Management is initiated by what process device?
   a. Incident
   b. Request for change
   c. Release
   d. Service request

4. In what area does Access Management not provide value to the business?
   a. Access control
   b. Compliance
   c. Configuration information
   d. Auditability of service use
5. The actual settings that user access establishes are defined by what principle?
   a. Authorization
   b. Identity
   c. Rights
   d. Service groups
10.5.6 Process Activities

A request for access can be received as part of a service request, request for change, human resources’ request, or application script. Once a request has been received, both the user and the request must be verified. User verification simply ensures that the user has the right to make the request, typically because they are an employee of the business or under contract with the business. Request verification ensures the requested access and access rights are appropriate for the person based on their role or job position.

If both verifications pass, action is taken based on the request, which can include:

- Adding access.
- Increasing access rights.
- Restricting access rights.
- Revoking access.

Until access is given, the request will be monitored until with appropriate updates to the request record. Upon access being provided, Access Management will continue to monitor the user’s access to the system through logs and tracking mechanisms. This ensures the access is used according to policy and not abused. If an incident occurs, such as a security breach, Incident Management will be engaged.

The entire Access Management process is reliant on the information security management process and information found in the security management information system.
10.5.7 Triggers, Inputs, and Outputs

Access Management will be triggered by the following events:

- Service Request.
- Request for change.
- Request from human resources.
- Request from a manager.

The inputs and outputs of Access Management are summarized in the following table:

<table>
<thead>
<tr>
<th>Inputs</th>
<th>Outputs</th>
</tr>
</thead>
<tbody>
<tr>
<td>Information Security Policies</td>
<td>Access provided to IT services in accordance with policy</td>
</tr>
<tr>
<td>Operational and service level requirements related to granting access to services, Access Management administrative activities and response to access-related events</td>
<td>Access Management records and history of access granted to services</td>
</tr>
<tr>
<td>Authorized requests for change</td>
<td>Access Management records and history of access being denied to services, with reason for denial</td>
</tr>
<tr>
<td>Authorized request to grant or terminate access and access rights</td>
<td>Communications regarding inappropriate access or abuse of services</td>
</tr>
</tbody>
</table>
The major interfaces for Access Management are:

- **Demand Management** – identifies the necessary resource levels required to handle expected volumes for requesting access.
- **Strategy Management for IT Services** – determines whether Access Management will be performed within individual business functions or as a centralized function.
- **Information Security Management** – develops the policies and tools required to execute Access Management.
- **Service Catalog Management** – identifies and maintains information about the services within scope of the Access Management process.
- **IT Service Continuity Management** – manages access to services in the event of a major business disruption, particularly access to alternative solutions.
- **Service Level Management** – maintained the agreements for access to each service.
- **Change Management** – controls the actual requests for access.
- **Service Asset and Configuration Management** – identifies the data storage and will interrogate configuration items to determine current details regarding access.
- **Request Fulfillment** – provides the means for users to request access to standard services.

### 10.5.8 Critical Success Factors and Key Performance Indicators

The following critical success factors and key performance indicators are samples related to Access Management. Each critical success factor has at least one key performance indicator, which is used to demonstrate achievement of the CSF.

- **Protect the confidentiality, integrity and availability of services in accordance with the information security policy:**
  - Percentage of incidents that found inappropriate security access or attempts to access services.
  - Number of audit findings that found incorrect access settings for users because of job transfers or termination.
  - Number of incidents requiring reset of access rights.
  - Number of incidents caused by incorrect access settings.

- **Provide appropriate access to services in a timely manner that meets business requirements:**
• Percentage of requests of access which were provided within established SLA/OLAs.
  • Provide timely communication about improper access or abuse of services:
  • Average duration of access-related incidents.

10.5.9 Challenges and Risks

The challenges facing Access Management include:

• Monitoring and reporting access activity as well as incidents and problems related to access.
• Verifying the identity of the user.
• Verifying the identity of the approving person or group.
• Verifying user qualification for access to a specific service.
• Linking multiple access rights to individual users.
• Determining status of users at any time.
• Managing changes to user’s access requirements.
• Restricting access rights to unauthorized users.
• Building and maintaining a user database and the rights that they have been granted.

The risks associated with Access Management include:

• Lack of appropriate technologies to manage and control access.
• Controlling access from “back door” sources.
• Managing and controlling access using external third-party suppliers.
• Lack of management support for Access Management.
• Ensuring the necessary levels of access and controls are provided in a manner that is not detrimental to the business.
10.5.10 Elearning Module 15 & Workbook Review Questions

1. Incident management is invoked when?
   a. A service request is made
   b. A security incident occurs
   c. A user is given access
   d. A problem with access is found

2. Which of the following is not a valid trigger of Access Management?
   a. Request from human resources
   b. Service request
   c. Request for change
   d. Change proposal

3. Which of the following is not an output of Access Management?
   a. Provision of access to IT service
   b. Communications concerning inappropriate abuse of services
   c. Authorized requests for change to access services
   d. History of access granted or denied to services

4. What does Service Catalog Management provide to Access Management?
   a. Methods and means by which users can access IT services and service descriptions
   b. Expected volumes of requests for access
   c. Controls the actual requests for access
   d. Methods and means by which users can request access to standard services
5. The critical success factor, timely communication about improper access or abuse of services, is supported by what key performance indicator?
   a. Average duration of access-related incidents
   b. Percentage of requests for access provided within established service targets
   c. Number of incidents caused by incorrect access settings
   d. Percentage of incidents involving inappropriate security access
11 Service Operation Activities

Most Service Operation activities are routine day-to-day activities across the entire spectrum of IT services. While the extent of the activities covered in this chapter may depend on what the organization actually provides as its services, it is important to not be surprised by “hidden” support requirements: for instance, the existence of a server will require both server and network support and the existence of a database will require a database and storage support.

A goal of Service Operation is to raise the maturity of the organization as quickly as possible. Maturity is defined as “a measure of the reliability, efficiency and effectiveness of a process, function, organization, etc.” (Service Operation, page 331). There are typically five stages attributed to any maturity model. In ITSM, the lower maturity stages generally focus on technological aspects of the environment, including what technology is used, control of that technology, and integration. The upper stages are concerned with what the services provide the business and strategic contribution of IT. To provide value to the business, technology concerns need to be addressed, but they are done so in the context of supporting the business, not simply because it is required to manage the technology.

The role of technology managers will change depending on how mature the organization is. For example, in a technology-driven organization (level 1), the following conditions may be in place:

- IT is driven by technology.
- Most initiatives focus on understanding the infrastructure and dealing with exceptions.
- Technical experts perform technology management because they are the only people who understand how to manage each device or platform.
- Incidents drive most teams.
• Improvements focus on making management of the service easier, not the services themselves.
• Technology specializations are entrenched and integration between groups is not encouraged.
• Management tools focus on managing single technologies and are often duplicated.
• Incident Management is very immature

In technology controlled environments (level 2), the conditions may be:

• Most initiatives focus on achieving control and increasing infrastructure stability.
• Most technology components have been identified and the entire support staff has an understanding why the technology is used.
• The achievement of high performance from each component is the focus of technical management.
• Availability of components is measured and reported.
• The organization performs reactive Problem Management and inventory control.
• “Mission-critical” components are under change control.
• Point solutions are used to automate processes, usually concentrating on platform.

Technology integration (level 3) that the following characteristics:

• Critical services and their technology dependencies have been identified.
• Integration of systems are made to achieve required performance, availability and recovery of those services.
• Focus is on measuring performance across multiple devices an platforms.
• Configuration and asset data will have a virtual map to enable a single Change Management process for operations.
• Some services will consolidate availability and capacity planning.
• Disaster recovery planning is integrated.
• Cost savings are reached by integrating systems effectively.
Level 4 maturity (Service provision) will have the following characteristics:

- Services are quantified.
- Initiations focus on delivering agreed service levels.
- Procurement is driven by service requirements and technology constraints.
- Performance requirements and operational norms are defined by Service Design.
- Consolidated systems will support multiple services.
- All technology is mapped to services.
- All technology is managed to service requirements.
- Change Management is used in both development and operation of services.

Level 5 maturity organization (Strategic contribution) will have the following characteristics:

- IT is measured according to its business contribution.
- All services are measured based on their value provision
- Investment and performance targets are driven by the service portfolio.
- Technologies expertise is entrenched in everyday operations.
- IT is perceived as an utility of the business.

Service operation activities can be a litmus test for discovering the maturity level of the organization. For instance, a mature organization will see the activities as a “means to an end” rather than the end themselves: that is, the activities are mapped to the achievement of business objectives. In this respect, any activity that cannot be mapped appropriately is regarded as unnecessary. Additionally, the presence of an activity does not make an organization mature, more like the effectiveness of the activity: for example, procurement requests may already require some justification based on service requirements, but the organization may still be at a lower maturity if procurement requests which do not support service requirements are approved, or the service requirement are not priority strategically.
Service operation activities are not organizationally restrictive. While some organizations may choose to have different departments support different technologies or platforms, there is no “perfect” organizational structure to recommend. Discussed in this chapter are not organization-specific or maturity-specific activities, but are listed because they will be present in some form or another in any IT organization. Some activities may be specific to a single group while others are performed by multiple groups.

11.1 Monitoring and Control

Effective ITSM requires measurement and control of the service which is derived by an appropriate level for monitoring, reporting and response. While monitoring and control efforts are an activity of Service Operation, it is also the basis for setting strategy, designing and testing services and improving the service environment. Monitoring also provides the organization with the foundation for measuring and achieving service level targets.

Monitoring is simply the activity of “observing a situation to detect changes.” Within the context of Service Operation, monitoring refers to:

- The use of tools to monitor configuration item status and key operational activities.
- Ensuring the achievement of specified conditions and raising alerts when those conditions are not met.
- Ensuring the performance or utilization of a component is within a specified range.
- Detecting abnormal levels of activity in the infrastructure.
- Detecting unauthorized changes.
- Ensure compliance with organizational policies.
- Track outputs to business and ensure those outputs meet quality and performance expectations.
- Track information used to measure key performance indicators.
Reporting is the effort of analyzing, producing and distributing the output of monitoring: it includes the following activities:

- The use of tools to collate monitoring information to be distributed to various groups, functions or processes.
- Interprets the meaning of the information provided by monitoring.
- Determines where the information would benefit the business.
- Ensures decision makers have access to the information.
- Ensures the appropriate person, group or tool has the reported information.

Control is the process of managing the behavior of the device, system or service being monitored. If an unwanted change is detected during monitoring, control mechanisms can be initiated to correct the change before it has a significant impact on the service. For a control to be effective, it must have:

- A defined standard or norm for which the monitored system must conform.
- The conditions for taking action are clearly defined, understood, and confirmed.
- Specific actions to be defined, approved, and appropriate for the conditions.

Control in the world of Service Operation speaks to:

- The tools used to define normal and abnormal working conditions.
- Ability to regulate the performance of devices, systems, or services.
- Ability to measure availability by initiating corrective action.
11.1.1 Monitor Control Loop

A common model for understanding monitoring and control requirements is the monitor control loop. The process is rather simple and starts with monitoring an activity and the outputs of that activity. By monitoring the activity, the organization is focused on the performance of the activity or efficiency; the time it takes to complete the activity, the number of handshakes, the number of resources used, etc. By monitoring the outputs of the activity, the organization is focusing on the effectiveness of the activity or its ability to create a quality output.

The data gathered during monitoring will be compared against a defined standard norm. For instance, the quality of an activity’s output is based on the output’s ability to meet a minimum set of specifications or the activity will be considered efficient if it can be performed within a defined time frame. If the monitored activity is achieving the conditions defined by the standard norm, the organization does not need to take any corrective action.

However, when the standard norm is not met, corrective action is required. This is where control over the activity occurs. Let’s take a commonly seen monitor control loop for most people: airport security checkpoints. The activity being monitored is authorized people allowed in airport terminals. An authorized person is someone who has a legitimately obtained ticket to ride on an airplane. As people pass through a checkpoint, they are asked to show a valid source of identification and their ticket. The identification verifies the person and the name on the ticket must match that of the name on the ticket. If this simple condition is not met, the control activity is the person is removed from the line and prevented from boarding the airplane.

In the airport example, the security guard is the monitoring agent, the source of identification and airline ticket is the standard norm, and the control is the subsequent actions taken when the norm is or is not met. Standard airport checkpoints are considered an open loop system because they are designed to occur regardless of environmental conditions. In other words, you can always expect to hand over your passport and airline ticket to a security guard at least once in an airport (at least in
Closed loop systems also exist and they monitor environments based on prescribed conditions. For instance, security checkpoints may be set up in random locations or under specific conditions, like bomb threats. In this situation, the need to show identification is also required and the control activity may also end in detainment of people. The difference from the airport example is these checkpoints may be temporary and are often the result of some threat. In terms of IT services, a closed loop system may be initiated when the utilization of an IT component reaches a maximum threshold and load-balancing efforts kick in. In this example, load-balancing would be the closed loop system.

In practice, a process is a series of activities and each activity can be monitored individually as well as the entire process. In terms of monitor control loops, one is applied to each activity. The data from each activity can be compiled to understand the performance of the entire process and by monitoring the final output of the process, adjustments to individual activities can be controlled to change the performance and quality of the process. In the end, the organization can have a clear understanding of:

- Performance of individual activities in a process.
- Effectiveness of the process or procedure.
- Performance of individual devices used by the process.
- Performance of a series of devices.

When building monitor control loops, the following questions need to be asked:

- Who defines what needs to be monitored?
- What are the appropriate thresholds to be monitored?
- Will monitoring be automated or manual?
- How is “normal” operation defined?
- What must be in place for normal state Service Operation?
- What must be in place to monitor and control a normal state Service Operation?
- How frequently should the activity be measured (how often does it occur)?
• Are measurements active or passive?
• Who performs the monitoring and how do they relate to a central IT operational management function?
• If multiple lops (activities) exist, who is responsible for each loop? (This question refers to who is responsible for monitoring and correcting the activity, not the activity itself.)

ITSM can be seen in terms of a complex monitor control loop, where:

• Each Service Management process or activity of the process is being monitored.
• The monitoring agent is Continual Service Improvement
• The standard norm is defined by service catalog, service level agreements and other agreements, or cost of service.
• The control activities are dependent on the nature of the deviation and can require a change to:
  o Service Strategy – the architecture is not delivering on its promises.
  o Service Design – the service is too expensive, or service level targets need to be adjusted.
  o Service Operation – a non-compliance to Service Design exists.

In this control loop, Service Transition facilitates the monitoring and control activities, specifically by ensuring services can meet expected norms and controlling any changes needed to bring the processes under control.

11.1.2 Monitoring Strategies

The very first question of monitoring addresses what needs to be monitored? The answer is largely based on the desired outcome of a process, device or system. Children are a good example of changing monitoring requirements based on expected outcomes. If the parents’ intent is to encourage success in business, they would monitor the child’s education achievements, thus success in sports, physical and health achievements, success in the arts, creative achievements, and so on.
Children also provide the basis of pointing another concept in monitoring control—the idea of internal and external monitoring. For children, the parents may monitor their growth and progress and the school or government may also monitor their growth and progress. Hopefully, the monitoring systems are aligned and will provide a bigger picture of the child's potential place in the world. The same conditions exist in a service environment where a single department may monitor those processes, devices and services they are responsible while the larger organization or regulatory body is monitoring their contributions to the whole.

Both internal and external monitoring and control is necessary. Focus on internal monitoring will lead to a well-managed infrastructure which provides little contribution to the overall quality of services, while a focus on external monitoring may identify poor service quality but will be unable to identify the source of problem or how to change it.

An important concept in monitoring and control to understand is its objectives are not based on what is being monitored, but what outcomes are expected by what is being monitored. In short, we don't manage the child; we manage what the child grows up to be. So the first place to start defining the objectives of monitoring and control are the desired outcomes of the customer. These are documented in terms of service requirements and service level requirements. Services are designed to meet these requirements and will actively provide the inputs for defining monitoring in operations, control norms and mechanisms. During Service Design, the organization will:

- Work with customers to determine how service outputs will be measured.
- Identifying key configuration items, how they should be configured, and what level of performance and availability is required from them.
- Identify any constraints or limitations of service components in meeting performance or availability requirements.
- Applying instrumentation to each service for the purpose of generating meaningful events to be monitored.
Monitoring can be performed in terms of:

- Active or passive – active monitoring will poll a device or system for information, while passive monitoring will have the device or system generate and transmit an alert to a monitoring agent or “listening device.”
- Reactive or proactive – reactive monitoring focuses on taking action as a result of a certain type of event or failure, while proactive monitoring looks for patterns which can lead to an event and taking action before the event can occur.
- Continuous or exception-based – continuous measurements will monitor a device or system in real-time to ensure it complies with a performance norm. Continuous measurement sounds like active monitoring, but does not require to be active. Exception-based measurement is more concerns with detecting and reporting against exceptions rather than real-time performance measurements.
- Performance or quality – the performance of the service is distinctly different from the quality of the service’s output, but is often confused by IT organizations.

11.1.3 Measurements and Reporting

Monitoring and control plays a part in gathering and reporting measurements pertinent to the management of Service Operation. A measurement is any technique from which the extent, dimension or capacity of an item can be evaluated against a standard or unit. Extent is the degree of compliance or completion the item provides. Dimension is the size of the item. Capacity is the total capability of an item.

Measurements only have meaning when they can be compared to a standard or desired norm, which is defined in Service Design. Metrics are a means of assessing the process, system or function in quantitative terms. A metric is used to define what is measured, how it is measured, the acceptable range of performance desired, and what actions to take when normal performance is missing.
Measurements and metrics are communicated through reports, which are used to create awareness in the areas of interest for stakeholders. When action items are established on the findings in the reports, results are created for the business: knowing that the number of incidents has increased over the last month by 25% is one thing, doing something about the increase is another.

Immature, or poorly run organizations can be identified in how they relate to their reports, for instance:

- Reports are used to shift blame to another group, i.e. the rise in incidents is the result of the lack of capabilities in the Service Desk, not an increase in the number of maintenance windows missed.
- Reports are used to identify who is responsible for making a decision, i.e. since Incident Management is owned by the Service Desk, the person responsible for fixing the problem is the Service Desk Manager.
- Reports are used to create action plans for future occurrence: now that the number of incidents is a problem, we need to seek a resolution.

In a mature organization, the responsible persons, groups, and action plans are already in place long before the report is generated; the report is simply a trigger for the action to be executed. As the number of incidents increase, the findings can be tied to a justified situation, such as a new service or release being introduced or some other major change in the environment. Why the level of increase may be a concern, the organization can demonstrate they have the situation under control and was even expecting an increase in the number of incidents.

Another characteristic of an immature organization is they generate a number of reports which are not adequate read by anyone in the organization. Monitoring and reporting has no consequence of effectiveness if there is no control or action in response to the data.
11.1.4 Testing and Audits

Monitoring operational components will occur long before those components are deployed in a production environment. In fact, monitoring begins during service testing. One of the aspects of service testing is to ensure adequate monitoring, management and control is exists for the service in accordance to its level of service required; however, monitoring during the service test is also important for establishing a performance baseline for the service. If service testing demonstrates that the service acceptance criteria for the new or changed service has been met, the data generated when running the service during the test can be used as the standard norm when monitoring during service operation. For instance, if the availability metric is averaging 93.5% on an SLA of 92%, the test demonstrates the SLA can be met and a possible threshold to observe. During Service Operation, if the service begins slipping below 93.4% regularly than further, more detailed monitoring may be required.

One activity commonly seen during service operations are audits. Audits can be initiated by any team and some audits are regulated. Audits that can be internal or externally driven.

The purpose of an audit is to ensure:

- Processes and activities are performing as intended or designed.
- Processes and activities are worked according to their design with no circumvention.
- To verify they still meet requirements, or are fit for purpose.
- To identify any required changes or improvements.

While service managers can perform audits on the areas they are responsible for, the best approach is to have an independent auditor perform the work: an independent auditor will be more objective because they are not responsible for the end result. Some organizations will maintain an internal audit team and some will use a third-party auditor(s) exclusively. Most organizations will be subjected to some standard, regulation, or legislation which requires an independent audit from a third party.
11.2 IT Operations

“IT operations” is a broad term to describe a number of routine activities performed in service operation: including:

- Console management/operations bridge.
- Job scheduling.
- Backup and restore.
- Print and output management.

11.2.1 Console Management

Console management is a structured set of activities designed to coordinate the management of events, incidents, routine activities and reporting on the performance or status of IT service components. The key characteristic of console management is the use of a central console to manage all relevant activities and events. Console management is for IT service operation in the same manner air traffic control is for airport operations.

Console management is a 24/7 job, even if services or other functions are not. If the services are provided 24/7, but functions like the Service Desk are not, the console management/operations bridge will act as that function during off-hours. In some organizations, console management/operations bridge, and the service desk will fall under the same line of business organizationally. The function is a critical component of ITSM, and will handle and have access to massive amounts of sensitive data; therefore, its location will usually have a high level of security access required. In smaller organizations, a separate function may not be feasible, and the work is performed by a single team of technical staff who monitors the console as part of their regular duties.
11.2.2 Job Scheduling

In an environment where control is essential to ensure proper service delivery and support, routine work must be scheduled. Every IT environment will have routine work; whether the work is part of the service or housekeeping required to maintain the operating environment. Job scheduling is a means of defining and initiating routine activities, usually through automated systems.

Job scheduling involves the development of software packages that are routinely run in real-time or as batches during slow periods. These packages can be run daily, weekly, monthly, annually or as needed to meet business needs. Job schedules are established as part of Service Design, but amendments and adjustments may be performed during service operation as dependencies on the jobs are identified and addressed. Alerts and exceptions may be provided when job do not occur as expected. Change Management will need to assess the impact of change on existing job schedules.

Consider job scheduling in terms of airports flight schedules. Each airplane scheduled to takeoff needs to be prepped. In IT, this preparation is done by receiving the run-time parameters and/or files to be received. A debrief is performed after each flight: or run-time logs are checked for failures. If failures do occur, they have to be re-run: at an airport, a failure is a missed takeoff or arrival time and can potentially cause a delay in subsequent flights.

However, the primary concern of an airport is to maintain the schedule; which can be difficult if the schedule is filled. Imagine the pressure of if an airplane must depart every five minutes over an airplane departing every fifteen minutes. Heavy schedules in IT can have an adverse impact on the overall quality and performance of the service: though must jobs are performed in off-hours, heavy schedules may force jobs to execute during business hours.
Job scheduling requires a high degree of workload management, specifically:

- Avoiding contention on specific devices and resources and improving overall throughput.
- Migrating workloads to alternative platforms or environments to gain improved performance and/or throughput.
- Ensuring maximum utilization of available resources.

11.2.3 Backup and Restore

Backup and restore activities are vital for effective service continuity and are established as part of the Service Design. While backup and restore processes are a good practice for any organization, some types of organizations (financial) are regulated to have a strong backup and restore strategy in place which can be audited. These regulations can vary between countries and industries.

Why is backup and restore good practice? Simply put, there is always the possibility of failure in the environment. Having backups on hand minimizes the level of loss experienced from the failure. In terms of sports, a player is likely to be injured at any point in the game: if that happens, they are replaced in the field by another player. In IT, a backup is comprised of all the data required to support the service: when this data is required because of a failure, it is restored as part of the resolution. You cannot have restoration of data without a backup of that data.

Back up is an activity where a system’s data are copied and stored in a separate remote location of the system. A backup strategy will address all of the following:

- What data will be backed up?
- What frequency or interval will the data be backed up?
- How many generations of data will be backed up?
- What are the types of backup (full, partial, incremental) and checkpoints?
- Where data will be stored and rotation schedules used?
- What mechanisms will be used to verify readability of data after backup is performed?
- What transportation methods will be used to send data to storage location?
• What testing/checks are performed?
• What are the recovery point objectives?
• What are the recovery time objectives?
• How will the backups be validated to ensure they will work when restored?
• What is the procedure for procuring and managing media used in backups?

Backup and restoration of data may be performed automatically or may be initiated by the operations bridge. Manual work is required to ensure that the required media is loaded before backing up and to transport the backed up data to a remote location. Transportation may be performed by the organization’s security staff or by a third party security contractor.

Restore activities can be initiated for any number of reasons, including:
  • Corrupted data.
  • Lost data.
  • Back-out after failed change (remediation)
  • IT service continuity.
  • Historical data used in forensic investigation.

Steps taken in restoration of activities include:
  • Checking location for appropriate data/media.
  • Checking the authorization of the user/customer to get access to data.
  • Transferring data back to data center or location of system.
  • Agreement on checkpoint recovery point.
  • Restoration of file/data.
  • Ensuring success of data restore.
  • User/customer sign-off.
11.2.4 Print and Output Management

In many organizations, the capability for delivery of information in printed or electronic form is critical to the effective management of IT services. These capabilities are important as they often represent the tangible output of a service or contain vital information needed for the running of a business process.

Activities that are typically performed within this context are:

- Scheduling and execution of large print runs.
- Maintenance of the printers and consumables required.
- Maintaining control of high-value stationary.

11.2.5 Server and Mainframe Management

While mainframes are beginning to be replaced by (virtualized) servers, they are still in wide use and form the central component of many services. Unlike many other infrastructure components, mainframes typically require highly specialized staff to manage all aspects of daily operations, either as a single-centralized team, or several teams or departments.

Normal activities involved with managing a mainframe include:

- Operating system maintenance and support.
- Third-level support for associated incidents/problems.
- Procurement.
- Writing batch jobs and scripts.
- System programming.
- System security.
- Architecture improvements.
- Capacity and performance management.
Replacing mainframes as the central component for delivery services, servers provide dynamic capabilities for hosting applications, databases, client/server, file management, storage, and print services. While the activities will depend largely on the server technologies utilized and generally the same as mainframes, normal activities for server management and support include:

- Checking server log files.
- Applying necessary service packs and updates.
- Operating system support.
- Checking capacity and performance levels.
- Definition and management of virtual server.
- License management.
- Verifying core file and folder permission.
- Checking application functionality.
- Testing redundancy.
- Recommending necessary software and hardware upgrades.

### 11.2.6 Network Management

Network management is the set of activities that manage all of the organization's own Local Area Networks (LANs) and Wide Area Networks (WANs) with responsibilities also extending to the interfaces maintained with third-party network suppliers.

The activities of network management include:

- High level planning of network architectures.
- Third-level support for associated incidents/problems.
- Installation of devices and CIs.
- Configuration of routers and switches.
- Network operating system and middleware maintenance and support.
- Monitoring network traffic.
- Balancing network loads to improve performance.
- Network security.
• Managing IP addresses, DHCP, and DNS servers.
• Managing firewalls and secure gateways.
• Managing Internet service providers.
• Implementing intrusion detection systems.
• Updating configuration management as required for new, modified, and removed CIs.

11.2.7 Storage and Archive

For many organizations, there will be regulatory and legislative requirements governing the storage of data in physical and electronic form for a defined period of time. Beside this, there will be many organizational drivers for the archival of data, such as to understand marketplace trends, customer management, and product development. Policies and procedures developed in agreement with the business should cover:

• The length of time different forms of data should be kept for.
• Naming conventions and placement decisions.
• Maintaining data storage infrastructures, including storage devices, network attached storage (NAS), storage area networks (SAN), direct attached storage (DAS) and content addressable storage (CAS).
• Maintenance and support of utility and middleware data storage software.
• What procedures should be used.
• Compliance with governance, regulatory and legislation requirements.
• Rules and schedules for the archiving of data.
• Internal housekeeping of data storage facilities.
• Rules for retrieving archived data.
• Managing archiving technologies.
• What tools and systems will be used to support the organization’s information needs.
• Third-level support for associated incidents/problems.
11.2.8 Database Administration

Database administrators will often work closely with application management teams in the design and improvement of systems requiring database storage mechanisms. Typical responsibilities performed within these roles are:

- Creation of database standards and policies.
- Design of physical database.
- Development of logical data models.
- Creating physical databases.
- Creating data services.
- Managing database availability and performance.
- Establishing data resilience.
- Configuring and managing security levels.
- Monitoring and optimizing databases.
- Installing and configuring SQL application services.
- Administrating database objects.
- Defining event triggers and Event Management.
- General database housekeeping.
- Monitoring usage of database.
- Generating reports.
- Managing security issues.
- Assisting in backup and restore of database.
- Third-level support for associated incidents/problems.

11.2.9 Directory Services Management

Directory services allow users and applications to find network resources, such as users, groups, servers, applications, tools, services, and other information, over a distributed network. The goal of directory services is to ensure that, through using interfaced tools, systems, and processes, information is accessible through the network by any authorized requester.
Online directories are often designed to be dynamic, flexible, and secure. They frequently change as users and network resources move but must be secure so that access can be restricted to specific users, groups, or types of access.

Normal activities that are performed as part of directory services management include:

- Locating resources on network and tracking status.
- Creating objects that can be utilized within the directory services (users, groups, etc.).
- Assisting in the procurement and selection of directory services tools and systems.
- Managing the rights of specific users, groups, and other objects.
- Ensuring consistency in naming conventions.
- Monitoring events on the directory services.
- Maintaining tools used to manage directory services.
- Working with Service Design and Service Transition so that released components can be controlled within directory services.

**11.2.10 Desktop and Mobile Device Support**

Desktop and mobile support has overall responsibility for all company-owned user devices, including desktops, laptops, tablets, smartphones, device-specific software and peripherals. Specific responsibilities will include:

- Defining desktop and mobile computing policies and procedures.
- Designing standard desktop and device images.
- Service maintenance.
- Implementing desktop and mobile device archiving/rebuild policies.
- Third-level support for associated incidents/problems.
- Support for connectivity issues.
- Configuration control and audit for all desktop and mobile device hardware.
11.2.11 Middleware Management

Middleware describes the technology that connects software components or applications. The software consists of a set of enabling services that allow multiple processes running on one or more machines to interact across a network. In particular, the deployment of Service-Oriented Architectures (SOA) requires interfacing at the Middleware layer to operate effectively. Middleware provides the following functionality:

- Data transfer mechanisms.
- Communications between applications or processes.
- Data transmissions.
- Release and Deployment Management for software modules.
- Collation and distribution of system messages.
- Multicasting (simultaneous delivery of information to multiple destinations).
- Queue management.

Middleware Management is usually performed by staff within the application management and technical management functions, where normal activities performed include:

- Ensuring interoperability is supported by the middleware solutions implemented.
- Ensuring the normal operation of middleware through monitoring and control.
- Detecting and resolving incidents related to middleware.
- Managing upgrades to middleware, including licenses and new versions.
- Describing relationships to middleware solutions for recording in the CMS.

11.2.12 Internet Management

In organizations where the business relies on the internet and availability of internal and external websites, it may be beneficial to create a separate Internet/Web support team with specific responsibilities to manage the intranet and Internet services provided by the IT department.
Activities performed within these roles include:

- Working with Service Design on the development of standards for web-based applications, content, and websites.
- Managing and operating firewalls and secure gateways.
- Managing and operating secured sub-networks.
- Defining internet and web services architectures.
- Design, test, implement and maintain websites.
- Administrating any Content Management Systems used by the organization.
- Maintaining web development and management applications.
- Liaising with ISPs, hosts, and other third party suppliers involved in the delivery and support of internet/intranet services.
- Providing third-level support for internet/website incidents and problems.
- Maintaining Internet and website performance and availability through monitoring and control.
- Working with information security specialists to ensure the resilience and security of any internet/website solution.

11.2.13 Facilities and Data Center Management

In addition to the IT-specific duties of Service Operation, some effort needs to be placed on the management and maintenance of the physical facilities of the IT department. Commonly called data centers or computer rooms, these facilities may be shared between the IT department and the corporate customer, but should be managed based on the requirements from IT. These types of facilities will often require rooms which limit dust, raised floors, specific designs for power and cooling, and specialized fire suppression systems.
The components of facilities management include:

- Building maintenance
- Equipment hosting.
- Power management.
- Building monitoring systems.
- Safety compliance with regulations and legislation.
- Physical access control.
- Shipping and receiving.
- Contract management or third-party contractors.
- General maintenance and housekeeping.

Managing data centers involves more than the management of physical space and requires the adoption of a defined strategy for management and control of operations. The factors influencing that strategy include:

- Level of automation.
- Policy-based management.
- Real-time services.
- Capacity management of environmental requirements (power, cooling, space, etc.).
- Standardization of equipment.
- Service-oriented architectures.
- Virtualization.
11.3 Support from other Lifecycle Stages

Several processes associated with other service lifecycle stages have operational aspects to them and will fulfill some responsibilities within the Service Operation stage.

11.3.1 Demand Management

The goal of demand management is to assist the IT service provider in understanding and influencing customer demand for services and the provision of capacity to meet these demands. Demand management is often associated with capability management but is a basis for establishing strategies. The purpose for demand management overall is to provide information about capacity requirements before the design for capacity occurs, namely who is using what functionality, how, and when. This information is used to answer the questions:

- Why does the business need this capacity?
- Does the benefit of providing the required capacity outweigh the costs?

Demand management is responsible for understanding and strategically responding to business demands for services by:

- Analyzing patterns of activity and user profiles.
- Provisioning capacity in line with strategic objectives.

Service Operation is responsible for managing demand by utilizing two techniques:

- Physical/Technical constraints (e.g., restrict number of connections, users, running times).
- Financial constraints (e.g., using expensive charging for services near full capacity or over capacity quotas).
The intent of demand management in Service Operation is to optimize the utilization of infrastructure resources. This can be accomplished by:

- Rescheduling a particular workload to run at a different time of day, day of the week, etc., which has an impact on job scheduling.
- Moving a workload from one location or configuration item to another to balance utilization or traffic.
- Supporting technical virtualization to provide dynamic performance and resilience to systems.
- Limiting or moving demand for resources using techniques specific to demand management.

11.3.2 Financial Management for IT Services

The goal of financial management for IT services is to provide cost effective stewardship of the IT assets and the financial resources used in providing IT services. This enables an organization to account fully for spending on IT services and to attribute these costs to the services delivered to the organization’s customers.

Using financial management to provide services with cost transparency (e.g., via a service catalog) clearly understood by the business and then rolled into the planning process for demand modeling and funding is a powerful benefit for the organization. It enables the best balance to be struck between the opportunities available for the business against the capabilities levels of the IT organization.

Service Operation should support the overall IT budgeting and accounting system and may be actively involved in any defined charging system that may be in place. Typically, the Service Operation manager will be involved in regular reviews of operational and capital expenditure. Service Operation should also be involved in any cost-saving initiatives, as some actions made by the business may actually increase IT costs.
11.3.3 Capacity Management

The goal of capacity management is to ensure that the current and future capacity and performance demands of the customer regarding IT service provision are delivered against justifiable costs. Capacity management is the process that manages:

- The right capacity.
- At the right location.
- At the right moment.
- For the right customer.
- Against the right costs.

Capacity management provides the predictive and ongoing capacity indicators needed to align capacity to demand. It is about finding the right balance between resources and capabilities and demand.

- Too many resources and capabilities = $$$$.
- Too little resources and capabilities = loss in performance.
Some of the activities of Capacity Management are defined in the context of three sub-processes consisting of Business, Service and Component Capacity Management. Besides these, there will also be discussion of the operational activities required as well as the techniques that are utilized in various forms by the three different sub-processes.

• Business Capacity Management is the sub-process that covers the activities responsible for ensuring that the future business requirements for IT services are considered and evaluated in terms of their potential impact on capacity and performance. As business plans, operations and processes continually change, this will consequently affect the service provider’s ability to satisfy the business and customer’s requirements, including those already documented in SLAs. Some of the primary inputs into Business Capacity Management that trigger the activities here come from:
  o Project and Program Management.
  o Change Management.
  o Service Portfolio Management (as investments are evaluated and authorized).
  o Patterns of Business Activity (from Demand Management).
  o New Service Level Packages and Service Level Requirements (from Service Level Management).

• The primary focus of the Service Capacity Management sub-process is to monitor and analyze the use and performance of IT services and ensure that they meet their agreed SLA targets. The regular monitoring of service capacity and performance, and comparison against normal service levels will identify trends, breaches or any near misses that might occur. As a result, this process will need to work closely with Service Level Management to understand the agreed levels of service and to report back any targets achieved and breached, and concerns or advice in regards to capacity and performance issues. There will also need to be process integration with Incident and Problem Management so that there is early detection of disruptions where the root cause may be due to insufficient capacity being provided, as well as appropriate action taken to resolve the disruption so that agreed business targets are still met.

• The objective of Component Capacity Management is to ensure that the implementation and management of each of the individual components that support IT services is performed effectively to deliver optimum capacity and performance to meet business
needs. This includes the constant monitoring and analysis of each component to understand the performance, capacity and utilization characteristics that exist. This subprocess is a vital component to the overall quality of Capacity Management, as each component does have a finite capacity that, when reached, will begin to impact on the service levels being delivered and business operations being supported.

Service Operation is responsible for the following capacity management activities:

- **Capacity and performance monitoring**: Measuring, monitoring the performance of IT infrastructure components.
- **Handling capacity or performance incidents**: By means of event, incident and Problem Management, disruptions are diagnosed and resolved. Where appropriate, long term resolutions are implemented under the control of Change Management.
- **Demand and workload management**: Using technical and financial constraints to balance available capacity against demand. This could involve rescheduling services to run at a different time, moving the workload from one location or CI to another or using virtualization to enable dynamic workload sharing across multiple CIs.
- **Storage of capacity management data**: Utilizing existing capacity databases and the Configuration Management System.
- **Capacity planning**: Service Operation should provide input to the Service Design stage so that planning takes into account operational needs.
- **Reporting**: Service Operation should report any disruptions, events, and trends that are of importance to the capacity manager.
11.3.4 Availability Management

Availability Management’s primary goal is to optimize the capability of the IT infrastructure and support the organization to deliver a cost-effective and sustained level of availability that enables the business to satisfy its objectives. Other availability objectives are:

- Reduction in the frequency and duration of availability-related incidents.
- Maintain a forward looking availability plan.

For a consumer/user of an IT service, its availability and reliability can directly influence both the perception and satisfaction of the overall IT service provision.

While primarily a Service Design process, there are many elements involved in Availability Management that interact throughout the Service Lifecycle. Using a combination of both proactive and reactive activities, the scope of the process covers design, implementation, measurement, management and improvements of IT service and component availability. Activities involved in availability management can form two continuous cycles of planning and improvement. Service Operation is responsible for the monitoring, measuring, analysis, and management of all events, incidents, and problems regarding availability.

An aim of availability management is to ensure the duration and impact from incidents impacting IT services are minimized to enable business operations to resume as quickly as possible. The expanded incident lifecycle enables the total IT service downtime for any given incident to be broken down and mapped against the major stages that all incidents progress through.
The expanded incident lifecycle is a method used for analyzing the relationship between incident and availability management. The following metrics measured to evaluate the overall performance of the Incident Management process. Availability management uses this information to understand where improvement actions would be best made to optimize availability levels for the business, specifically:

- Detection Time: Time for the service provider to be informed of the fault (reported).
- Diagnosis Time: Time for the service provider to respond after diagnosis completed.
- Repair Time: Time the service provider restores the components that caused the fault.
- Calculated from diagnosis to recovery time.
- Restoration Time: (MTRS): The agreed level of service is restored to the user. Calculated from detection to restore point.
- Restore Point: The point where the agreed level of service has been restored.

Metrics observed through the expanded incident lifecycle:

- Mean time between failures (MTBF) or uptime:
  - Average time between the recovery from one incident and the occurrence of the next incident—relates to the reliability of the service.
- Mean time to restore service (MTRS) or downtime:
  - Average time taken to restore a CI or IT service after a failure.
  - Measured from when CI or IT service fails until it is fully restored and delivering its normal functionality.
- Mean time between system incidents (MTBSI):
  - Average time between the occurrence of two consecutive incidents.
  - Sum of the MTRS and MTBF.
  - Used to measure the reliability of a service.

Relationships in metrics important to Service Operation:

- High ratio of MTBF/MTBSI indicates that there are many minor faults.
- Low ratio of MTBF/MTBSI indicates that there are few major faults.
11.3.5 IT Service Continuity Management

IT service continuity management (ITSCM) is utilized as a supporting element for business continuity management (BCM) by ensuring that the required IT infrastructure and the IT service provision can be recovered within required and agreed business time scales. This is often referred to as disaster recovery planning and mitigation.

Service Operation is responsible for the operational management of the ITSCM process. The typical activities performed by staff include:

- Education and awareness of ITSCM procedures.
- Training for staff, suppliers, customers, and end users.
- Risk assessments and execution of agreed risk management measures.
- Assisting in generating actual recovery plans.
- Reviews and ongoing testing.
  - At least annually for all involved staff.
  - Following major changes and projects where necessary.
- Communication during continuous events.
- Audits of recovery procedures, risk-reduction measures, and for compliance to procedures.

11.3.6 Change Management

The ability to control and manage changes to defined IT services and their supporting elements is viewed as a fundamental element of quality Service Management. The ability to provide effective and efficient delivery and support of services has particular requirements for effective change control to occur. Changes arise for a number of reasons:

- From requests of the business or customers seeking to improve services, reduce costs, or increase ease and effectiveness of delivery and support.
- From internal IT groups looking to proactively improve services or to resolve errors and correct service disruption.
The process of Change Management typically exists in order to:

- Optimize risk exposure (defined from both business and IT perspectives).
- Minimize the severity of any impact and disruption.
- Deliver successful changes at the first attempt.

Service Operation should be involved in the design of change models for the diverse types of changes that will be assessed and how a balance can be maintained in regards to the varying needs and potential impacts of changes. In light of this, it is important to interpret the following Change Management guidance with the understanding that is intended to be scaled to suit the organization and the size, complexity, and risk of changes being assessed.

The goal of Change Management is to ensure that standardized methods and procedures are used for controlled, efficient, and prompt handling of all changes in order to minimize the impact of change-related incidents upon service quality and, consequently, to improve the day-to-day operations of the organization.

Remember: Not every change is an improvement, but every improvement is a change!

Change Management’s purpose is also to ensure that:

- All changes to service assets and configuration items (CIs) are recorded in the Configuration Management System (CMS).
- Overall business risk is optimized.
There must be policies and standards defined that clarify for Service Operation groups (and other involved parties) guidelines such as:

- Creating a culture of Change Management – with zero tolerance for unauthorized changes.
- Aligning the service Change Management process with business, project and stakeholder Change Management.
- Prioritization of changes.
- Establishing accountability and responsibilities.
- Segregation of duty controls.
- Establish a single focal point for changes.
- Prevent people who are not authorized to make changes from accessing production environment.
- Integration with other Service Management processes.
- Change windows.
- Performance and risk evaluation.
- Performance measures for the process.

The definition of different process models will allow an organization to maintain a balance between providing an appropriate level of control for changes without causing bottlenecks or restricting business growth. Change models define how various categories of changes are assessed and authorized with different mechanisms and activities used to process and deliver changes based on the change type. The defined change models should also include:

- What steps should be taken to manage the change.
- Roles and responsibilities.
- Time scales and thresholds for actions.
- Escalation procedures.
Some day-to-day activities of Change Management include:

- Raising and submitting requests for change.
- Reviewing RFCs by the change advisory board.
- Implementing authorized changes.
- Backing out changes as directed.
- Assisting with physical moves of assets.
- Defining and maintaining change models.
- Receiving and executing according to the change schedule.
- Ensuring Service Operation requirements and concerns are addressed when planning and designing new or changed services.

11.3.7 Release and Deployment Management

Often forgotten or ignored in many ITSM implementations or initiatives, release and deployment can be mistakenly seen as the poor cousin of Change Management, being of less importance and priority to both the business and IT organizations.

Much of the confusion and misunderstanding is perpetuated by the idea that release and deployment only focuses on the actual distribution of changes to the live environment. While timely and accurate distribution is indeed a goal of the process, the actual scope includes all of the activities, systems, and functions required to build, test, and deploy a release into production and enable effective handover to service operation.

In conjunction with the use of Change Management, release and deployment will enhance an organization’s capabilities to develop, compile, reuse, distribute, and rollback releases in accordance with defined policies that improve efficiency and reduce business disruption.
The primary objective of the Release and Deployment Management is to deploy new releases into production, transition support to Service Operation, and enable its effective use in order to deliver value to the customer. Other objectives of Release and Deployment are:

- To define and agree upon Release policies and Release and Deployment plans with customers and stakeholders.
- Ensure that the integrity of constructed release packages and that they are recorded accurately in the Configuration Management System (CMS).
- Ensure that all release packages can be tracked, installed, verified, uninstalled or backed out if necessary.
- Ensure that the required skills and knowledge is transferred to support staff, customers, end-users, suppliers and any other relevant stakeholders; and there is minimal unpredicted impact on the production services, customers and service operation.

Governing the activities of Release and Deployment Management are the release policy, release plan, and deployment plan. In many cases, the release and deployment plans will be created as part of planning the release, though some releases may have common characteristics to allow template-based plans to be used. The release policy is the overarching strategy for releases and was derived from the Service Design stage of the Service Lifecycle. The release plan is the operational implementation for each release. The deployment plan is the documented approach for distributing a single release.

The operational activities of Release and Deployment Management include:

- Actual implementation of Service Operation components or services.
- Participation in planning of major releases.
- Physical handling of configuration items.
- Backing out of failed releases.
11.3.8 Service Asset and Configuration Management

The goal of Service Asset and Configuration Management is to support the agreed IT service provision by managing, storing, controlling, and providing information about configuration items (CIs) and service assets throughout their lifecycle. Quality and timely information supplied about CIs and service assets will enhance the effectiveness and efficiency of other Service Management processes and, in particular, those used within Service Operation. Other objectives include:

- To support the business and customer’s control objectives and requirements.
- To minimize the number of quality and compliance issues caused by improper configuration of services and assets.
- To optimize the service assets, IT configurations, capabilities, and resources.

The scope of Service Asset and Configuration Management includes any IT or service asset used within the Service Lifecycle. It provides a complete inventory of assets and defines who is responsible for their control, as well as financial information used in Financial Management for IT. Configuration Management identifies, documents, baselines and maintains Configuration data so that changes to the IT infrastructure can be controlled. It provides a logical model of the infrastructure, recording services, assets, and infrastructure and the relationships that exist between them. Service Asset and Configuration Management may cover non-IT assets or business products used or involved in the delivery and support of services.

The majority of benefits enabled by effective Service Asset and Configuration Management can be seen in improvements of other Service Management processes. By having quality asset and configuration data available, the benefits to other processes include:

- Better forecasting and planning of changes.
- Changes and releases to be assessed, planned, and delivered successfully.
- Incidents and problems to be resolved within the service level targets.
- Changes to be traceable from requirements.
- Enhanced ability to identify the costs for a service.
Benefits that may be seen to be provided primarily by the process alone include:

- Better adherence to standards.
- Greater compliance to legal and regulatory obligations.
- Optimum software licensing by ensuring correlation between licenses needed against the number purchases.

Operational activities attributed to Service Asset and Configuration Management are:

- Identifying and communicating any discrepancies found between the CMS and actual configuration items.
- Correcting any found discrepancies.
- Labelling and tagging physical assets.
- Assisting in configuration audits.
- Providing the necessary information needed to update the CMS.

### 11.3.9 Knowledge Management

The quality of decision-making within Service Operation depends on the ability and understanding of those parties involved, the understanding of the benefits and consequences of actions taken, and the analysis of any of the surrounding issues involved. All of this, in turn, depends on the availability of accurate and timely knowledge, information, and data provided in a way that can be easily accessed and interpreted by the appropriate parties.

The goal of knowledge management is to enable organizations to improve the quality of management decision-making by ensuring that reliable and secure information and data is available throughout the service lifecycle. The primary purpose is to improve efficiency by reducing the need to rediscover knowledge.
This requires accessible, quality, and relevant data and information to be available to staff. The objectives of knowledge management are to:

- Enable the service provider to be more efficient and improve quality of service, increase satisfaction, and reduce the cost of service.
- Ensure staff have a clear and common understanding of the value that their services provide to customers and the ways in which benefits are realized for the use of those services.
- Ensure that, at a given time and location, service provider staff have adequate information on:
  - Who is currently using their services.
  - The current states of consumption.
  - Service delivery constraints.
  - Difficulties faced by the customer in fully realizing the benefits expected from the service.

This equates to better real-time information and data for operational staff responding to user requests and incidents, as well as documented procedures for resolving known errors and requests.

Activities performed within service operation include:

- Errors within the service detected will be recorded and analyzed, and the knowledge about their existence, consequences, and workarounds will be made available to service operation in an easy-to-use fashion.
- Frontline Incident Management staff on the service desk and second-line support are the point of capture for much of the everyday ITSM data.
- Problem management staff will be key users of collected knowledge and will be typically responsible for the normalization of data capture by means of developing and maintaining scripts supporting data capture within Incident Management.
11.3.10 Information Security Management

Though Access Management has a direct interface with information security management, the remaining Service Operation processes will contribute to the achievement of the process’ objectives, specifically by:

- Enforcing policies and reporting discrepancies.
- Providing technical assistance to investigate and resolve security incidents.
- Providing operational security control.
- Screening and vetting IT staff according to policies and procedures.
- Maintaining security training and awareness programs.
- Verifying security issues are addressed in all documented policies and procedures.

11.4 Improving Service Operations

Improvements in Service Operation can be obtained by:

- Automating manual tasks.
- Reviewing and formalizing makeshift activities or procedures.
- Performing operational audits.
- Using incident and Problem Management as improvement tools.
- Communicating.
- Educating and training.
11.5 Elearning Module 16 & Workbook Review Questions

1. Service operation ensures performance while integrating which of the following?
   a. Confidentiality, integrity and availability
   b. Functionality, performance and price
   c. Technology, people and process
   d. Functionality, schedule and resources

2. What is fundamental to the delivery, support, and improvement of services?
   a. Monitoring, reporting and control
   b. Excellent technology performance
   c. Console Management
   d. Skills, knowledge and competency

3. What is reporting?
   a. Activity of observing a situation to detect changes over time
   b. Analysis, production, and distribution of the output of monitoring
   c. The process of managing the utilization or the behavior of a device, system or service
   d. The actions taken as a result of detecting change through monitoring

4. Which of the following conditions is not required to control a device, system or service?
   a. The outcome conforms to a defined standard or norm
   b. Conditions prompting action must be defined, understood and confirmed
   c. Actions must be defined, approved and appropriate for these conditions
   d. An appropriate level of authority must be engaged to ensure proper subjugation
5. In a monitor control loop, what is monitored for quality of service?
   a. Activity
   b. Output
   c. Input
   d. Norm

6. In IT operations, what activity best supports the organization’s ability to support continuity efforts for the customer?
   a. Console management
   b. Job scheduling
   c. Backup and restore
   d. Print and output management

7. When server and mainframe management responsibilities are divided among different teams, what is the most likely distinction between the teams justifying the separation?
   a. Technology platforms
   b. Supported services
   c. Resource location
   d. Customer lines of business

8. Which of the following acronyms is not used to describe a form of data storage technology?
   a. CAS
   b. SAN
   c. DAS
   d. WAN
9. Which of the following Service Management processes would Service Operation staff be less likely to participate?
   a. Financial Management for IT Services
   b. Service Portfolio Management
   c. Service Level Management
   d. Change Management
12 Organizing for Service Operations

An organization will generally be structured according to how it operates and this idea continues in ITSM. For this reason, the organization of service operation is often seen in terms of functions, rather than processes. Therefore, customer relationship and satisfaction is often seen as a function of the Service Desk, while different platforms and architectures are supported by technical sufficient groups. While this approach to distinguishing responsibility may have its benefits, it’s important to note that the processes use in IT must be versatile. Every platform will deal with availability, capacity, performance and security planning and concerns. Configuration items will be supported by a myriad of support individuals. Every person in IT will eventually be involved with incidents, problems, service requests and changes.

12.1 Functions

Functions refer to the logical grouping of roles and automated measures that execute a defined process, an activity, or combination of both. The functions within Service Operation are needed to manage the steady state operation IT environment. Just like in sports where each player will have a specific role to play in the overall team strategy, IT functions define the different roles and responsibilities required for the overall service delivery and support of IT services.
The functions introduced in service operation include:

- Service Desk.
- Technical Management.
- IT Operations Management:
  - IT Operations Control.
  - Facilities Management.
- Applications Management.

The size of the function and the responsibilities they have will be based on:

- Size and location of the organization.
- Complexity of technology used.
- Availability of skills.
- Cultural factors.
- Financial concerns.

Additionally, some functions and responsibilities may be outsourced to an external organization.

12.2 The Service Desk

A service desk is a functional unit that acts as the primary point (first line) of contact for the end-user community, for all incidents, requests, and general communication that may arise. It plays an essential and valuable role for any organization, contributing significantly to the satisfaction of users and the overall impression of the IT organization. Depending on the type of business, services, and technology supported, the exact size and physical organization of the service desk will vary from a small, centralized team to a diverse range of teams in multiple locations and time zones.
The primary goal of the Service Desk is to support the agreed IT service provision by ensuring the accessibility and availability of the IT organization and by performing various supporting activities. Other objectives include:

- To act as a single point of contact for all user incidents, requests and general communication.
- To restore “normal Service Operation” as quickly as possible in the case of disruption.
- To improve user awareness of IT issues and to promote appropriate use of IT services and resources.
- To assist other IT functions by managing user communication and escalating incidents and requests using defined procedures.

While many organizations have already seen the justification for the creation of a Service Desk team(s), in many cases the business case for the improvement fail to gain support from various levels of management. As discussed earlier, the needs and requirements will vary significantly for each organization, however the typical benefits gained through the implementation/improvement of a Service Desk function include:

- Improved customer service perception, and satisfaction.
- Increased accessibility through the use of a single point of contact.
- Better quality and speedier turnaround of requests.
- Improved teamwork and communication.
- Better managed infrastructure and control.
- Improved usage of IT resources.

Many factors will influence the way in which a Service Desk function will be physically structured, such as the location, languages and cultures of end-users, diversity in services and technology supported and the objectives governing the implementation of the Service Desk such as improved satisfaction or reduced operating costs. The following are some of the main options chosen when implementing a Service Desk function.
12.2.1 Service Desk Organizational Structures

Many factors will influence the way in which a service desk function will be physically structured, such as the location, languages, and cultures of end users; diversity in services and technology supported; and the objectives governing the implementation of the service desk, such as improved satisfaction or reduced operating costs.

The following are some of the main options chosen when implementing a service desk function:

- Local Service Desk – A local service desk structure is where the service desk is co-located within or physically close to the user community it serves. This may aid in communication and give the service desk a visible presence, which some users may like. It may, however, be inefficient and expensive as a result of having multiple service desks operating.

<table>
<thead>
<tr>
<th>Benefits of a local service desk structure</th>
<th>Disadvantages of a local service desk structure</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Local and specific user knowledge</td>
<td>• Higher costs for replicated infrastructure and more staff involved</td>
</tr>
<tr>
<td>• Ability to effectively communicate with multiple languages</td>
<td>• Less knowledge transfer, each service desk may spend time rediscovering knowledge</td>
</tr>
<tr>
<td>• Appropriate cultural knowledge</td>
<td>• Inconsistency in service levels and reporting</td>
</tr>
<tr>
<td>• Visible (and physical) presence of the service desk</td>
<td>• Service desks may be focused on local issues</td>
</tr>
</tbody>
</table>
- **Centralized Service Desk** – A centralized structure uses a service desk in a single location (or smaller number of locations); although, some local presence may remain to handle physical support requirements, such as deploying, moving, and disposing of user workstations. This could be more efficient, enabling less staff to manage a higher volume of calls with greater visibility of repeat incidents and request.

<table>
<thead>
<tr>
<th>Benefits of a centralized service desk structure</th>
<th>Disadvantages of a centralized service desk structure</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Reduced operational costs</td>
<td>• Potentially higher costs and challenges in handling 24 × 7 environment or different time zone</td>
</tr>
<tr>
<td>• Improved usage of available resources</td>
<td>• Lack of local knowledge</td>
</tr>
<tr>
<td>• Consistency of call handling</td>
<td>• Possible gaps in language and culture</td>
</tr>
<tr>
<td>• Improved ability for knowledge sharing</td>
<td>• Higher risk (single point of failure), in case of power loss or other physical threat</td>
</tr>
<tr>
<td>• Simplicity for users (call one number) to contact the service desk</td>
<td></td>
</tr>
</tbody>
</table>
• Virtual Service Desk – A virtual service desk, through the use of technology (particularly the Internet) and the use of corporate support tools, can give users the impression of a single, centralized service desk when, in fact, the personnel may be spread or located in any number or type of geographical or structural locations.

<table>
<thead>
<tr>
<th>Benefits of a virtual service desk structure</th>
<th>Disadvantages of a virtual service desk structure</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Support for global organizations</td>
<td>• Initial cost of implementation, requiring diverse and effective voice technology</td>
</tr>
<tr>
<td>• 24 × 7 support in multiple time zones</td>
<td>• Lack in the consistency of service and reporting</td>
</tr>
<tr>
<td>• Reduced operational costs</td>
<td>• Less effective for monitoring actions of staff</td>
</tr>
<tr>
<td>• Improved usage of available resources</td>
<td>• Staff may feel disconnected from other service desk staff</td>
</tr>
<tr>
<td>• Effective matching of appropriate staff for different types of calls</td>
<td></td>
</tr>
</tbody>
</table>

• Follow the Sun – The Follow the Sun model will combine two or more geographically dispersed service desks to provide 24-hour service. This type of configuration is usually implemented by global or international organizations.

<table>
<thead>
<tr>
<th>Benefits of a follow-the-sun service desk structure</th>
<th>Disadvantages of a follow-the-sun service desk structure</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Support for global organizations</td>
<td>• Typically higher operating costs</td>
</tr>
<tr>
<td>• 24 × 7 support in multiple time zones</td>
<td>• Cost of required technology</td>
</tr>
<tr>
<td>• Improved quality of service</td>
<td>• Challenges in using single language for multiple regions when recording knowledge, workarounds, known errors, etc.</td>
</tr>
<tr>
<td>• Improved customer/user satisfaction</td>
<td></td>
</tr>
<tr>
<td>• Effective knowledge sharing and high level visibility of distributed infrastructure</td>
<td></td>
</tr>
</tbody>
</table>

12.2.2 Specialized Service Desk Groups

Depending on the requirements defined for the Service Desk, organizations will need to consider what skill level is appropriate for the Service Desk and the support it will offer. This skill level can be defined in many ways, but most often is associated with the first time resolution achieved for calls, incidents and requests made to the Service Desk by users. The 3 types of Service Desks are:

• Call Center: Responsible for handling/logging of large volumes of calls.
• Help Desk: Responsible for managing and co-ordinate incidents.
• Service Desk: Responsible for managing incidents and requests, and also provides a wide variety of supporting services (e.g. supporting Human Resources).
Based on the skill level required and the size of the service desk, some organizations may decide to create specialized groups within the Service Desk function. These groups will often support a smaller subset of users or services.
12.2.3 Elearning Module 17 & Workbook Review Questions

1. Which of the following functions will not be responsible for console management at any point in a service’s lifecycle?
   a. Service Desk
   b. Technical Management
   c. IT Operations Management
   d. Application Management

2. Facilities Management is a sub-function of what ITIL driven function
   a. Service Desk
   b. IT Operations Management
   c. Technical Management
   d. Application Management

3. Which of the following is not a term commonly attributed to a Service Desk?
   a. Single point of contact
   b. Single point of coordination
   c. First point of contact
   d. Single source of services

4. Which of the following is not a responsibility of the service desk?
   a. Handling incidents
   b. Managing communication with users
   c. Maintain status quo of service environment
   d. Handling service requests
5. A service desk which supports employees working from home is most likely using what organization structure for the service desk?
   a. Local service desk
   b. Centralized service desk
   c. Virtual service desk
   d. Follow the sun model
12.2.4 Service Desk Staffing

One of the most challenging issues facing a service desk manager is that of staffing with many organizations finding it increasingly difficult to acquire and retain quality employees. Additionally, determining appropriate staff levels can be difficult with call rates being very volatile and dynamic.

Most service desk managers will have a list of key competencies or selection criteria that is used when hiring new staff members. Depending on the type of service desk that has been implemented and what types of technologies are being supported, these criteria will vary; however, typical skills required include:

- Communication skills.
- Technical knowledge.
- Business understanding.
- Diagnosis and analysis skills.
- Understanding of the role/value of processes and procedures.
- Typing skills.

Communication skills are ultimately the most important as they will need to be able to deal effectively with a wide-range of people and stressful situations.

The number of staff employed on the service desk is dependent on the needs of the business, the objectives/goals defined, and a range of other important criteria including:

- Business budget.
- Customer service expectations.
- Size, maturity, design, complexity of the IT infrastructure and service catalog.
- The number of customers and users to support.
- The volume of requests, incidents, and general communication required.
- Period of support cover required.
- Workload pattern of requests.
• SLA definitions in place.
• Level of training required.
• Support technologies available.

To ensure a balanced mix of experienced and newer staff, Service Desk Managers should use a number of methods and incentives to retain quality staff and to avoid disruption and inconsistency in the quality of support offered. Some ways in which this can be done include:

• Recognition of staff achievements contributing to service quality.
• Rotation of staff onto other activities (projects, second-line support etc.).
• Team building exercises and celebrations.
• Promote the Service Desk as a potential stepping stone for staff to move into other more technical or supervisory roles (after defined time periods and skills achieved).

Super users are often useful positions to be appointed across an organization to act as liaison points with the IT organization and the service desk in particular. Super users can be used in a number of ways such as:

• To assist in general communication between the service desk and users.
• To filter requests and issues raised by the user community.
• To assist in user training.

While super users can be a valuable resource if they are properly coordinated, the following rules should be in place:

• Roles and responsibilities are clearly defined.
• Escalation channels are defined.
• Standard support processes defined and used.
• All requests recorded and maintained consistently.
12.2.5 Measuring Service Desk Performance

To evaluate the true performance of the Service Desk, a balanced range of metrics should be established and reviewed at regular intervals. Especially dangerous is the tendency to focus on “average call time” or “number of calls answered” metrics which can mask underlying issues with the quality of support provided. Some of the typical metrics reviewed when monitoring the performance of the Service Desk include:

- The number of calls to the service desk (broken down by type, time of day and day of the week).
- First-line resolution rate.
- Average Service Desk cost of handling any incident or request.
- Number of knowledge base articles created.
- Number or percentage of SLA breaches.
- Call resolution time.
- Customer satisfaction (surveys).
- Use of self-help (where exists).

Although fairly common, there are potential risks that can be introduced when outsourcing an organization’s Service Desk. When reviewing the potential for this to occur, Service Managers should consider the following items when developing contracts to reduce these risks:

- Use of your own Service Management tool, not theirs.
- Retain ownership of data.
- Ability to maintain required staffing levels.
- Agreements on reporting and monitoring needs.
- Proven up-to-date procedures.
- Agreed and understood support needs.
- Engage contract specialists for assistance.
The Service Desk is, for the most part, a point of integration for the entire organization because it is the function from which all user contact is funneled and actions for other groups are initiated in service operation. From the perspective of IT process and support, it is convenient and beneficial to view the Service Desk as the beginning and end of the process: with inputs from users, customers, suppliers, and internal teams to initiate incidents, problems, changes, and requests and ending with outputs in the form of confirmation of completion and customer satisfaction. Viewing the Service Desk from this context will allow IT management to see the vast requirements on the Service Management system just to support this function, particularly in the area of Knowledge Management; but it also exposes risks related to the ineffectiveness of Service Desk if not properly supported.

In some organizations, the Service Desk is not viewed appropriately, especially since the majority of the staff positions on the Service Desk are “entry” positions into the organization. As a result, the Service Desk is commonly overlooked in the early strategy decisions, design efforts, and transitions and may not be engaged properly to obtain their requirements on a new or changed service. Organizations adopting the ITSM framework may have to radically change their cultural views about the Service Desk.

12.2.6 Customer/User Satisfaction Surveys

Customer satisfaction surveys are a means of understanding Service Desk performance from the perspective of the users and are critical in evaluating the “soft” skills of the function. The survey used at the Service Desk is different than the customer satisfaction survey initiated by Business Relationship Management and is often given after the closure of an incident or request record.
The different types of delivery for the customer satisfaction survey are represented in the table below:

<table>
<thead>
<tr>
<th>Technique/Tool</th>
<th>Advantages</th>
<th>Disadvantages</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>After-call survey</strong></td>
<td>- High response rate because the caller is already on the phone.</td>
<td>- People may feel pressured into taking the survey, resulting in a negative service experience.</td>
</tr>
<tr>
<td></td>
<td>- Caller is surveyed immediately after the call so their experience is recent.</td>
<td>- The surveyor is seen as part of the service desk being surveyed, which may discourage open answers.</td>
</tr>
<tr>
<td><strong>Outbound telephone survey</strong></td>
<td>- Higher response rate because the caller is interviewed directly.</td>
<td>- This method could be seen as intrusive if the call disrupts the user or customer from their work.</td>
</tr>
<tr>
<td></td>
<td>- Specific categories of user or customer can be targeted for feedback (e.g., people who requested a specific service or people who experienced disruption to a particular service).</td>
<td>- The survey is conducted some time after the user or customer used the service desk, so their perception may have changed.</td>
</tr>
<tr>
<td>Technique/Tool</td>
<td>Advantages</td>
<td>Disadvantages</td>
</tr>
<tr>
<td>------------------------</td>
<td>----------------------------------------------------------------------------</td>
<td>--------------------------------------------------------------------------------------------------</td>
</tr>
</tbody>
</table>
| **Personal interviews** | - The interviewer is able to observe non-verbal signals as well as listening to what the user or customer is saying.  
                          | - Users and customers feel a greater degree of personal attention and a sense that their answers are being taken seriously. | - Interviews are time-consuming for both the interviewer and the respondent.  
                          |                                                                     | - Users and customers could turn the interviews into complaint sessions. |
| **Group interviews**   | - A larger number of users and customers can be interviewed.  
                          | - Questions are more generic and, therefore, more consistent between interviews.                  | - People may not express themselves freely in front of their peers or managers.  
<pre><code>                      |                                                                     | - People’s opinions can easily be changed by others in the group during the interview. |
</code></pre>
<table>
<thead>
<tr>
<th>Technique/Tool</th>
<th>Advantages</th>
<th>Disadvantages</th>
</tr>
</thead>
</table>
| **Postal/email surveys** – Survey questionnaires are mailed to a target set of customers and users. They are asked to return their responses by email or post. | Specific or all customers or users can be targeted.  
Postal surveys can be anonymous, allowing people to express themselves more freely.  
Email surveys are not anonymous but can be created using automated forms that make it convenient and easy for the user to reply and increase the likelihood it will be completed. | Postal surveys are labor-intensive to process.  
The percentage of people responding to postal surveys tends to be small.  
Misinterpretation of a question could affect the result. |
12.2.7 Elearning Module 18 & Workbook Review Questions

1. Which of the following is not a factor used in determining staffing levels at the service desk?
   a. Customer expectations
   b. Size of the IT infrastructure
   c. Skill level of technical teams
   d. Level of self-help tools available

2. Which of the following does not drive the level of skill required on the service desk?
   a. Target resolution times
   b. The information contained in the KEDB
   c. Complexity of systems supported
   d. What the customer is buying

3. For most service desks, including call centers, what is the most important skill to develop?
   a. Interpersonal skills
   b. Business awareness
   c. Service awareness
   d. Technical awareness

4. In order to support the effectiveness of the service desk, what role is generally assigned in customer environments?
   a. Subject matter expert
   b. User facilitator
   c. Moderator
   d. Super User
5. Which of the following metrics would not contribute to understanding the average service desk cost of handling an incident?
   a. Total cost of the service desk divided by the number of calls
   b. Percentage of call duration time on the desk overall and cost per minute
   c. Cost per call per type
   d. Average cost of resolving incidents which have been escalated

6. What type of survey would have the highest response rate?
   a. After-call survey
   b. Online survey
   c. Email surveys
   d. Personal interviews
12.2.8 Outsourcing the Service Desk

Although fairly common, there are potential risks that can be introduced when outsourcing an organization’s service desk. When reviewing the potential for this to occur, service managers should consider the following items when developing contracts to reduce these risks:

- Use of your own Service Management tool, not theirs.
- Retain ownership of data.
- Ability to maintain required staffing levels.
- Agreements on reporting and monitoring needs.
- Proven up-to-date procedures.
- Agreed and understood support needs.
- Engage contract specialists for assistance.
12.2.9 Elearning Module 19 & Workbook Review Questions

1. When a service desk is outsourced, who is responsible for the outcomes of the decision?
   a. The customer
   b. The user
   c. The outsourced service desk
   d. The service provider

2. An outsourced service desk does not need access to which of the following?
   a. Known error data
   b. Service portfolio
   c. All incident records and information
   d. Configuration management system

3. What is not an effective method communication between an outsourced service desk and other support groups?
   a. Suggestion or complaint boxes
   b. Performance reviews
   c. Cross-training tutorials
   d. Partnership arrangements
12.3 Technical Management

To enable regular Service Operation, one or more technical support teams or departments will be required to provide Technical Management and support for the IT Infrastructure. In all but the smallest organizations where a single combined team or department may suffice, separate teams or departments will be needed for each type of infrastructure being used. In many organizations the Technical Management departments are also responsible for the daily operation of a subset of the IT Infrastructure. Technical Management plays an important role within Service Operation by:

- Being the custodian of technical knowledge and expertise related to managing the IT Infrastructure.
- Providing detailed technical skills and resources needed to support the ongoing operation of the IT Infrastructure.
- Providing the actual resources to support the ITSM lifecycle.
- Ensuring resources are effectively trained and deployed to design, build, transition, operate and improve the technology to deliver and support IT Services.

The Technical Management function's primary goal is to plan, implement and maintain a stable technical infrastructure that supports the organization’s business processes. This is achieved through:

- Well designed, highly resilient, cost effective technical architectures.
- The use of adequate technical skills to maintain the technical infrastructure in optimum condition.
- Swift use of technical skills to speedily diagnose and resolve any technical failures that do occur.
To enable quality knowledge sharing and continual improvement of services, technology, processes and other capabilities, Technical Management staff should develop effective communication channels and meet regularly to discuss issues or potential ideas. History demonstrates that quality design requires involvement from those who will be supporting the product/service, as does quality support require involvement from the designers in turn.

12.3.1 Technical Management Activities

The activities of technical management can be classified into two categories

- Generic activities to the technical management function.
- Shared activities performed by the three functions of technical, application, and IT operations management.

The generic technical management activities are:

- Identifying the knowledge and expertise required to manage and operate the IT infrastructure and to deliver IT services.
- Documenting the skills that exist in the organization, as well as those skills that need to be developed.
- Initiating training programs to develop and refine the skills.
- Designing and delivering training for users, the service desk, and other groups.
- Recruiting or contracting resources with skills that cannot be developed internally or where there are insufficient people to perform the required technical management activities.
- Procuring skills for specific activities where the required skills are not available internally or in the open market.
- Defining the standards used in the design of new architectures.
- Participating in the definition of technology architectures during the Service Strategy and Design stages.
- Researching and developing solutions.
- Participating in the design and development of new services.
- Participating in projects.
• Engineering availability and capacity management for IT services to meet the levels of service.
• Assessing risk, identifying critical service and system dependencies.
• Defining and implementing countermeasures.
• Designing and performing tests for the functionality, performance, and manageability of IT services.
• Managing suppliers.
• Defining and managing Event Management standards and tools.
• Participating in resolution of incidents.
• Participating in resolution of problems.
• Defining coding systems that are used in incident and Problem Management (e.g., incident categories).
• Supporting Problem Management in validating and maintaining the KEDB.
• Supporting the Change Management process to evaluate changes.
• Assisting with the deployment of releases.
• Providing information for, and operationally maintaining, the CMS and its data.
• Identifying opportunities for improvement.
• Ensuring that all systems and operating documentation are up-to-date and properly utilized.
• Updating and maintaining data used for reporting on technical and service capabilities, e.g., capacity and performance management, availability management, problem management, etc.
• Assisting financial management for IT services to identify the cost of technology and IT.
• Human resources used to manage IT services.
• Defining the operational activities performed as part of IT operations management.
12.3.2 Measuring Technical Management Performance

The metrics chosen to evaluate the performance of Technology Management will largely depend on which technology is being managed. However, some generic metrics areas include:

- Measurement of agreed outputs:
  - Contribution in support/enhancement of business processes.
  - Knowledge transferred to other teams and functions.
  - Training provided.
  - Availability of key infrastructure provided.
  - Transaction rates supported.
  - Installation and configuration of CIs under their control.
- Process metrics:
  - Number of events captured and managed (grouped by type).
  - Resolution time frames for escalated incidents and problems.
  - Number of changes implemented and backed out.
  - Costs incurred against those budgeted.
  - Security issues detected and resolved.
  - SLA compliance/exceptions.
- Technology performance:
  - Capacity provided.
  - Utilization rates.
  - Availability of services and systems.
  - Individual CI performance rates.
- Mean time between failures of specified equipment:
  - Percent of purchase components that remain in place for the length of time as expected.
  - Measurement of maintenance activity.
  - Training and skills development.
12.3.3 Elearning Module 20 & Workbook Review Questions

1. What is the general responsibility of the technical management function?
   a. The daily operation and management of the IT infrastructure
   b. The monitoring, reporting and control of the physical and logical aspects of the services
   c. The daily effort to identify and correct any deviation in service, system or device performance
   d. The improvement of service performance and quality

2. Which of the following statements is not an objective or technical management?
   a. Using well-designed, highly resilient and cost-effective technical topology
   b. Develop technical skills to maintain the technical infrastructure in the best condition
   c. Develop technical skills to swiftly diagnose and resolve technical failures
   d. Ensure the required functionality is available at the desired levels of services

3. Specialist technical architects are primarily involved in what service lifecycle stage?
   a. Service Strategy
   b. Service Design
   c. Service Transition
   d. Service Operation

4. What is an example of a process metrics applied to technical management?
   a. Number of maintenance windows exceeded
   b. Number of escalations to third-party support organizations
   c. Number of unauthorized changes detected
   d. General availability and performance achievements
12.4 IT Operations Management

IT Operations Management is the function that provides capabilities for performing the daily operational activities required to maintain a stable production (live) environment. In many ways, the function performs many of the logistical activities required for the effective and efficient delivery and support of services (e.g. Event Management).

IT Operations Management is often seen as authoritative oversight to Technical Management and Application Management functions, as many of the activities performed will involve elements of the technical infrastructure or applications being supported. In some organizations this means that many of the IT Operations Management activities are performed by the other functions themselves, but in larger organizations it is more common that a centralized group of staff will be designated with responsibility. Good practice generally recommends that Technical and Application Management areas should manage new and unstable systems and applications, and transfer them to IT Operations Management when they have matured.

The primary goal of IT Operations Management is to perform the IT organization’s day-to-day operational activities using repeatable and consistent actions. Some of the objectives include:

- Maintenance of the “status quo” to achieve stability of the organization’s day-to-day processes and activities.
- Regular scrutiny and improvements to achieve improved service at reduced costs, whilst maintaining stability.
- Swift application of operational skills to diagnose and resolve any IT operations failures that occur.
One role played by IT Operations Management is that of Operations Control. This role is concerned with the execution and monitoring of the operational activities and events in the IT infrastructure (possibly using an Operations/Network Bridge). In addition to the routine tasks to be performed in accordance with the design specifications of the IT infrastructure, Operations Control is also responsible for the following:

- Monitoring and Control.
- Console Management.
- Job Scheduling.
- Backup and restores.
- Print and Output Management.

Facilities Management refers to the role responsible for management of all physical IT environments, usually data centers, computer rooms and recovery sites. In some organizations, many physical components have been outsourced and Facilities Management may include the management of the outsourcing contracts. For any organization, this is a very important element of ITSM, and will contribute to the ability to provide a safe working environment. Facilities Management should be involved in any large-scale and project planning to provide advice regarding any physical accommodation of staff or infrastructure required.

12.4.1 Measuring IT Operations

IT Operations are measured in terms of its effective execution of specified activities and procedures, as well as its execution of process activities. Some typical metrics areas that are evaluated include:

- Successful completion of scheduled jobs.
- Number of exceptions to scheduled activities and jobs.
- Number of data or systems restores required.
- Equipment installation statistics.
- Process metrics.
- Maintenance activities.
12.4.2 Elearning Module 21 & Workbook Review Questions

1. Which of the following is an activity of Facilities Management?
   a. Console management
   b. Backup and recovery
   c. Recovery sites
   d. Job scheduling

2. Which of the following statements is not an objective of IT Operations Management?
   a. Maintain the status quo to achieve stability in the day-to-day processes and activities of the organization
   b. Providing regular scrutiny and improvement to achieve improved service at reduced costs
   c. Swift application of operational skills to diagnose and resolve any IT operations failures
   d. Develop technical skills to maintain the technical infrastructure in the best condition

3. The centralization of IT operations management activities is obtained though establishing what type of entity?
   a. Service desk
   b. Operations bridge
   c. Dashboard
   d. IT steering committee
12.5 Application Management

The Application Management function (much like the Technical Management function) is responsible for managing applications throughout their lifecycle. This scope can include any staff developing, testing, supporting and improving applications, including those in project roles. In smaller organizations, Applications Management will typically be responsible for performing the daily operations required for applications under their control. Application Management also plays roles such as:

- Supporting and maintaining operational applications, and so plays an important role in design, testing and improvement of applications that form part of IT Services.
- Supporting the organization’s business processes by helping to identify functional and manageability requirements for application software.
- Assisting in the design and deployment of those applications.
- Providing ongoing support and improvement of those applications.
- Identifying skills required to support the applications.

Application Management’s primary goal is to develop, maintain, and support quality applications that enhance the organization’s business processes. This goal is achieved through:

- Applications that are well designed, interface with existing architectures, are resilient and cost-effective.
- Ensuring the functionality and performance requirements of the business are delivered in optimal fashion.
- The use of technical skills to maintain availability of applications.
- Swift response to diagnose and resolve any disruptions that occur.
One of the key decisions that Application Management is faced with is whether to:

*Buy an application that supports the required functionality.*

**OR**

*Build the application specifically for the organization’s requirements.*

In most cases, the final decision will be made by a Chief Technical Officer (CTO) or IT Steering Group, but to do so they require information from a number of sources. Application Management will assist in the decision making process by providing:

- Application sizing and forecasting workloads and demand cycles.
- Specification of manageability requirements.
- Identification of ongoing operational costs.
- Data access requirements for reporting or integration into other applications.
- Analysis of whether functionality can be met by existing tools – and how much customization will be required to achieve this.
- Estimating the cost of customization.
- Identification of what skills will be required to support the solution.
- Administration requirements.
- Security requirements.
If the decision is made to build the application, a further decision needs to be made on whether the development will be outsourced or built by employees. Most decisions will be made during the Service Strategy and Design phases, but there are some important considerations for Service Operation, including:

- How will manageability requirements be specified and agreed?
- What are the Acceptance Criteria for operational performance?
- How and where will the solution be tested and who will perform the tests?
- Who will own and manage the Definitive Library for that application?
- Who will design and maintain the operational management and administration scripts for these applications?
- Who is responsible for environment set-up and owning and maintaining the different infrastructure components?
- How will the solution be instrumented so that it is capable of generating the required events?

**12.5.1 Application Management Lifecycle**

Application Development processes should be implemented as part of a coordinated approach to ITSM, although, in many cases, this fails to happen. When the development of applications is not integrated with the rest of ITSM, it often leads to a breakdown in communication channels between developers and support staff and, ultimately, released applications that are not optimal in supporting business processes.

The Application Management Lifecycle has the following stages:

- Requirements.
- Design.
- Build.
- Deploy.
- Operate.
- Optimize.
The requirements phase is where the requirements for the new/modified application are gathered through consultation with the business and customers who will be using it. Primarily driven by the Service Design and Service Strategy phases of the ITSM Service Lifecycle, it encompasses the tasks that go into determining the needs or conditions to meet for a new or altered product, taking account of the possibly conflicting requirements of the various stakeholders, such as customers, users or the IT organization.

When gathering the requirements for any application, they are usually grouped into six main categories:

- **Functional requirements** are developed to specify particular behaviors of a system to support a particular business function.
- **Manageability requirements** are identified from the perspective of the IT organization, addressing the need for a responsible, available and secure service. They also seek to ensure that the application can be built, deployed and supported by Service Operation.
- **Usability requirements** address the needs of the end-user, evaluating the accessibility of the application and what training may be required to facilitate its effective use.
- **Architectural requirements** evaluate how the application will integrate within existing architectures, or whether any modifications are required.
- **Interface requirements** to see where there may be dependencies between existing applications or tools and the new application.
- **Service Level Requirements** which should specify the performance requirements, the quality of its output and any other qualitative measures that are identified from the customer or user perspective.

In the Design phase of the Application Management Lifecycle, the requirements are translated into specifications by the system architects and other developers. This enables the design of the application itself, the architecture to be used and the supporting environment for its operation.
Where the application is being purchased from an external supplier, this phase may involve consultation to ensure compatibility for its introduction and to facilitate any modifications or plug-ins that is required for its use. Consideration as to the level of customization of purchased software will often affect the decision whether to build or buy an application.

During the Build phase, the application is configured and made ready for deployment. Typically, this will integrate with the processes of Release and Deployment and Service Validation and Testing, so any application components are coded, integrated and tested effectively. Using techniques such as the Service V model for testing provides a framework to help organize the levels of Configuration Items that are needed and the associated testing and validation activities within and across stages of the development of an application. The left hand side represents the specification of the service requirements down to the detailed Service Design. The right hand side focuses on the validation and test activities that are performed against the specifications defined on the left hand side, and there is direct involvement by the equivalent party on the right hand side.

It shows that service validation and acceptance test planning should start with the definition of the high level requirements. It also describes that the person/group or sign off on the requirements on the left side should be involved on the right side to accept that the requirements have been met.

The Service V Model is a concept of establishing acceptance requirements against the various levels of requirements that apply in order to justify release to the customer for trial and assessment.
The actual tests required at each level should reflect the approach to risk and level of confidence that is required for the service change being transitioned. There are many frameworks and sources of guidance focused specifically on testing, e.g. Test Management Approach (TMAP) that provide more details about the specific types of testing activities that can be performed. These normally include:

- Usability testing.
- Process and procedure testing.
- Knowledge transfer and capability testing.
- Performance, capacity and resilience testing.
- Volume, stress, load and scalability testing.
- Availability, security backup, and recovery testing.
- Logistics, deployment and migration testing.
- Build, packaging and distribution testing.
- Operability and maintainability testing.

The Deploy phase provides a controlled mechanism for the deployment of the application and associated operational model (using Release and Deployment Management). The quality of transition to Service Operation is a crucial element to the success of the overall deployment that is being implemented. Rather than simply hand off support post-deployment, the application development teams should assist provide Early Life Support, managing any calls, incidents and problems that are detected in the early of the new or modified service. This enables more stability in this vulnerable period, increased customer and user satisfaction, enhanced learning and better momentum for continual improvement. The resource allocation from these teams will then be gradually reduced while Service Operation takes on more responsibility for support.

In the Operate phase, Service Operation delivers and supports the application as required by the business and customers. The techniques described earlier in this book will be used to monitor, control and respond to any disruptions or questions that arise in the use of the application. It is important to note, however, that the application is but one component making up an IT Service, and so an end-to-end view of the service should be maintained for effective Service Operation.
The Optimize stage is primarily driven by Continual Service Improvement, where the measurements taken during Service Operation are analyzed and acted upon. Improvement actions may seek to make functionality, usability, performance, or any other range of improvement actions that are desired. Internally, ways in which the application management lifecycle itself is utilized may be improved to develop quality applications with less cost/effort.

12.5.2 Application Management Generic Activities

Most application management teams will focus on supporting a single application or set of similar applications, however some activities of these teams will be common amongst all of them.

- Identifying the knowledge and expertise required to manage and operate applications in the delivery of IT services.
- Initiating training programs to develop and refine the skills in the appropriate application management resources.
- Maintaining training records for these resources.
- Recruiting or contracting resources with skills that cannot be developed internally or where there are insufficient people to perform the required application management activities.
- Designing and delivering end-user training
- Insourcing for specific activities where the required skills are not available internally or in the open market or where it is more cost-efficient to do so.
- Defining standards used in the design of new architectures.
- Participating in the definition of application architectures.
- Researching and developing solutions.
- Participating in the design and building of new services.
- Participating in projects.
- Designing and performing tests for the functionality, performance, and manageability of IT services.
- Designing applications to meet the levels of service required by the business.
- Assistance in assessing risk, identifying critical service and system dependencies.
- Defining and implementing countermeasures.
- Managing suppliers.
• Being involved in the definition of Event Management standards and especially in the instrumentation of applications for the generation of meaningful events.
• Providing application management resources that contribute to the execution of the Problem Management process.
• Defining coding systems that are used in incident and Problem Management (e.g., incident categories).
• Providing resources to support Problem Management in validating and maintaining the KEDB together with the application development teams.
• Supporting Change Management to evaluate changes.
• Participating in Release and Deployment Management activities.
• Defining, managing, and maintaining attributes and relationships of application CIs in the CMS.
• Identifying opportunities for improvement and assisting in the evaluation of alternative solutions.
• Ensuring a mechanism is in place to store and maintain documentation related to applications.
• Collaborating with technical management on performing training needs analysis and maintaining skills inventories.
• Assisting financial management for IT services to identify the cost of the ongoing management of applications.
• Defining the operational activities related to applications that will be performed as part of IT operations management.
• Providing input into and maintenance of software configuration policies.
12.5.3 Measuring Application Management

Some typical metric areas utilized to evaluate the performance of the Application Management function include:

- Measurement of agreed outputs:
  - Accessibility of deployed applications.
  - Recorded Known Errors and workarounds.
  - User measures of the quality of outputs as defined in SLAs.

- Process metrics:
  - Time taken to build, test and deploy applications.
  - Response times to incidents and problems.
  - Resolution times for incidents and problems.
  - Number of changes implemented and backed out.
  - Defined budgets compared against actual costs incurred.
  - Utilization levels of application compared to estimates.

- Application Performance:
  - Response times (actual and synthetic transactions).
  - Application availability, Mean Time between System Incidents, Mean Time to Restore Service etc.

- Measurement of Maintenance activity:
  - Exceptions to agreed maintenance or deployment schedules.
  - Number of fixes and updates applied.

- Projects:
  - Time and costs spent on projects.

- Training and skills development:
  - User training facilitated.
  - Service Desk training.
  - Knowledge transfers.
12.5.4 Elearning Module 22 & Workbook Review Questions

1. Which of the following activities is part of but distinct from application management?
   a. Application design
   b. Application development
   c. Application deployment
   d. Application support

2. The application management lifecycle consists of six stages; which stage is handled through the Service Operation lifecycle stage?
   a. Deploy
   b. Build
   c. Operate
   d. Optimize

3. Which of the following is not a factor in how an application is managed?
   a. Purpose of the application
   b. Functionality of the application
   c. Type of technology used
   d. Skills of the staff involved
12.6 Organizational Development

Organizational change does not occur on its own: it must be planned, designed, and implemented. Organizational change does not occur instantaneously: it can take months and years to achieve its goals. There is no single, or best, way to organize.

Organizations tend to move between two paradigms: centralization and decentralization. Centralization focuses on bringing components under a single, or central, authority and is often initiated when problems within the organization are persistent and complex. Decentralization allows decisions to be made locally to the operations and provides greater autonomy to lower level managers; however, their decisions can be narrow, short-sighted, and incongruent to the larger organization’s objectives.

Organization structures are influenced by:

- Commitment of senior management.
- Industry, regulatory, and legislative factors.
- Corporate and IT strategies.
- Organization age, size, and scope.

12.6.1 Stages of Organizational Development

Management styles will generally describe how an organization operates and can be used to identify and plan the growth and maturity of the organization. There are five dominate management styles:

- Network.
- Directive.
- Delegative.
- Coordination.
- Collaborative.
The organization can be served by each of these management styles for a while, but growth will usually require the organization to change management styles to succeed. To move from one management style to the next, an organization will typically need to overcome a specific challenge related to the dominate management style.

The Network management style represents an informal, rapidly paced, and ad hoc delivery of services. Organizations with this dominant style are entrepreneurial and innovative, will focus heavily on its technology and are avoid establishing formal structures. Past successes will reinforce the need to continue in this style, but growth in service demand makes the model not sustainable over time.

The network management style relies heavily on localized knowledge and dedication from staff members. Actions between individuals and groups are coordinated by agreements, rather than authority; relying on people to complement each other without formal structures. To grow as an organization, leadership must be identified and empowered. This focus on leadership will fly in the face of the autonomy present in the network style because it begins to create a formalized structure from which decisions and policies are made.

The advantages of a network structure are:

- Bureaucratic costs due to complex structures are avoided.
- Fewer managers are required, making the organization “flat.”
- The structure of the organization is highly adaptable and can be altered quickly to meet different challenges.
The disadvantages of a network structure are:

- Management must ensure the integration of individual activities from staff members.
- Significant problems exist when coordinating activities.
- Sourcing functional activities to external providers is extremely challenging as sourcing decisions are made locally.

Overcoming the leadership challenge of a network structure will move the organization into a directive structure, where upper management becomes focused on “directing” strategy and lower management will assume responsibilities at the operational or functional level. The focus of a directive structure is to establish a hierarchy where functional activities are separated and managed. In an IT organization, this may separate technical teams, support for particular applications, systems or processes, and even shared functions like the service desk.

In this style, communication becomes more formal and processes are implemented. Interactions may be defined entirely by the process or through operational level agreements (OLA) which supplement existing SLAs. Managers in functional areas will often be forced to choose between taking the initiative or to follow the process; leading to shift towards centralization as the organization because a major driver in decision making.

Autonomy becomes the challenge of organizational growth at this stage: approval is required at high-levels of the organization while successful performance at lower levels go unnoticed and unrewarded. To move forward, the organization must be willing and able to shift responsibility downward into the organization though delegation. This downward shift requires management to empower and recognize the efforts of managed personnel.

The structure of delegation shifts authority for minor decisions to lower level managers: whose increased control is matched by a corresponding reward system. Delegation combines the best elements of both network and directive structures: allow the organization to encourage innovation.
while leveraging efficiencies in the environment. The delegation structure is a decentralized structure which shifts responsibilities appropriately from a functional paradigm to a process paradigm.

When problems arise with the delegation structure, the typical response is to return to a centralized solution at the functional level: which does not enable growth for the organization. The proper response, however, is greater control of the process(es) to improve coordination of individual efforts.

Greater control in the organization results in the implementation of formal systems: a hallmark of the coordination structure. Senior managers will see formal systems as critical to business success and take responsibility for their implementation and use. Coordination techniques and solutions support planned structures for Service Management, which are continuously reviewed and improved. In the coordination structure, functions are centralized and processes are decentralized.

The challenge for the organization at this stage is its agility: the organization’s ability to respond rapidly to changes in the internal and external environments, usually because of pressure to adhere to procedural requirements. In theory, the capability towards rapid response is the product of collaboration, as information flows through a diverse group of people rather than a single individual.

The most developed organizational structure will encourage greater collaboration between functional units within an organization, with external organizations, and between processes. Matrix-based organization structures are representative of the collaborative stage, which identified roles and responsibilities based on function and product or customer.
The advantages of a matrix structure are:

- Barriers between functions are overcome and reduced.
- Personnel can respond better to change, internal and external.
- Communication is improved between functional personnel, or specialists.
- Cross-training between functions is possible.
- Skills and experience from supporting different products and customers can be leveraged for problematic or new ventures.

The disadvantages to a matrix structure are:

- A control structure is lacking which can develop stable expectations across functional and customer responsibilities.
- Conflict with roles can develop as greater ambiguity may be perceived, especially in similar roles supporting different customers.
- Conflict can develop over time, between functional and customer teams.

To approach organizational growth and structuring, upper management must understand:

- What stage of development the organization already resides.
- What range of options is available and appropriate to the organization.
- Each solution will create new challenges to overcome.
12.7 Roles and Responsibilities

A role is a set of responsibilities, activities and authorities assigned to a person or team. Roles and job titles (position) are not synonymous terms. Roles are defined by process; job titles are defined by organization. A person fulfilling the responsibilities associated with a job title may be fulfilling several roles. There are two categories of roles:

- Generic – roles which are found in every process, such as process owner and process manager.
- Specific – roles which are developed for specific processes.

Roles can be accountable or responsible for a specific activity: meaning several roles may participate in the successful completion of an activity. RACI models are useful tools for separating responsibilities for an activity between different roles.

12.7.1 Service Owner

The service owner is a generic role with responsibility for managing a service within a business context. The service owner is accountable for the delivery of a single, and specific, service across the entire lifecycle of the service. Accountability over the service is independent of where technological components, processes or professional capabilities reside in the organization.

A person fulfilling the service owner role may do so for several services. The specific responsibilities of a service owner are (responsibilities are associated with relevant Service Strategy processes):

- Ensures service delivery and support consistently meet agreed customer requirements.
- Participating in internal service review meetings (with IT).
- Assist in defining service models and service assessments.
- Identify opportunities for service improvements.
- Raise RFCs for service improvements.
• Provide input on service attributes (performance, availability, capacity, etc.).
• Understand the service.
• Solicit required data, statistics and reports for analysis.
• Facilitate effective service monitoring and performance.
• Understand and translate customer requirements into service-related activities, measures, and components used in meeting those requirements.
• Ensure consistent communication with customer(s) for service-related questions and issues.
• Discuss potential service improvements with customer.
• Serve as a point of escalation for major incidents in service delivery.
• Participate in external service review meetings (with customer).
• Ensure service entry in service catalog is accurate and maintained.
• Liaison with appropriate process owners throughout the service lifecycle.
• Represent the service across the organization.
• Represent the service in change advisory board meetings.
• Participate in negotiating SLAs and OLAs.
• Raise service improvement opportunities in CSI register.
• Review and prioritize improvements in CSI register.
• Make improvements to service.

The service owner is a primary stakeholder in all Service Management processes that underlie and support the delivery of the service they own, including:

• Incident Management.
• Problem Management.
• Release and Deployment Management.
• Change Management.
• Service Asset and Configuration Management.
• Service Level Management.
• Availability Management.
• Capacity Management.
• IT Service Continuity Management.
- Information Security Management.
- Financial Management for IT Services.

### 12.7.2 Process Owner

The specific roles associated with other Service Design processes are usually restricted to process owner and process manager. A process owner is accountable for ensuring a process is fit for purpose, or the process performs according to agreed and documented standards and meets the aims of the process definition. A process manager is accountable for the operational management of a process. The same person may be assigned to fulfill the process owner and process manager roles.

The specific responsibilities for process owner are (additional responsibilities for individual Service Design processes are also provided):

- **Generic:**
  - Sponsor, design, and manage change to the process and its metrics.
  - Define process strategy.
  - Assist in process design.
  - Ensure the availability and currency of process documentation.
  - Define policies and standards relative to the process.
  - Audit the process regularly to ensure compliance.
  - Communicate process information or changes.
  - Provide process resources to service lifecycle activities.
  - Ensure technicians working the process have the required knowledge and understanding of business and technical information needed to deliver the process.
  - Identify, review and prioritize opportunities for process improvements (with CSI manager).
  - Address process issues.
  - Implement process improvements.
  - Carry out the above responsibilities for their assigned Service Management process.
• Incident Management:
  o Design incident models and workflows.
  o Working with other process owners to ensure integrated approach to design and implementation of Incident Management, Problem Management, Event Management, Access Management, and request fulfillment.

• Problem Management:
  o Design problem models and workflows.
  o Working with other process owners to ensure integrated approach to design and implementation of Incident Management, Problem Management, Event Management, Access Management and knowledge management.

• Request Fulfillment:
  o Design service request models and workflows.
  o Working with other process owners to ensure integrated approach to design and implementation of Incident Management, Problem Management, Event Management, Access Management and Change Management.

• Event Management:
  o Plan and manage support for Event Management tools and processes.
  o Working with other process owners to ensure integrated approach to design and implementation of Incident Management, Problem Management, Event Management, Access Management.

• Access Management:
  o Plan and manage support for Event Management tools and processes.
  o Working with other process owners to ensure integrated approach to design and implementation of Incident Management, Problem Management, Event Management, Access Management.
12.7.3 Process Manager

The specific responsibilities for process manager are (additional responsibilities for individual Service Design processes are also provided):

- **Generic:**
  - Work with process owner to plan and coordinate all process activities.
  - Ensure all relevant service lifecycle activities are executed.
  - Appoint people to required roles.
  - Manage resources assigned to process.
  - Work with service owners and other process managers to ensure smooth running of services.
  - Monitor and report on process performance.
  - Identify, review and prioritize opportunities for process improvements (with CSI manager).
  - Implement process improvements.
  - Carry out the above responsibilities for their assigned Service Management process.

- **Incident Management:**
  - Plan and manage support for Incident Management tools and processes.
  - Coordinate interfaces between Incident Management and other Service Management processes.
  - Drive efficiency and effectiveness of Incident Management process.
  - Produce management information.
  - Manage efforts of incident support staff.
  - Monitor effectives of Incident Management and make recommendations for improvement.
  - Develop and maintain Incident Management systems.
  - Manage major incidents.
  - Develop and maintain Incident Management process and procedures.

- **Problem Management:**
  - Plan and manage support for Problem Management tools and processes.
  - Coordinate interfaces between Problem Management and other Service Management
processes.

- Work with problem resolution groups to ensure swift resolution of problems.
- Own and maintain the Known Error Database.
- Gatekeeper for inclusion of all known errors.
- Management of search algorithms for KEDB.
- Formal closure of all problem records.
- Work with suppliers, contractors, etc. to ensure contractual obligations are met in relation to Problem Management.
- Arrange, run, document, and follow-up with major problem reviews.

- **Request Fulfillment:**
  - Plan and manage support for request fulfillment tools and processes.
  - Coordinate interfaces between request fulfillment and other Service Management processes.
  - Handle concerns, requests, issues and inquiries from staff, customer and management.
  - Meet service level targets regarding request fulfillment activities.
  - Review and analyze all request fulfillment reports to identify opportunities for improvements.
  - Oversee actions to obtain feedback from customs on quality of activities for request fulfillment.
  - Assist with identifying staffing request levels to handle demand on request fulfillment activities.
  - Ensure all authorized service requests are fulfilled in a timely manner.
  - Represent request fulfillment activities at CAB meetings.
  - Review initial prioritization and authorization of service request to maintain accuracy and consistency.

- **Event Management:**
  - Plan and manage support for Event Management tools and processes.
  - Coordinate interfaces between Event Management and other Service Management processes.

- **Access Management:**
  - Plan and manage support for Access Management tools and processes.
Coordinate interfaces between Access Management and other Service Management processes.

12.7.4 Functional Management

The introduction of functions within the organization requires a look at the generic management roles found in each function. At the Service Desk, management roles are typically seen in terms of manager and supervisor. The responsibilities of the service desk manager include:

- Appointing people to the required roles.
- Managing resources assigned to the service desk.
- Managing service desk activities.
- Acting as escalation point for the service desk supervisor(s).
- Fulfilling a wider customer service role.
- Reporting to senior managers on any issue that could significantly impact the business.
- Attending CAB meetings.
- Taking overall responsibilities for incident and service request handling on the service desk.
- Monitoring and reporting on service desk performance.
- Identifying opportunities for improvement.
- Working with CSI manger to review and prioritize improvements in the CSI register.
- Making improvements to service desk.

The service desk supervisors are similar to shift managers in a production environment and are responsible for the day-to-day floor operations of the service desk. In small organizations, the service desk supervisor may also be a service desk analyst. The responsibilities of the service desk supervisor include:

- Ensuring staffing and skill levels are maintained throughout operational hours by managing staff schedules, etc.
- Undertaking human resource activities needed.
- Acting as escalation point where difficult or controversial calls are received.
- Producing statistics and management reports.
• Representing the service desk at meetings.
• Arranging staff training and awareness sessions.
• Working with senior management.
• Working with Change Management.
• Performing briefings to service desk staff on changes or deployments which may affect service desk volumes.
• Assisting analysts in providing first-line support.

Another centralized function in the organization is the operations bridge, or operations center. This function will also have manager and “supervisor” roles. The IT Operations manager is responsible for all activities of IT operations management and will include:

• Providing overall leadership, control and decision-making and responsibility for IT operations management teams and department.
• Reporting to senior management on all IT operations issues.
• Performing line management for all IT operations team or department managers/supervisors.

Since the operations center is a 24-hour operation, floor activities are typically managed by shift leaders who have the responsibility for:

• Taking overall responsibility for leadership, control and decision-making during assigned shift.
• Ensuring all operational activities are performed satisfactorily and according to agreed time scales and policies and procedures.
• Working with other shift leader(s) to ensure proper handover, continuity and consistency between shifts.
• Acting as line manager for all operations analysts.
• Assuming overall health and safety, and security responsibility for the shift.
Technical and application management functions are often divided based on specialty and assigned to each team is a manager or team leader. The technical manager or team leader is responsible for:

- Taking overall responsibility for leadership, control and decision-making for the technical team.
- Providing technical knowledge and leadership in assigned technical areas.
- Ensuring necessary training, awareness and experience levels are maintained within the team or department.
- Reporting to senior management on all technical issues relevant to their assigned responsibilities.
- Performing line management for all team members.

The applications manager or team leader has similar responsibilities:

- Taking overall responsibility for leadership, control and decision-making for application team.
- Providing technical knowledge and leadership in assigned application support.
- Ensuring necessary training, awareness and experience levels are maintained within the team or department.
- Providing ongoing communications to users and customers regarding application performance and business requirements.
- Reporting to senior management on all application issues relevant to their assigned responsibilities.
- Performing line management for all team members.

12.7.5 Analysts in Service Operations

The Service Operation processes specifically call out the role of analyst as it pertains to each process; with Incident Management providing level tiers for the analyst roles. Analyst is a generic role that is applied to any IT staff who is operating within a specific process.
Incident Management introduces levels in the analyst role which corresponds to responsibilities, skills, and competency. These levels are analogous to different lines of defense, with a first, second, and third line typically found in an organization. The intent of service operation is to respond to the majority of incidents with the first-line; allowing only a few incidents to require support of the second or third line. In this context, the first line analyst would encounter the incident first. The first line analyst is responsible for:

- Recording incidents.
- Routing incidents to support specialist groups.
- Ensuring correct prioritization and classification for incident.
- Providing initial support.
- Providing ownership, monitoring, tracking, and communication of incidents.
- Providing resolution and recovery of incidents.
- Closing incidents.
- Monitoring the status and progress towards resolution of assigned incidents.
- Keeping users and the service desk informed about incident progress.
- Escalating incidents as necessary per established escalation policies.

The first line analyst role is often seen combined with the service desk analyst in an organization; however, this depends on the role of the service desk. The responsibilities of the service desk analysis are typically restricted to taking calls from users and providing initial support for incidents and service requests. While this may include creating an appropriate record and following clear guidelines for resolving incidents or fulfilling requests, the service desk may not be expected to do so in every case. First-line analysts can also be part of the operations bridge or technical and application teams.
Request fulfillment analyst responsibilities are often assigned to persons who also fulfill the first-line analyst role, but these responsibilities can extend to other support lines. The responsibilities include:

- Single point of contact and end-to-end responsibilities for insuring submitted service requests are processed appropriately.
- Providing initial triage of service requests to determine what IT resources are required to fulfill them.
- Communicating service requests to other IT resources involved in the fulfillment of the request.
- Escalating service requests according to agreed service targets.
- Ensuring service requests are appropriately logged.

Second and third line analyst roles will have greater skill and competency in resolving incidents and fulfilling requests. This also translates in more responsibilities for the people filling these roles as they may also be filling the roles of

- Problem analyst.
- Request fulfillment analyst.
- IT operators.
- Technical analyst/architect.
- Application analyst/architect.

In addition to increased skill, second line analysts are often given more time to respond to an incident that cannot be resolved by a first line analyst. The responsibilities may be similar to a first-line analyst but with one clear advantage – they will not be interrupted by telephone calls or other requests. The organization for second-line analyst would benefit from being located near the service desk and may be considered a second level service desk themselves. They may be part of the IT operations center and handle all incidents, requests and events not covered by the service desk which can be resolved using remote procedures. They may even be associated with third-line support as they are assigned to specific technical and application teams.
Third line analysts are highly specialized persons assigned to specific teams within the IT organization, such as:

- Network support.
- Voice support.
- Service support.
- Desktop support.
- Application management.
- Database support.
- Hardware maintenance.
- Environment equipment suppliers.

Problem analysts are involved in the actual investigation and resolution of problems and may require one or more technical support groups or suppliers to complete successfully. While multiple people may be involved in investigating and resolving a particular problem, the problem analyst is typically the person accountable for the output from Problem Management. In most organizations, the person with the most expertise in the problem area will be assigned responsibilities as the problem analyst and their responsibilities include:

- Review incident data.
- Analyze problems for correct prioritization and classification.
- Investigate assigned problems to resolution or root cause.
- Coordinate actions of others assisting with analysis and resolution actions for problems and known errors.
- Raise requests for changes to resolve problems.
- Monitor progress on resolution of known errors and advising Incident Management staff on best workarounds.
- Update the Known Error Database with new or updated known errors and workarounds.
- Assist in the handling of major incidents and identifying root causes.
As mentioned before, these process roles may be combined with similar roles based on function. Organizationally, the next tier of roles above the Service Desk is the IT Operators. In this role, the day-to-day operational activities defined in technical management or application management are performed and the IT operators responsibilities will typically include:

- Perform backups.
- Console operations.
- Manage print devices.
- Ensure batch jobs, archiving, and other activities in job scheduling are performed.
- Run scheduled housekeeping jobs.
- Burn images for distribution and installation.
- Physical installation of standard equipment.

The IT Operator is a different role from the IT Operations Analyst who is responsible for determining the most effective and efficient approach to conducting a services or operations. The IT Operational Analyst is a senior IT operations staff person and is often associated with technical management. Technical management may assign personnel to technical operator roles who are responsible for the day-to-day operations tasks per the technical team they are assigned.

Delving deeper into the functional roles of the organization are the technical analyst/architect and application analyst/architect. These roles will perform activities essential for managing different aspects of the IT environment, but are not part of the day-to-day operational duties. The responsibilities of the technical analyst/architect include:

- Working with users, sponsors, application management, and other stakeholders in order to determine evolving needs.
- Working with application management and other technical management teams to determine the highest level of system requirements required to meet service requirements within the constraints of the budget and technology.
- Defining and maintaining knowledge about how systems relate and ensuring dependencies are understood and managed.
• Performing cost-benefit analysis to determine most appropriate approach to meeting stated requirements.
• Developing operational models to ensure optimal use of resources and meeting appropriate performance levels.
• Ensuring performance of infrastructure is consistent and reliable to deliver the required level of service.
• Defining all tasks required to manage the infrastructure and ensuring tasks are performed appropriately.
• Providing input into the design of configuration data required to manage and track infrastructure and application components.

A brief review of these responsibilities will show that they are not exclusive to service operation but are advantageous to Service Design and Service Transition. In similar fashion, the application analyst/architect role will match service requirements to application specifications, their responsibilities include:

• Working with users, sponsors and other stakeholders to determine evolving needs.
• Working with technical management to determine the highest level of system requirements required to meet service requirements within the constraints of the budget and technology.
• Performing cost-benefit analysis to determine the most appropriate approach to meeting stated requirements.
• Developing operational models to ensure optimal use of resources and meeting appropriate performance levels.
• Ensuring that applications are designed to effectively manage, given the organization's technology architecture, available skills and tools.
• Developing and maintaining standards for application sizing, performance modeling, etc.
• Generating a set of acceptance test requirements.
• Providing input into the design of configuration data required to manage and track application components.
Unlike many other Service Management processes, the Service Transition processes require multiple people unaffiliated with the processes to performed routine and repeatable tasks to meet their intended objectives. For instance in Change Management, the people must likely to “implement” the change are not directly dedicated to the Change Management process, but are members of a technical team and could be operating only direct guidance by another manager focused on a service, a technology, or a process. These people are best described as practitioners.

Here are the responsibilities of these practitioners based on the different Service Transition processes:

• Transition Planning and Support:
  o Maintain and integrate plans for specific Service Transitions.
  o Maintain and monitor progress for Service Transition changes, issues, risks and deviations.
  o Maintain records and provide management information on resource use, Service Transition progress and financial status.
  o Communicate with stakeholders.

• Change Management:
  o Verify requests for change are completed correctly.
  o Allocate requests for change to appropriate change authorities based on defined criteria.
  o Engage change evaluation process by submitting requests for evaluation.
  o Communicate formally decisions of change authorities to affected parties.
  o Monitor and review team and function activities to build and test changes to ensure proper completion of work (for all changes not related to releases).
  o Publish change schedule and projected service outage and ensure availability.

• Release and Deployment Management (release packaging and build practitioner):
  o Help design the release package during the Service Design stage.
  o Establish the final release configuration, including knowledge, information, hardware, software, and infrastructure.
  o Provide input to support authorization to check-in release to the Definitive Media Library.

• Release and Deployment Management (deployment practitioner):

Copyright The Art of Service | Distributed by Quint Wellington Redwood | Accredited by PeopleCert
Help plan service deployment during Service Design stage.

Ensure all deployment activities are authorized by Change Management.

Perform final deployment of physical service components.

Coordinate release documentation and communication, including training and customer, Service Management and technical release notes.

Provide technical and application guidance and supports throughout the release process.

Provide feedback on release effectiveness.

Record and report deployment metrics according to service level agreements.

• Early Life Support Practitioner (Release and Deployment Management):
  
  Provide IT service and business functional support from deployment to final acceptance of a transitioning service.

  Ensure appropriate support documentation is delivered to operational teams.

  Provide release acceptance for providing initial service support.

  Provide support to service desk responding to incidents and known errors detected within a transitioning service.

  Adapt and perfect elements, such as user documentation, support documentation and data management.

  Embed activities for a transitioning service.

  Deal with the final transition of a service-to-service operation and Continual Service Improvement.

  Monitor incidents and problems, raising requests for change when necessary.

  Provide initial performance reporting and assessing service risk based on performance.

• Service Validation and Testing:
  
  Conduct tests as defined in test plans and designs and documented in the Service Design package.

  Record, analysis, diagnose, report, and manage test events, incidents, problems and retests.

  Administer test assets and components.

• Change Evaluation:
  
  Use Service Design package and release package to develop an evaluation plan as input
to service validation and testing.
  o Establish risks and issues associated with Service Transition.
  o Create an evaluation report as input to Change Management.
• Knowledge Management:
  o Identify, control and store any information pertinent to a service which is not available by any other means.
  o Maintain currency, relevance and validity of controlled knowledge items.
  o Monitor assimilation of knowledge polices, processes and tools to ensure no information is duplicated and a central source of information is used across the organization.

12.7.6 Other Roles in Service Transition

In addition to the more general roles described before, each process may have specific roles necessary to support the Service Transition processes. These roles may be fulfilled by anyone dedicated to the process or managed outside of the process. These roles include:

• Change Initiator (Change Management):
  o Identify requirement for change.
  o Complete and submit change proposal, if appropriate.
  o Complete and submit request for change.
  o Attend CAB meeting to provide future information, if invited.
  o When requested by Change Management, review change (especially before closure of change record).
• Change Authority (Change Management):
  o Review specific RFC categories.
  o Formally authorize changes at agreed points in the change lifecycle.
  o Participate in change review before closing change record.
  o Attend CAB meetings to discuss and review changes.
• Change Advisory Board Member (Change Management):
  o Participate in CAB meetings.
  o Represent group or function when authorizing changes.
  o Prepare for CAB meetings by circulating relevant RFCs in group or function and
coordinating feedback.
- Review RFCs and recommend authorization.
- Review successful and failed changes.
- Review unauthorized changes.
- Review change schedule and provide information regarding potential conflicts or resource issues.
- Review projected service outage and provide feedback on potential impact.

- Change Authority Board Chair (Change Management):
  - Determine CAM members and meeting participates.
  - Plan, schedule, manage and chair CAM meetings.
  - Select RFCs for review according to the change policy.
  - Circulate RFCs in advance of CAB meeting to facilitate member’s preparation.
  - Conduct emergency change advisory board (ECAB) meetings when emergency changes are required, according to policy.
  - Select successful and failed changes for review at CAB meetings.

- Configuration Analyst (SACM):
  - Propose scope for Service Asset and Configuration Management.
  - Support the creation of principles, processes and procedures with process owner and process manager.
  - Define the configuration management system structure(s), including CI types, naming conventions, attributes and relationships.

- Configuration Librarian (SACM):
  - Control the receipt, identification, storage and withdraw of all supported CIs.
  - Maintain status information on CIs and provide status to appropriate stakeholders when necessary.
  - Archive superseded CIs.
  - Assist with configuration audits.
  - Identify, record, store and distribute SACM issues.

- Build and Test Environment Manager (Release and Deployment Management):
  - Ensure service infrastructure and application are built to design specifications.
  - Plan the acquisition, build, implementation and maintenance of the ICT infrastructure.
- Ensure all components are from controlled sources.
- Develop an integrated application software and infrastructure build.
- Deliver appropriate build, operations, and support documentation for build and test environments.
- Build, deliver and maintain required test environments.
- Knowledge Creator (knowledge management):
  - Create and share knowledge relevant to the transitioning service.
12.8 Elearning Module 23 & Workbook Review Questions

1. What role is accountable for the delivery of a specific IT service?
   a. Service Owner
   b. Process Manager
   c. Service Desk Manager
   d. IT Operations Manager

2. The role most likely to be working toward integration with other Service Management processes would be?
   a. Service Owner
   b. Process Owner
   c. Process Manager
   d. IT Analyst

3. The operational management of a process is fulfilled through what role?
   a. Service Owner
   b. Process Owner
   c. Process Manager
   d. Shift Leader

4. An Incident Manager is another name for what role?
   a. Incident Management process owner
   b. Incident Management process manager
   c. First-line analyst
   d. Second-line analyst
5. The KEDB is updated by what role?
   a. Problem manager
   b. Incident analyst
   c. Technical operator
   d. Problem analyst

6. Which of the following roles is unlikely to be combined with the service desk manager role?
   a. Incident Management Process Owner
   b. Request Fulfillment Process Owner
   c. Event Management Process Owner
   d. Service Desk Supervisor

7. Which of the following roles are not critical to 24/7 operations?
   a. Service desk supervisor
   b. Shift leaders
   c. First-line analyst
   d. Applications team leader

8. Which organizational structures enable the development of internal performance objectives?
   a. Organization by technical specialization
   b. Organization by activity
   c. Organization to manage process
   d. Organization by geography
13 Technology Considerations

Technology used in service operation is designed and implemented to ensure faster and accurate responses to events, incidents, problems, and service requests. It is prudent the technology is integrated with different tools used for each Service Operation process and other Service Management processes, particularly Change Management, Service Asset and Configuration Management, and Service Design. Automation is a key characteristic of technology development in service operation, as well as self-help facilities to allow the user more control and involvement in managing IT services for themselves.

13.1 Generic Requirements

Many of the technology solutions seen in service operation will have the following generic requirements:

- Self-help capabilities – typically creating a web-based interface to allow users to report incidents make service requests, and obtain status, but can also include access to workarounds and resolutions found in the known error database to resolve incidents on their own.
- Workflow or process engine – enables the organization to predefine and control activities through the process automatically.
- Integrated configuration management system – ensures all information to IT assets, components, services and ancillary configuration items are centrally accessed and managed to all Service Operation processes.
- Discovery/deployment/licensing technology – allows CMS data to be automatically verified
and updated, as well as allow new software to be deployed to appropriate target locations automatically or when requested though self-help interfaces.

- Remote control – allows control of a device or system to be taken remotely when required to resolve incident or problem, make changes or perform routine housekeeping.
- Diagnostic utilities – aids in diagnosing incidents, problems and events which can potentially impact the business adversely.
- Reporting – allows service, process and performance data to be retrieved and used.
- Dashboards – enables visibility into the overall IT service performance and availability levels.
- Business integration – facilitates alignment with the business, its applications and tools.
- SaaS technologies – provides Service Management capabilities over the Internet on a utility basis.

### 13.2 Event Management

Any technology used for purposes of Event Management should consider the following options:

- An interface which is open and usable across multiple environments to allow monitoring and alerts across the entire IT environment.
- Easy, cost-effective deployment.
- Standard agents to monitor most common environments, systems and components.
- Ability to accept any standard event input and generation of multiple alerts.
- Centralized routing of all events to a single location, with option to move to different locations when required.
- Configurable and programmable functionality to correlate similar events.
- Capability to manipulate events through programming after they are generated but before they are communicated.
- Capability to suppress or flag events during periods of scheduled outages.
- Support for design and test stages.
• Programmable assessment and handling of alerts.
• Ability to allow operator to acknowledge an alert and escalate if no response is entered within a defined time frame.
• Ability to provide good reports and report data, as well as feedback into design and transition stages.

13.3 Incident Management

Incident Management technology is concerned with two critical factors: integration with Service Management and workflow management. Within Service Management integration, the following functionality is desirable:

• Efficient entry of incident data, categorization, prioritization, tracking and reporting of incidents.
• Integration with CMS to enable relationships to be automatically discovered and maintained between incidents, service requests, problems, known errors, workarounds, and other configuration items.
• Using the CMS to aid determination of priority and investigation and diagnosis of incidents.
• Ability to predefine and automatically control processes, using a process flow engine.
• Automatic alerts and escalation capabilities.
• Open interface to Event Management tools to allow automatic raising of incident records when failures are imminent.
• Ability to provide self-help and service request assistance through a web interface.
• Integration with KED to allow easier diagnosis, resolution and identification of incidents.
• Easy-to-use reporting capabilities to produce incident-related metrics.
• Diagnostic tools.
• Efficient access to incident histories and summarization of incidents by category.
Workflow management capabilities allow tools to automatically monitor individual incident records to control target times towards resolution and ensure the proper people are working the incidents based on priority and classification. Additionally, escalation mechanisms can be used to automatically notify management of any issues regarding the handling of incidents according to service targets.

### 13.4 Request Fulfillment

Integration of request fulfillment systems is important, particularly with connecting service requests with the incidents and/or events that initiate them. These systems are often found as a special category within the Incident Management technology. Self-help solutions are advantageous because it allows an open interface to users to request services, find information, and make adjustments to their “technology profile” (what services and rights they utilize). Workflow management mechanisms can be established to control the flow of the service request tough the process, ensuring the proper authorizations are made and time frames are maintained.

### 13.5 Problem Management

The Problem Management process has a few technology considerations to address, including:

- ITSM integration to associate problems with related incidents.
- Change integration to automatically raise requests for changes when resolving problems or to associate problems with the changes that cause them.
- Integration with CMS to link problems with the configuration items causing or affected by them.
- Establishment of an effective known error database to store and retrieve known errors.
13.6 Access Management

The following technology considerations should be addressed for Access Management:

- Integration with human resource management technology to enable verification of a user’s identity, required access and track their employment status.
- Directory services technology to enable the assignment of names to resources on the network and allow access to those resources based on user profiles.
- Access Management features in applications, middleware, operating systems and network operating systems.
- Integration with Change Management systems.
- Integration with request fulfillment technology to ensure proper logging of access requests.

13.7 Service Desk

As an entity, the service desk utilizes technology in numerous capacities. At the forefront is an ability to communicate with the customer, usually though telephony technology, specifically:

- Automated call distribution system to allow a single telephone number of be answered by multiple agents.
- Computer telephony integration software to allow caller recognition and automatic population of caller’s information in record.
- Voice over internet protocol to reduce telephony costs.
- Statistical software to gather and analysis telephony data, including.
  - Number of calls received.
  - Call arrival profiles and answer times.
  - Call abandon rates.
  - Call handling rates.
  - Average call durations.
• Hands-free handset capabilities.

The service desk may use a number of support tools including:

• Known error database.
• Diagnostic scripts.
• Self-help web interface for:
  o Frequently asked questions.
  o How-to’s.
  o Service status and alerts on bulletin.
  o Password change capabilities.
  o Software fix downloads.
  o Software repair.
  o Software removal requests.
  o Software downloads.
  o Advanced notice on planned downtimes of service outages.
• Remote access or remote control capabilities.
13.8 Elearning Module 24 & Workbook Review Questions

1. Service operation technology specifically designed for user consumption includes which of the following requirements?
   a. Integration with configuration management system
   b. Remote control of device or system
   c. Diagnostic utilities
   d. Self-help capabilities

2. What feature of Event Management is required from the list below?
   a. Open interface
   b. Integration with configuration management system
   c. Process flow engine
   d. Integration with known error database

3. From a tool perspective, what processes will the Incident Management process not require integration?
   a. Problem Management
   b. Event Management
   c. Change Management
   d. Service Asset and Configuration Management

4. What non-IT function will Access Management interface with?
   a. Change Management
   b. Human resources
   c. Information security
   d. Facilities management
14 Implementing Service Operation

14.1 Managing Change

Change is inevitable. The job of Service Operation is not to resist change, but to ensure the service environment remains stable despite the change. Still, change needs to be controlled and a good working interface with Change Management is necessary to ensure the required stability.

Understanding what triggers a change is important for service organizations, because they can put mechanisms in place to monitor and be notified when change will happen. Some reasons why change occurs:

- New or upgraded hardware or network components.
- New or upgraded applications software.
- New or upgraded system software.
- Changes to legislation, regulations or governance requirements or conformance requirements.
- IT components aging or becoming obsolete.
- Changes in business strategies, plans or requirements.
- Enhancements to processes, procedures or tools to improve IT delivery or reduce financial costs.
- Changes in management or personnel.
- Changes in service levels or service provision.
To ensure operational issues are carefully considered, Service Operation staff should be involved in the assessment of all changes. Ideally, this involvement should begin as early as possible, such as during strategic decisions.

Success in change can be measured by the impact the customer or user experiences in service variation or outage. If nothing is experienced, the change is most successful.

14.2 Project Management

The day-to-day focus of Service Operation may be perceived as justification that project management is not required during this lifecycle stage; however, this is not the case. There are instances when Service Design and transition may not be involved formally, such as the deployment of new or changed procedures.

Project management can achieve the following benefits:

• Clear statement of benefits from the effort.
• Greater visibility in what is being accomplished and how it is being managed; allowing for contributions to be clearly measured.
• Funding can be obtained easily.
• Greater consistency and improved quality in output.
• Higher credibility when objectives are achieved.
14.3 Risk Management

The existence of potential changes and known errors in the service environment are relatively high reasons for assessing and managing risk; however risk is a large part of any Service Operation effort. Service operation staff needs to be involved in the assessment of risk and impact of:

- Failures or potential failures.
- New projects.
- Environmental risks.
- Suppliers or third-party risks.
- Security risks.
- New customers or services supported.

14.4 Operational Support in Other Lifecycle Stages

The involvement of Service Operational staff in Service Design and Service Transition stage ensures that new or changed services are fit for purpose, and:

- Capable of being supported with the existing or pre-agreed resources and skill levels.
- Does not adversely impact other existing technical or operational working practices, processes or schedules.
- Does not unexpectedly increase operational costs or ongoing expenditures.
- Requires no complex support paths, particularly with third-party suppliers.
14.5 Service Management Technologies

In addition to supporting the various components and resourced delivered to the customer in the form of services, service operation is also responsible for maintaining the tools and resources required to ensure that service delivery is successful. This requires the implementation and maintenance of Service Management tools and technology, specifically:

- License management.
- Deployment options.
- Capacity checks.
- Training and knowledge.
1. Which of the following is not a trigger for change in a Service Operation environment?
   a. New hardware component
   b. Upgraded system software
   c. Component depreciation
   d. New personnel

2. Which of the following is not a benefit of project management in Service Operation?
   a. Clearly state benefits
   b. Higher competency
   c. Greater visibility
   d. Greater consistency

3. Where does Service Operation participate in risk assessment and management on a daily basis?
   a. New projects
   b. Use of suppliers
   c. Known errors
   d. Environmental risks
15 Challenges, Critical Success Factors, and Risks

15.1 Challenges for Service Operation

The general challenges to Service Operation include:

- Lack of involvement in design or transition – traditionally, and in some cases because of legislation, the organization deliberately separated those departments responsible for operational duties and those departments delivering new functionality into operational environments. While this separation was intended as a means of separating duties and minimizing collusion, it will sometimes create rivalries and conflict. Sometimes, ITSM is seen as just an operational requirement and has nothing to do with service development or projects.

- Justifying funding for service operation – the ongoing nature of Service Operation makes it difficult to justify funding or investment; a new service will usually have a higher profile in investment planning than improving how a component of service operation performs. However, improvements in Service Operation areas can save money and show a positive ROI better than the introduction of new customers, services, or strategies.

- Differences in perspective across the service lifecycle – the differences in Service Design, Service Transition and Service Operation will often have a significant impact on the management of Service Operation and how it is perceived. For example:
  - Service operation is responsible for multiple services simultaneously, while design and transition efforts will typically focus on a single service at a time.
  - Service operation performs ongoing, repeatable management processes and activities, while design and transition efforts are usually performed as projects: the result is that operational staff may not be available to do project work, which can lead to Service
Designs and transitions that are difficult to operate.

- Metrics for the various lifecycle stages are sometimes radically different. The problems are the costs, performance targets, and schedules estimated in design and transition for operational activities may be difficult to forecast until months of operating. While the design or transition project may be successful because it completed on budget, on schedule and provided the necessary deliverables, it may have delivered a service with poor estimates for operational costs: where the operation management is held responsible for not meeting.

- Service Transition is not always used effectively, particularly in suing Change Management to deploy changes which have already been made without sufficient testing or evaluation of those changes to identify operational issues.

### 15.2 Risks of Service Operation

Risk describes a possible event that can cause harm or loss, or impact the organization's ability to achieve objectives. Risk is measured in terms of probability, vulnerability, and impact. Handling of risk in an organization involves to major activities:

- Risk Assessment.
- Risk Management.

The ultimate risk in Service Operation is the loss of critical IT services to the customer. However, this risk can be appropriately managed through effective Service Operation. The risks affecting Service Operation are:

- Inadequate funding and resources.
- Loss of momentum.
- Loss of key personnel.
- Resistance to change.
• Lack of management support.
• Faulty Service Design.
• Distrust in Service Management.
• Different customer expectations.

15.3 Critical Success Factors in Service Operation

Service Operation executes ongoing, repeatable activities to ensure stable and reliable services are available and delivered to the customer. To do so successfully, the following critical success factors must be in place:

• Management support.
• Business support.
• Operation champions.
• Proper staffing and retention of skilled staff.
• Service Management training.
• Suitable tools.
• Proper testing of new services and components.
• Effectiveness is measurement and reporting.
## 16 Answers to Elearning Module & Workbook Review Questions

### Module 3
1. C  
2. B  
3. D  
4. A  
5. D  
6. B

### Module 4
1. B  
2. A  
3. D  
4. C  
5. A  
6. D  
7. B  
8. C

### Module 5
1. A  
2. D  
3. B  
4. C  
5. D

### Module 6
1. A  
2. B  
3. C  
4. D  
5. A  
6. B  
7. C  
8. C  
9. D  
10. B

### Module 7
1. D  
2. C  
3. B  
4. A  
5. C  
6. B  
7. D

### Module 8
1. B  
2. A  
3. C  
4. D  
5. B  
6. C  
7. A
<table>
<thead>
<tr>
<th>Module 9</th>
<th>Module 10</th>
<th>Module 11</th>
</tr>
</thead>
<tbody>
<tr>
<td>2. A</td>
<td>2. C</td>
<td>2. A</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Module 12</th>
<th>Module 13</th>
<th>Module 14</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. D</td>
<td>1. C</td>
<td>1. A</td>
</tr>
<tr>
<td>5. A</td>
<td>5. B</td>
<td>5. B</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Module 15</th>
<th>Module 16</th>
<th>Module 17</th>
</tr>
</thead>
<tbody>
<tr>
<td>2. D</td>
<td>2. D</td>
<td>2. B</td>
</tr>
<tr>
<td>5. A</td>
<td>5. A</td>
<td>5. C</td>
</tr>
<tr>
<td>Module 18</td>
<td>Module 20</td>
<td>Module 21</td>
</tr>
<tr>
<td>----------</td>
<td>-----------</td>
<td>-----------</td>
</tr>
</tbody>
</table>
17 Glossary

Glossary terms and definitions are based on the content taken from the five ITIL official lifecycle books (SS, SD, ST, SO, CSI) Copyright © AXELOS Limited 2011. Reproduced under license from AXELOS.

<table>
<thead>
<tr>
<th>Term</th>
<th>Definitions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Accounting</td>
<td>In the context of ITSM, this is a synonym for IT Accounting.</td>
</tr>
<tr>
<td>Agreement</td>
<td>A Document that describes a formal understanding between two or more parties. An Agreement is not legally binding, unless it forms part of a Contract.</td>
</tr>
<tr>
<td>Application Management</td>
<td>The Process responsible for managing Applications throughout their Lifecycle.</td>
</tr>
<tr>
<td>Asset Management</td>
<td>(Financial Management) Asset Management is the Business Process responsible for tracking and reporting the value and ownership of financial Assets throughout their Lifecycle.</td>
</tr>
</tbody>
</table>
| Availability            | (Availability Management) (Security Management) 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 measurements of the Business output of the IT Service.  
<table>
<thead>
<tr>
<th><strong>Term</strong></th>
<th><strong>Definitions</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Availability Management</td>
<td><em>(Availability Management)</em> 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.</td>
</tr>
<tr>
<td>Baseline</td>
<td>The recorded state of something at a specific point in time. A Baseline can be created for a Configuration, a Process, or any other set of data. For example, a baseline can be used in:</td>
</tr>
<tr>
<td></td>
<td>• Continuous Service Improvement, to establish a starting point for planning improvements.</td>
</tr>
<tr>
<td></td>
<td>• Capacity Management, to document performance characteristics during normal operations.</td>
</tr>
<tr>
<td></td>
<td>• Configuration Management, to enable the IT Infrastructure to be restored to a known configuration if a Change fails. Also used to specify a standard Configuration for data capture, release or Audit purposes.</td>
</tr>
<tr>
<td>Budgeting</td>
<td><em>(Financial Management)</em> 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.</td>
</tr>
<tr>
<td>Build</td>
<td><em>(Release Management)</em> 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.</td>
</tr>
<tr>
<td>Term</td>
<td>Definitions</td>
</tr>
<tr>
<td>-------------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Business Continuity Plan (BCP)</td>
<td><strong>(IT Service Continuity Management)</strong> A Plan defining the steps required to Restore Business Processes following a disruption. The Plan will also identify the triggers for Invocation, people to be involved, communications etc. IT Service Continuity Plans form a significant part of Business Continuity Plans.</td>
</tr>
<tr>
<td>Business Impact Analysis (BIA)</td>
<td><strong>(IT Service Continuity Management)</strong> 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.</td>
</tr>
</tbody>
</table>
| Business Relationship Management (BRM) | **(Business Relationship Management)** The Process responsible for maintaining a Relationship with the Business. This Process usually includes:  
  • Managing personal Relationships with Business managers.  
  • Portfolio Management.  
  • Ensuring that the IT Service Provider is satisfying the Business needs of the Customers.  
This Process has strong links with Service Level Management. |
<p>| Capacity                             | <strong>(Capacity Management)</strong> The maximum Throughput that a Configuration Item or IT Service can deliver whilst meeting agreed Service Level Targets. For some types of CI, Capacity may be the size or volume, for example a disk drive. |</p>
<table>
<thead>
<tr>
<th>Term</th>
<th>Definitions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Capacity Management</td>
<td>(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.</td>
</tr>
<tr>
<td>Change</td>
<td>(Change Management) The addition, modification or removal of anything that could have an effect on IT Services. The Scope should include all Configuration Items, Processes, Documentation, etc.</td>
</tr>
<tr>
<td>Change Advisory Board (CAB)</td>
<td>(Change Management) A group of people that assists 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.</td>
</tr>
<tr>
<td>Change Advisory Board / Emergency Committee (CAB/EC)</td>
<td>(Change Management) A sub-set of the Change Advisory Board who make decisions about Emergency Changes. Membership of the CAB/EC may be decided at the time a meeting is called, and depends on the nature of the Emergency Change.</td>
</tr>
<tr>
<td>Change Management</td>
<td>(Change Management) 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.</td>
</tr>
<tr>
<td>Charging</td>
<td>(Financial Management) 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.</td>
</tr>
<tr>
<td>Term</td>
<td>Definitions</td>
</tr>
<tr>
<td>-------------------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Configuration Item (CI)</td>
<td>(Configuration Management) 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 CMDB and is maintained throughout its Lifecycle by Configuration Management. CIs are under the control of Change Management. CIs typically include hardware, software, buildings, people, and formal documentation such as Process documentation and SLAs.</td>
</tr>
<tr>
<td>Configuration Management</td>
<td>(Configuration Management) The Process that is responsible for maintaining information about Configuration Items required to deliver an IT Service, including their Relationships. This information is managed throughout the Lifecycle of the CI. The primary objective of Configuration Management is to underpin the delivery of IT Services by providing accurate data to all IT Service Management Processes when and where it is needed.</td>
</tr>
<tr>
<td>Configuration Management Database (CMDB)</td>
<td>(Configuration Management) A Database used to manage Configuration Records throughout their Lifecycle. The CMDB records the Attributes of each CI, and Relationships with other CIs. A CMDB may also contain other information linked to CIs, for example Incident, Problem or Change Records. The CMDB is maintained by Configuration Management and is used by all IT Service Management Processes.</td>
</tr>
<tr>
<td>Cost</td>
<td>(Financial Management) The amount of money spent on a specific Activity, IT Service, or Business Unit. Costs consist of real cost (money), notional cost such as people’s time, and Depreciation. Cost is also used as the name of a Charging Policy that recovers the exact cost of providing the service.</td>
</tr>
<tr>
<td>Term</td>
<td>Definitions</td>
</tr>
<tr>
<td>----------------------------------</td>
<td>----------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Critical Success Factor (CSF)</td>
<td>Something that must happen if a Process, Project, Plan, or IT Service is to succeed. KPIs are used to measure the achievement of each CSF. For example a CSF of “protect IT Services when making Changes” could be measured by KPIs such as “percentage reduction of unsuccessful Changes,” “percentage reduction in Changes causing Incidents,” etc.</td>
</tr>
<tr>
<td>Customer</td>
<td>Someone who buys goods or Services. The Customer of an IT Service Provider is the person or group who defines and agrees the Service Level Targets. The term “Customers” is also sometimes informally used to mean Users; for example, “this is a Customer Focused Organization.”</td>
</tr>
<tr>
<td>Definitive Hardware Store (DHS)</td>
<td><strong>(Release Management)</strong> One or more physical locations in which hardware Configuration Items are securely stored when not in use. All hardware in the DHS is under the control of Change and Release Management and is recorded in the CMDB. The DHS contains spare parts, maintained at suitable revision levels, and may also include hardware that is part of a future Release.</td>
</tr>
<tr>
<td>Definitive Software Library (DSL)</td>
<td><strong>(Release Management)</strong> One or more locations in which the definitive and approved versions of all software Configuration Items are securely stored. The DSL may also contain associated CIs such as licenses and documentation. The DSL is a single logical storage area even if there are multiple locations. All software in the DSL is under the control of Change and Release Management and is recorded in the CMDB. Only software from the DSL is acceptable for use in a Release.</td>
</tr>
<tr>
<td>Term</td>
<td>Definitions</td>
</tr>
<tr>
<td>-----------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Demand Management</td>
<td><em>(Capacity Management)</em> Optimizing the use of Capacity by moving Workload to less utilized times, Servers, or places. Demand Management often uses Differential Charging to encourage Customers to use IT Services at less busy times. Demand Management also makes use of other techniques such as limiting the number of concurrent Users.</td>
</tr>
<tr>
<td>Emergency Change</td>
<td><em>(Change Management)</em> A Change that must be introduced as soon as possible. For example, to resolve a Major Incident or implement a Security patch. The Change Management Process will normally have a specific Procedure for handling Emergency Changes.</td>
</tr>
<tr>
<td>Financial Management for IT Services</td>
<td><em>(Financial Management)</em> The Process responsible for managing an IT Service Provider’s Budgeting, Accounting and Charging requirements.</td>
</tr>
<tr>
<td>Help Desk</td>
<td><em>(Service Desk)</em> 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 interaction. The term Help Desk is often used as a synonym for Service Desk.</td>
</tr>
<tr>
<td>Incident</td>
<td><em>(Incident Management)</em> An unplanned interruption to an IT Service or reduction in the Quality of an IT Service. Any event which could affect an IT Service in the future is also an Incident. For example Failure of one disk from a mirror set.</td>
</tr>
<tr>
<td>Incident Management</td>
<td><em>(Incident Management)</em> The Process responsible for managing the Lifecycle of all Incidents. The primary Objective of Incident Management is to return the IT Service to Customers as quickly as possible.</td>
</tr>
<tr>
<td>Term</td>
<td>Definitions</td>
</tr>
<tr>
<td>---------------------------------------</td>
<td>-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Information Technology (IT)</td>
<td>The use of technology for the storage, communication, or processing of information. The technology typically includes computers, telecommunications, Applications and other software. The information may include Business data, voice, images, video, etc. Information Technology is often used to support Business Processes through IT Services.</td>
</tr>
<tr>
<td>IT Infrastructure Library (ITIL)</td>
<td>A set of Best Practice guidance for IT Service Management. ITIL is owned by the AXELOS and is developed in conjunction with the itSMF. ITIL consists of a series of publications giving guidance on the provision of Quality IT Services, and on the Processes and facilities needed to support them. See <a href="http://www.axelos.com">http://www.axelos.com</a> for more information.</td>
</tr>
<tr>
<td>Key Performance Indicator (KPI)</td>
<td>A Metric that is used to help manage a Process, IT Service or Activity. Many Metrics may be measured, but only the most important of these are defined as KPIs and used to actively manage and report on the Process, IT Service or Activity. KPIs should be selected to ensure that Efficiency, Effectiveness, and Cost Effectiveness are all managed.</td>
</tr>
<tr>
<td>Knowledge Management</td>
<td>The Process responsible for gathering, analyzing, storing and sharing knowledge information within an Organization. The primary purpose of Knowledge Management is to improve Efficiency by reducing the need to rediscover knowledge.</td>
</tr>
<tr>
<td>Known Error (KE)</td>
<td>(Problem Management) A Problem that has a documented Root Cause and a Workarround. Known Errors are created by Problem Control and are managed throughout their Lifecycle by Error Control. Known Errors may also be identified by Development or Suppliers.</td>
</tr>
<tr>
<td><strong>Term</strong></td>
<td><strong>Definitions</strong></td>
</tr>
<tr>
<td>--------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Known Error Database</td>
<td><em>(Service Desk) (Incident Management) (Problem Management)</em> A Database containing all Known Error Records. This Database is created by Problem Management and used by Incident and Problem Management.</td>
</tr>
<tr>
<td>Lifecycle</td>
<td>The various stages in the life of a Configuration Item, Incident, Problem, Change etc. The Lifecycle defines the Categories for Status and the Status transitions that are permitted. For example:</td>
</tr>
<tr>
<td></td>
<td>• The Lifecycle of an Application includes Design, Build, Test, Deploy, Operate, etc.</td>
</tr>
<tr>
<td></td>
<td>• The lifecycle of an Incident includes Detect, Respond, Diagnose, Repair, Recover, Restore.</td>
</tr>
<tr>
<td></td>
<td>• The lifecycle of a Server may include: Ordered, Received, In Test, Live, Disposed, etc.</td>
</tr>
<tr>
<td>Major Incident</td>
<td><em>(Incident Management)</em> The highest Category of Impact for an Incident. A Major Incident results in significant disruption to the Business.</td>
</tr>
<tr>
<td>Operational Level Agreement (OLA)</td>
<td><em>(Service Level Management)</em> An Agreement between an IT Service Provider and another part of the same Business that provides Services to them. For example there could be an OLA with a facilities department to provide air conditioning or with the procurement department to obtain hardware in agreed times. An OLA may also be between two parts of the same IT Service Provider, for example between the Service Desk and a Support Group.</td>
</tr>
<tr>
<td>Policy</td>
<td>Formally documented management expectations and intentions. Policies are used to direct decisions, and to ensure consistent and appropriate development and implementation of Processes, Standards, Roles, Activities, IT Infrastructure etc.</td>
</tr>
<tr>
<td>Term</td>
<td>Definitions</td>
</tr>
<tr>
<td>-------------------------------</td>
<td>--------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Proactive Problem Management</td>
<td>(Problem Management) Part of the Problem Management Process. The Objective of Proactive Problem Management is to identify Problems that might otherwise be missed. Proactive Problem Management analyses Incident Records, and uses data collected by other IT Service Management Processes to identify trends or significant problems.</td>
</tr>
<tr>
<td>Problem</td>
<td>The root cause of one or more incidents.</td>
</tr>
<tr>
<td>Problem Management</td>
<td>(Problem Management) The Process responsible for managing the Lifecycle of all Problems. The primary objectives of Problem Management are to prevent Incidents from happening, and to minimize the Impact of incidents that cannot be prevented. Problem Management includes Problem Control, Error Control and Proactive Problem Management.</td>
</tr>
<tr>
<td>Release</td>
<td>(Release Management) A collection of hardware, software, documentation, Processes or other Components required to implement one or more approved Changes to IT Services. The contents of each Release are managed, tested, and deployed as a single entity.</td>
</tr>
<tr>
<td>Release Management</td>
<td>(Release Management) The Process responsible for Planning, scheduling and controlling the movement of Releases to Test and Live Environments. The primary objective of Release Management is to ensure that the integrity of the Live Environment is protected and that the correct Components are released. Release Management works closely with Configuration Management and Change Management.</td>
</tr>
<tr>
<td>Request for Change (RFC)</td>
<td>(Change Management) A formal proposal for a Change to be made. An RFC includes details of the proposed Change, and may be recorded on paper or electronically. The term RFC is often misused to mean a Change Record, or the Change itself.</td>
</tr>
<tr>
<td><strong>Term</strong></td>
<td><strong>Definitions</strong></td>
</tr>
<tr>
<td>----------</td>
<td>----------------</td>
</tr>
<tr>
<td><strong>Return on Investment (ROI)</strong></td>
<td><em>(Financial Management)</em> A measurement of the expected benefit of an investment. Calculated by dividing the average increase in financial benefit (taken over an agreed number of years) by the investment.</td>
</tr>
<tr>
<td><strong>Risk</strong></td>
<td>The possibility of suffering harm or loss. In quantitative Risk Management this is calculated as how likely it is that a specific Threat will exploit a particular Vulnerability.</td>
</tr>
<tr>
<td><strong>Risk Assessment</strong></td>
<td>The initial steps of Risk Management. Analyzing the value of Assets to the business, identifying Threats to those Assets, and evaluating how Vulnerable each Asset is to those Threats.</td>
</tr>
<tr>
<td><strong>Risk Management</strong></td>
<td>The Process responsible for identifying, assessing and managing Risks. Risk Management can be quantitative (based on numerical data) or qualitative.</td>
</tr>
<tr>
<td><strong>Service Catalog</strong></td>
<td>A Document listing all IT Services, with summary information about their SLAs and Customers. The Service Catalog is created and maintained by the IT Service Provider and is used by all IT Service Management Processes.</td>
</tr>
<tr>
<td><strong>Service Desk</strong></td>
<td><em>(Service Desk)</em> The Single Point of Contact between the Service Provider and the Users. A typical Service Desk manages Incidents and Service Requests, and also handles communication with the Users.</td>
</tr>
<tr>
<td><strong>Service Level Agreement (SLA)</strong></td>
<td><em>(Service Level Management)</em> An Agreement between an IT Service Provider and a Customer. The SLA describes the IT Service, documents Service Level Targets, and specifies the responsibilities of the IT Service Provider and the Customer. A single SLA may cover multiple IT Services or multiple customers.</td>
</tr>
<tr>
<td><strong>Term</strong></td>
<td><strong>Definitions</strong></td>
</tr>
<tr>
<td>----------------------------------------------</td>
<td>--------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Service Level Management (SLM)</td>
<td>(Service Level Management) The Process responsible for negotiating Service Level Agreements, and ensuring that these are met. SLM is responsible for ensuring that all IT Service Management Processes, Operational Level Agreements, and Underpinning Contracts, are appropriate for the agreed Service Level Targets. SLM monitors and reports on Service Levels, and holds regular Customer reviews.</td>
</tr>
<tr>
<td>Single Point of Contact (SPOC)</td>
<td>Providing a single consistent way to communicate with an Organization or Business Unit. For example, a Single Point of Contact for an IT Service Provider is usually called a Service Desk.</td>
</tr>
<tr>
<td>Single Point of Failure (SPOF)</td>
<td>Any Configuration Item that can cause an Incident when it fails, and for which a Countermeasure has not been implemented. A SPOF may be a person, or a step in a Process or Activity, as well as a Component of the IT Infrastructure.</td>
</tr>
<tr>
<td>Standard Change</td>
<td>A pre-approved Change that is low Risk, relatively common and follows a Procedure or Work Instruction. For example password reset or provision of standard equipment to a new employee. RFCs are not required to implement a Standard Change, and they are logged and tracked using a different mechanism, such as a Service Request.</td>
</tr>
<tr>
<td>Underpinning Contract (UC)</td>
<td>A Contract with an external Third Party that supports delivery of an IT Service by the IT Service Provider to a Customer. The Third Party provides goods or Services that are required by the IT Service Provider to meet agreed Service Level Targets in the SLA with their Customer.</td>
</tr>
<tr>
<td>Urgency</td>
<td>A measure of how long it will be until an Incident, Problem or Change has a significant Impact on the Business. For example a high Impact Incident may have low Urgency, if the Impact will not affect the Business until the end of the Financial Year. Impact and Urgency are used to assign Priority.</td>
</tr>
<tr>
<td>Term</td>
<td>Definitions</td>
</tr>
<tr>
<td>-------------------------------------</td>
<td>--------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>User</td>
<td>A person who uses the IT Service on a day-to-day basis. Users are distinct from Customers, as some Customers do not use the IT Service directly.</td>
</tr>
<tr>
<td>Workaround</td>
<td>(Incident Management) (Problem Management) Reducing or eliminating the Impact of an Incident or Problem for which a full Resolution is not yet available. For example by restarting a failed Configuration Item. Workarounds for Problems are documented in Known Error Records. Workarounds for Incidents that do not have associated Problem Records are documented in the Incident Record.</td>
</tr>
</tbody>
</table>


19 Index

A

access  56, 63, 65, 80, 92-3, 107, 122, 124, 129-30, 132, 136, 159-62, 164-9, 190
Access Management   50, 63, 92, 102, 108, 111, 124, 139, 159-60, 162, 164-8, 260, 262-3, 282
access rights   133, 164-6
agreements   71, 133, 166, 177, 185, 188, 225, 232, 253, 296, 304, 306-7
alignment  25, 27, 71, 77, 160, 279
application analyst   267, 269-70
application management   34, 51, 64, 191, 221, 242-3, 251, 268-9, 296
Application Management function   239, 242, 250, 265
application management lifecycle   244-5, 248, 251
application teams   120, 135, 265-7
applications   18, 33, 36-7, 63-4, 77-8, 92, 107, 109, 117, 122, 133, 189, 191, 242-51, 303-4
Applications Management   51, 214, 242
assets   35, 38, 138, 195, 204, 206, 278, 296, 306
audits   157, 166, 181, 190, 259
Authorized request   140, 165, 168
availability   42, 94, 99, 124, 126, 145, 149, 171, 178, 191-2, 199, 207, 210, 213, 258-9, 296-7
availability of services   72, 129, 166, 237
available resources   184, 217-18
AXELOS   15, 30, 38-41, 49, 51, 296, 303
AXELOS Limited   15, 30, 38-41, 49, 51, 296, 309

B
backup   1182, 184-5, 189, 211, 240-1, 269
balance   47, 55, 70, 72, 74, 76, 198, 202-3
baselines   33, 206, 297
Basic Concepts   97, 115, 131, 145, 160
book   15, 32, 247
budgets   88, 269-70, 291, 297
business   23-5, 27, 56-8, 69-72, 112-15, 118-20, 125, 130, 144-9, 151, 170, 194-5, 199-204, 298-9, 306-8
business continuity   61, 298, 308
business objectives   20, 56, 172
business processes   25-6, 28, 41, 186, 237, 244, 296, 298, 303, 308
Business Relationship Management (BRM)   86, 97, 226, 298
business requirements   65, 71-2, 78, 82, 149, 166, 197, 265
business units   34-5, 38-9, 48, 69-71, 80, 132, 300, 307
C

CAB meetings 89, 262-3, 273-4

capabilities 22-4, 30, 33-4, 38, 40, 47, 60-1, 68, 77, 94, 108, 125, 155, 186, 196, 279-80

capacity 42, 103, 124, 179, 186, 194, 196-8, 213, 236-7, 247, 258, 282, 288, 298-9, 302

Capacity Management 28, 99, 108, 124, 196-8, 236, 258, 297-9, 302

centralization 130, 241, 252, 254

Challenges and Risks 110, 126, 140, 155, 167

Change Management 60, 63, 66, 93, 108, 124, 128-9, 137, 139, 154, 197-8, 201-4, 271-4, 284-5, 299-300

Change Management process 67, 106, 118, 137, 236, 271

changed services 71, 78, 88, 99, 131, 154, 181, 204, 226, 287

choice 37, 42, 45

CMS (Configuration Management System) 67, 89, 126, 128, 135, 150-1, 155, 157-8, 191, 198, 202, 205, 207, 233, 280-1, 284

communication 22, 37, 40-1, 50, 77, 84-6, 90, 94, 98, 108, 118, 123, 153, 165, 214-16, 223-4

components 36, 45, 56-7, 68, 72, 80, 93, 101, 129, 135, 154, 171, 173, 186-7, 198, 278-9

conditions 108, 111, 117, 171, 173-6, 178, 210, 245

Configuration 171, 219, 237, 296-7, 299-300

Configuration Item (CI) 33, 93-6, 100-2, 104-5, 107-9, 113, 123, 126, 137-9, 153-4, 200, 205-7, 280-1, 297-8, 300-1, 307-8

configuration items (CIs) 93-6, 101-2, 104-5, 107-9, 113, 123, 126, 137-9, 151, 154, 195, 202, 205-6, 280-1, 297-8, 300-1

Configuration Management 206, 297, 300

configuration management system 67, 126, 128, 135, 150-1, 155, 198, 202, 205, 233, 284
consistency  69, 71, 74, 78, 82, 116-17, 131, 218, 262, 264

console management   182, 210-11, 221, 240-1

contact   64, 125, 214-15, 217, 221, 267, 302, 306-7

content   18, 43, 87, 125, 188, 192, 296, 305

Continual Service Improvement   30, 55, 60-1, 76, 88-9, 91, 95, 154, 177, 248, 309

continuity   82, 103, 264

contributions   48, 178, 237, 286

control   64, 94, 104, 130-2, 170, 173-81, 183, 191-3, 201, 203, 210, 237-8, 264-5, 273-4, 278-9

control activities   102, 175-7, 278

control of Change Management   137, 198, 300

Correlation engines   84, 101, 104-5

costs   33, 35-6, 39, 45, 61-3, 72-4, 130, 133, 139-40, 147-8, 194-5, 231, 236-7, 249-50, 300

Critical Services   90, 160, 171

Critical Success Factor (CSF)   21, 88-9, 109, 125, 139, 154, 166, 169, 290, 292, 301

Critical Success Factors and Key Performance Indicators   109, 125, 139, 154, 166

cultures   23, 74, 203, 215-17

Customer satisfaction surveys   127, 226-7


D

database   107, 137, 157, 170, 187, 189, 300, 304

decisions   59, 74, 77, 82, 98, 100, 133, 180, 233, 243-4, 246, 252-4, 271, 299
demand management  166, 194-5, 197, 302
departments  26, 51, 54, 68, 92, 130, 186, 191-2, 234, 264-5, 290, 304
deployment  46, 78, 131, 191, 204-5, 236, 242, 246-7, 264, 272, 278, 286, 288
Deployment Management  139, 142, 154, 157, 191, 204-5, 247, 258, 271-2, 274
design  55, 59-60, 62, 74, 85, 93, 99, 101, 103-5, 192, 234-5, 242, 244-5, 259-60, 279-80, 290-1
devices  170, 174, 176-9, 184, 187, 210, 238, 269, 279, 284
diagnose  83, 144, 146, 238-9, 241-2, 272, 304
diagnosis  146, 151-2, 157, 200, 223, 280
disruptions  26, 63, 114-15, 120, 122-3, 197-8, 202, 215, 224, 227, 242, 247, 298-9

E

Effective Service Operation  78, 247, 291
efficiency  26, 57, 60, 97, 170, 175, 204, 206-7, 303
Elearning Module  65, 80, 90, 102, 111, 120, 127, 135, 142, 149, 157, 162, 168, 210, 221
Emergency Change  274, 299, 302
environment  22, 50, 55-6, 60, 64, 67-9, 71, 83, 93, 99, 108, 139, 144, 170, 183-4, 239-40
Event Management  48, 50, 63, 66, 92-102, 105-12, 122, 125, 128, 151, 260, 262, 279-80, 284
event management process  105-6, 108, 114
events  52, 63, 84, 93-8, 100-1, 103-9, 111-12, 114, 123-4, 127, 147, 166, 178-9, 182, 198-9, 278-9
evidence  95, 97-8
experience  16, 22, 24, 58, 74, 78, 227, 256
F

facilities  129, 133, 192, 303-4

Facilities Management  64, 193, 214, 221, 240-1, 284

failures  52, 101, 110-13, 120, 148, 179, 183-4, 200, 217, 241, 280, 287

feedback  70, 89, 123-4, 153, 227, 262, 272, 274, 280

filtering  99, 105, 110, 112

financial management  133, 137-9, 153, 195, 206, 212, 236, 249, 259, 296-7, 299-300, 302, 306

First-line analysts  266-7, 276-7

focus  22, 26, 36-7, 39, 56, 60-1, 73, 83, 93, 97, 113, 146, 170-1, 178, 225, 253-4

framework  30, 32, 246-7

fulfillment  55, 133-4, 137-8, 267

functionality  62, 70-1, 80, 90, 109, 160, 194, 210, 236, 242-3, 248, 251

functions  33-4, 47, 50, 52-4, 63-4, 92, 120-1, 182, 213-15, 226, 239, 255-6, 263-4, 273

funding  62, 112, 195, 286, 290

G

generic  228, 235, 257, 259, 261

goal  23, 25, 57, 69, 94, 170, 189, 194-6, 202, 204, 206-7, 223, 242, 252

groups  34, 54, 64, 70, 77, 85-6, 92, 108, 137, 147, 151-2, 174, 180, 189-90, 228, 273

growth  71, 131, 178, 252-3, 255

guidance  30-1, 52, 60-1, 247, 303
H

handling incidents  117, 119, 145, 221
hardware  36, 45, 56, 84, 88, 101, 271, 300-1, 304-5
history  107, 111, 165, 168, 235
human resources  97, 164-5, 168, 219, 236, 284

I

identification  151-2, 175-6, 243, 274, 280
implementation  23, 151, 197, 199, 215-16, 218, 255, 274, 288, 304
improvement actions  37, 200, 248
Incident and Problem Management  139, 197, 304
Incident Management 63, 65-6, 92, 113-16, 118-20, 122-33, 144, 146, 148-9, 151, 260-1, 265-6, 302, 304
incident management process  92, 114-15, 137, 200, 261, 284
incident models  117-18, 121, 146
incident records  101, 118-19, 157, 233, 280, 308
incident resolution  119, 125, 236
incidents  73, 92, 96-8, 109, 112-28, 130-3, 137-40, 144-55, 166-7, 180, 198-200, 266-7, 278-81, 301-2, 304-5, 307-8
information  46-7, 86-9, 97, 100-1, 123-4, 129, 137, 151, 174, 189, 194, 207-8, 273-4, 300, 303
Information Security Management 108, 124, 159, 162, 166, 209, 259
information security policies  159-60, 166
infrastructure  22, 25, 33, 35-6, 74, 77-8, 81, 104, 110, 120, 170, 206, 234-5, 240, 270-1, 297

instructions  129, 137, 139

instrumentation  100, 104, 249

integration  75, 99, 103, 126, 129, 170-1, 203, 226, 243, 254, 276, 280-2, 284

internet  131, 191-2, 218, 279

involvement  72, 74, 92, 235, 278, 286-7, 290

ISPs (Internet Service Providers)  42, 45, 192

ITIL framework  24, 29-30, 32

ITSM  18, 20, 23-4, 26, 28-9, 55, 74, 115, 170, 177, 182, 213, 240, 244, 290


J

job scheduling  182-4, 195, 211, 240-1, 269

jobs  107, 132, 182-3, 240, 285

K

Key Performance Indicator (KPIs)  88-9, 109, 112, 125, 139, 143, 154, 166, 169, 173, 301, 303

key performance indicators  109, 125, 139, 143, 154, 166, 169, 303

knowledge  18, 22, 24, 60, 69-70, 72, 75, 78, 87-9, 120, 155, 205, 208, 210, 217

knowledge management  108, 154, 207-8, 226, 260, 273, 275, 303

Known Error (KE)  83, 88, 109, 123, 126, 128, 135, 144-6, 149-51, 153-4, 157, 262, 268, 280-1, 283-4, 303-4

known error database  128, 135, 144-5, 150, 154, 157, 262, 268, 278, 283-4, 304

known errors  83, 88, 109, 123, 126, 145-6, 149, 154, 157, 219, 262, 268, 272, 280-1, 287, 303
L

leadership  253-4, 264-5
licenses  15, 30, 38-41, 49, 51, 96, 132, 207, 296, 301
lifecycle  47, 64, 94, 113, 118, 129, 144, 206, 242, 296, 299-300, 302-5
lifecycle stages  32, 54, 58-61, 93, 194, 286-7, 291

M

mainframes  51, 186-7
management  23, 35, 54, 64, 69-70, 73, 77, 93, 95, 192-3, 197, 199, 240, 254, 296-306, 308
managers  35, 48, 54, 72, 74, 77, 86, 165, 228, 253-4, 263-5, 271
Material  30, 38-41, 49, 51
maturity  29, 74-5, 170, 172, 223, 252
mechanisms  96, 98-100, 122, 178, 184, 203, 249, 285, 307
meetings  25, 58, 85-7, 98, 258, 264, 270, 274, 291, 298-9
metrics  56, 69, 88-9, 179-80, 200, 225, 237, 259, 291, 303
minutes  17-18, 85, 116, 183
money  27, 35, 37, 72, 290, 297, 300
monitor  73, 90, 93-4, 96-7, 104-5, 108, 111, 117, 134, 148, 164, 176-9, 182, 197, 247, 261
monitor control loop  175-6, 211
monitoring  83, 93-4, 96, 98-102, 167, 173-81, 189, 191-2, 198-9, 210, 225, 232, 238, 240, 266
monitoring agent  175, 177, 179
N

norm  62, 93, 174-5, 179, 210-11
notification  104-5, 138
number  25, 73, 109, 112, 125-6, 128, 131, 139-40, 143, 145-7, 154-5, 166, 180, 217-18, 223-5, 237-8

O

OLAs (operational level agreements)  88, 107, 119, 167, 254, 258, 304, 307
operational activities  72, 78, 82, 173, 197, 205, 207, 236, 239-40, 249, 264, 269, 291
operations bridge  120, 182, 185, 241, 264, 266
Operations Management  34, 51, 64, 214, 221, 235-6, 239-41, 249, 264
operations management activities  95, 239, 241
operators  267, 269, 280
order  17-19, 28-9, 34, 45, 47, 57-8, 63, 65, 67, 71, 113, 117, 139, 147, 202
organization  21-5, 33-7, 60, 69-77, 96-8, 130-3, 146-8, 170-3, 175-6, 178-82, 202-4, 213-15, 239-42, 252-8, 266-9, 277-8
Organization structures  54, 222, 252
organizational objectives  23, 25, 58
organizational structures  51, 54, 255, 277
outcomes  25, 34-6, 39, 41, 48, 69, 177-8, 210, 233
outputs  23, 35, 48, 50, 63, 71, 87, 89, 91, 107, 123, 138, 152-3, 165, 175
package 42-3, 76, 183
parent 95-6, 133, 177-8
Participating 235-6, 248, 257
Participation 78, 85, 205
performance 33, 41-2, 69, 71, 78-9, 83-4, 96-7, 173-6, 178-9, 182-3, 196-8, 210, 225, 236-8, 247-8, 258
person 33, 35, 37, 48, 67-8, 77, 83, 87, 96, 116, 122, 175, 257, 267-8, 307-8
personnel 56, 62, 64, 68-9, 133, 160, 218, 256, 269, 285
perspectives 68, 70, 72, 202, 226, 245, 290
phase 19, 246-7
planning 97-9, 103-4, 198-9, 204-6, 297, 305
plans 18, 33, 58-9, 71, 87, 132, 234, 252, 260-2, 271, 274, 285, 298-9, 301
platforms 109, 170-1, 173, 184, 213
policies 18, 34, 58-9, 87, 90, 97-8, 115, 131, 133-4, 137, 145, 148, 159-60, 164-6, 188-9
power 64, 117, 192-3
practices, best 29, 60, 75
Proactive Problem Management 145, 150, 305
Problem analysts 267-8, 277
Problem Management 50, 63, 66, 92, 102, 108, 113, 144-6, 148-9, 151-8, 197-8, 236, 260-2, 303-5
problem management process 93, 152-3, 249, 281, 305
problem models 145-6, 150
problem records 89, 123, 127, 142, 151-2, 154, 262
problem resolutions  89, 91, 151, 153, 157, 236, 268
problems   64, 75-6, 83-4, 97-8, 106, 144-9, 151-2, 154-6, 180, 186-90, 236-7, 250, 268, 278-81, 303-5, 307-8
Process Activities  105, 122, 137, 151, 164, 240, 261
process manager   35, 48, 257, 259, 261, 274, 276
Process metrics   237-8, 240, 250
process owner   35, 48, 144, 257, 259-61, 274, 276
products   23, 28, 59, 71, 130, 152, 235, 255-6
progress   86, 118, 121, 126, 132, 178, 266
projects   33, 54, 59, 62, 69, 132, 201, 203, 224, 235, 248, 250, 290, 301
providers   35, 39-42, 121, 188, 304
Purpose and Objectives   94, 113, 129, 144, 159

Q
quality  7, 22-3, 26, 37, 47, 68-9, 72-4, 79, 89, 113-14, 124-5, 175-6, 179, 206-8, 224-5, 302-3

R
range   24, 42, 45, 72, 179, 214, 223, 248, 256
Reactive Problem Management   145, 149, 171
release   29, 33, 78, 123, 126, 153, 162, 204-6, 236, 246, 271, 297, 301, 305
Release and Deployment Management  139, 142, 154, 157, 191, 204-5, 247, 258, 271-2, 274
Release Management  297, 301, 305
reliability  170, 199-200, 296
request fulfillment  50, 63, 66, 92, 111, 129-30, 132-4, 138-42, 162, 166, 260, 262, 281
request fulfillment process  92, 132, 135, 137, 140
request fulfilment  129, 139
request models  130-1, 135, 137
request record  132, 137-8, 164, 226
requirements  23, 29, 42, 58, 62, 70, 73-4, 82, 178, 181, 192, 206, 226, 244-6, 270, 298-9
resolution  116-18, 121-5, 127, 144-6, 148-9, 151-4, 180, 184, 266, 268, 278, 280-1, 308
resolving incidents  115, 129, 191, 231, 266-7
resources  26, 35, 38, 47, 60-1, 64, 68-9, 74, 80, 98-9, 116, 195-6, 215, 267, 270, 282
response  19, 94, 97, 106-7, 111, 116, 149, 165, 173, 180, 229, 255, 278, 280
responsibilities  23-4, 34, 50, 52-4, 60-1, 66, 189-91, 203, 213-14, 238-9, 254-5, 257, 259, 261, 263-71
responsiveness  48, 68, 70-2, 80
restore  182, 184, 189, 200, 211, 215, 240, 250, 298, 304
review  62, 65, 78, 86, 106, 132, 137, 152, 201, 258-9, 261-3, 270, 273-4
RFCs (Request for Change)  89, 111, 151, 154, 162, 164-5, 168, 204, 257, 273-4, 305, 307
rights  30, 38-41, 49, 51, 63, 142, 159-61, 163, 167, 190, 281
Risk assessments  201, 287, 289, 291, 306
Risk Management 153, 287, 291, 306
risks 21, 26, 33, 35-6, 39, 47, 126, 140-1, 155-6, 167, 247-8, 287, 290-1, 306
roles 22-4, 34-5, 48, 50, 52-4, 95, 213-14, 223-4, 240, 242, 256-7, 266-7, 269, 273, 276-7
routine 64, 83-4, 94, 170
rules 53, 58-9, 85, 101, 107, 146, 188

S
scenario 15, 18-19
schedules 96, 183, 188, 210, 274, 287, 291
senior management 24, 252, 264-5
servers 51, 97, 170, 186-7, 189, 211, 302, 304
Service Asset and Configuration Management 76, 108, 124, 139, 154-5, 166, 206-7, 258, 274, 278, 284
service assets 39, 202, 206
service being 37, 115, 142, 174
service catalog 46, 88, 128, 135, 139, 150, 160, 177, 195, 223, 258, 306
Service Catalog Management 139, 166, 168
service components 61, 68, 70, 83, 93, 131, 178, 182
service continuity 185, 298, 308
Service Continuity Management 108, 154, 166, 201, 258, 298
service delivery 48, 50, 56, 69, 74, 97, 149, 183, 213, 257-8, 288
Service Design 30, 55, 58-9, 62, 67, 78, 88-91, 93, 102, 172, 177-9, 183-4, 192, 238, 246
Service Design processes 72, 199, 259
Service Design stage  59-60, 131, 198, 205, 271-2


service desk function  133, 215-16, 220

Service Desk Managers  180, 223-4, 263, 276

service environment   61, 67, 83, 93, 115, 152, 159, 173, 178, 221, 285, 287

service improvements   61, 97, 124, 151, 210, 257

service level management   28, 72, 76, 86, 108, 111, 124, 128, 154, 166, 197, 212, 258, 304, 306-7

Service Level Management (SLM)   28, 72, 76, 86, 108, 111, 124, 126, 128, 154, 166, 197, 212, 258, 304, 306-7

service level objectives   98, 123, 127, 157

service level requirements   73, 101, 111, 165, 178, 197, 245

service level targets   177, 206, 262, 298, 301

service levels   63, 95, 119, 134, 154, 197, 216, 285, 307

service lifecycle   20, 30, 54-5, 58, 67, 72, 74, 77, 84, 114, 199, 205-7, 258, 290

service lifecycle activities   92, 259, 261

service lifecycle stages   59, 61-2, 87, 89-91, 194, 238

Service Management   16, 21-6, 29-30, 34, 47-8, 67, 83, 87, 96, 104, 115, 225, 279-80, 305-6

Service Management processes   57-8, 63, 65, 87, 96, 99, 108, 128, 142, 151, 162, 177, 203, 206, 261-3, 300

service managers   181, 225, 232

service operation activities 10, 170, 172-3

service operation processes 21, 66, 92, 95, 102, 109, 111, 131, 209, 265, 278

service operation stage 60, 62, 145, 194

service organization 23, 25, 80, 85, 92, 116, 285

service outages 56-7, 65, 283

service owner 35, 257-8, 261, 276

service packages 41-3, 45

service performance 77, 102, 238, 279

service portfolios 46-7, 87, 92, 172, 233

service provider 23, 30, 35, 40, 45-7, 60, 62-3, 67-8, 70-2, 78-9, 115-16, 118-19, 131-3, 200, 298-9, 306-7

service provision 24, 172, 196, 199, 201, 206, 215, 285

service quality 61, 68, 70, 72-4, 80, 86, 124-5, 154, 178, 202, 208, 211, 224

service request handling 140, 221, 263


service requirements 172, 178, 246, 269-70

Service Strategy 30, 36, 41, 47, 55, 58-60, 72, 87, 89-91, 177, 238, 309

service targets 111, 169, 281

Service Transition 19, 30, 55, 58-60, 78, 88-91, 99, 177, 238, 271, 273, 291, 309

service validation 246, 272-3

severity 115-16, 202

shift leaders 264, 276-7
Single Point of Contact (SPOC) 302, 306-7
situation 60, 63, 73, 75-6, 94, 97, 106, 116, 147-8, 173, 176, 180, 210
skill levels 219-20, 263, 287
skills 24, 36, 64, 75, 155, 158, 210, 214, 223-4, 226, 230, 235, 243, 248, 251, 256
SKMS 59, 88-9, 107, 111
SLAs (Service Level Agreement) 22, 88, 107-8, 167, 181, 197, 225, 250, 300, 306-7
software 45, 56, 84, 101, 190-1, 246, 271, 300-1, 303, 305
specifications 175, 245-6
SPOC (Single Point of Contact) 302, 306-7
stability 30, 68, 70, 74, 80, 239, 241, 247
staff 23-4, 32, 37, 64, 69, 71-3, 75, 125-6, 149, 191, 201, 208-9, 216, 218, 223-4, 239-40
staff members 25, 75, 253-4
stakeholders 23-4, 34, 48, 118, 180, 205, 245, 269-71
standard norm 175, 177, 181
state 59, 73, 93, 95-6, 102, 109, 111, 121, 208
steps 117, 121-3, 133-4, 151, 157, 185, 203, 298, 307
structure 26, 30, 253-4
submitting requests 138, 204, 271
surveys 94, 125, 225-8, 231
systems 58, 67, 69, 71, 73, 80, 83-4, 98, 171, 174, 179, 184-5, 188-90, 210, 236-8, 279
<table>
<thead>
<tr>
<th>Term</th>
<th>Pages</th>
</tr>
</thead>
<tbody>
<tr>
<td>teams</td>
<td>34, 54, 86, 92, 118, 133, 181, 186, 211, 214, 234, 237, 247-8, 257, 265, 268</td>
</tr>
<tr>
<td>technical infrastructure</td>
<td>234, 238-9, 241</td>
</tr>
<tr>
<td>technical management</td>
<td>34, 51, 64, 171, 214, 221, 234-5, 238, 249, 269-70</td>
</tr>
<tr>
<td>technical management function</td>
<td>191, 234-5, 238, 242</td>
</tr>
<tr>
<td>techniques</td>
<td>69, 146-7, 151, 153, 179, 194-5, 197, 227-9, 246-7, 302</td>
</tr>
<tr>
<td>technology</td>
<td>22-3, 26, 41, 54, 56-7, 63, 70-2, 75, 78, 81, 170-3, 214-16, 234-7, 269-71, 278-9, 303</td>
</tr>
<tr>
<td>technology management</td>
<td>70, 170, 237</td>
</tr>
<tr>
<td>Term Definitions</td>
<td>25-6, 296-308</td>
</tr>
<tr>
<td>test</td>
<td>18, 147, 181, 192, 204, 244, 250, 304</td>
</tr>
<tr>
<td>thresholds</td>
<td>107-8, 111, 117, 203</td>
</tr>
<tr>
<td>tools</td>
<td>20, 30, 34, 52, 62, 75, 81, 94, 135, 146-7, 158, 173-4, 188-9, 278-9</td>
</tr>
<tr>
<td>Total number of incidents</td>
<td>125, 128, 140</td>
</tr>
<tr>
<td>training</td>
<td>63, 69, 76, 78, 85, 201, 209, 224, 235, 237, 245, 250, 288</td>
</tr>
<tr>
<td>transition</td>
<td>55, 59-60, 85, 93, 114, 226, 234, 247, 286, 290-1, 304</td>
</tr>
<tr>
<td>trends</td>
<td>75, 94, 98, 145, 152, 155, 197-8, 305</td>
</tr>
<tr>
<td>Underpinning Contract (UC)</td>
<td>88, 119, 126, 156, 307</td>
</tr>
<tr>
<td>underpinning contracts</td>
<td>88, 119, 126, 156, 307</td>
</tr>
<tr>
<td>understanding</td>
<td>18, 20, 36, 48, 58-9, 67, 71-5, 94, 98, 118-19, 134, 145, 170-1, 194, 207</td>
</tr>
<tr>
<td>user requests</td>
<td>129, 132, 208</td>
</tr>
<tr>
<td>user satisfaction</td>
<td>114, 122, 125, 140, 145, 149, 219, 247</td>
</tr>
</tbody>
</table>
users 63-4, 118, 122-3, 129, 131-3, 135-40, 142, 160-1, 164, 166-8, 185, 189-90, 199-201, 216-21, 226-9, 265-6

utility 44-5, 85, 88, 172, 188

V


Value to Business 96, 115, 130, 145, 160

VBF (Vital Business Function) 88, 90, 308

Vital Business Function (VBF) 88, 90, 308

Vital Business Functions 88, 90, 308

W

warning 97, 99, 103, 105-6, 132, 145

workarounds 123-5, 145, 148, 151, 153-4, 208, 219, 250, 268, 278, 280, 303, 308

Workbook Review Questions 65, 80, 90, 102, 111, 120, 127, 135, 142, 149, 157, 162, 168, 210, 221

workload 65, 71, 195, 198