ITIL V3 Foundation Exam Video Mentor

Jill Knapp

PEARSON

800 East 96th Street
Indianapolis, Indiana 46240 USA

ITIL V3 Foundation Exam Video Mentor

ISBN-13: 978-0-7897-4259-9
ISBN-10: 0-7897-4259-4

Printed in the United States of America

First Printing: December 2010

Associate Publisher
Dave Dusthimer

Acquisitions Editor
Betsy Brown

Senior Development Editor
Christopher Cleveland

Managing Editor
Sandra Schroeder

Senior Project Editor
Tonya Simpson

Copy Editor
Water Crest Publishing

Proofreader
Jovana San Nicolas-Shirley

Technical Editors
Charles Betz

Brian Hopper

Publishing Coordinator
Vanessa Evans

Multimedia Developer
Dan Scherf

Book Designer
Gary Adair

Compositor
Mark Shirar

Table of Contents

About the Author

Jill Knapp, ITIL Expert, is the president of Knapp I.T., Inc., a small but mighty IT service management training and consulting firm based in Wilmington, Delaware (www.knapp-it.com).

Jill has authored white papers and industry articles on service desk tools and implementations, outsourced IT management, process redesign, and fixing broken IT teams, all based on her own hands-on technical and professional experience that spans the Big 5 Consulting, medical, legal, financial, pharmaceutical, dot.com, Fortune 500, entertainment, publishing, and high-tech manufacturing industries.

In June 2007, Jill co-delivered the world's first ITIL V3 Foundation Certification class paired with the official ITIL V3 Certification Exam from APMG, and also served on Quint Wellington Redwood's international team to create their official ITIL V3 Foundation courseware. With a degree in education from Montclair State University, Jill is known for her energetic and fun teaching style, and her ITIL Foundation students for the past two years have earned a near-perfect pass rate.

Jill has personally provided consultancy and training services for prestigious clients and talented students from Dell, HP, Nortel, EMC, the Federal Reserve Bank, USDA, SAIC, Research in Motion, Canadian Armed Forces, Lower Colorado River Authority, Austin Energy, and Huntington Bank. Her company, Knapp I.T., Inc., is also a trusted and reliable partner of many training organizations worldwide, such as New Horizons Computer Learning Centers, Knowledge Peak, Third Sky, and ITPreneurs.

Active in the ITIL community as a service operation and team-building buff, Jill applies her past geek experience to turn ITIL concepts into real-world results for her students and clients.

She loves what she does, and she hopes it shows.

Dedication

Dedicated to my first teachers: Mom, Dad, and Jeff. Thank you for making my charmed life possible.

Acknowledgments

Creating this book would not have been possible without a few terrific people:

Jeremy Moskowitz, the Microsoft Group Policy guru, has been my best pal and geeky mentor for more than 16 years, and I remember when he borrowed my computer to write his first book on Windows 2000 Server back in 1999. Ten years later, Jeremy was the matchmaker who put Pearson Education in touch with me, so he is largely responsible for this book's conception.

Sincere gratitude goes to David Dusthimer at Pearson for bringing me on board, and to Betsy Brown, Chris Cleveland, and the rest of the Pearson team for being so easy to work with. Also, special thanks to Amrita Ghattaora from APM Group for assistance navigating the OGC copyright rules.

In addition, I'd like to thank Moira Stepchuk, who encouraged me early in my ITIL/ITSM career and inspired me to venture out on my own and pursue training and consulting full time. More thanks go to Rob "The IT Skeptic" England, whose brilliance, insight, and wry wit make me snarf coffee as I peruse the ITIL-related LinkedIn forums each morning. (Have you signed up for his newsletter at http://www.itskeptic.org? Do it now. I'll wait.)

I also need to shout "Thanks!" to Cale Corbett, a former student (and a great guy) who came up with the "TPS reports" way to remember the three types of measurements in *Continual Service Improvement*. If you get that question right on the exam, thank Cale, not me.

On a personal note, I'd like to thank my partner in crime, Matt Lichtenwalner, for providing several illustrations and diagrams for the book and slide deck ("You can draw!"), and also for his love, comic relief, pep talks, caffeination services, and quiet footsteps while I recorded. More gratitude and love to my dear PhilaDel gang for being smart, snarky, oh-so-talented, and fun, and for still inviting me to do stuff even though I had to turn them all down while I wrapped up this project. (Hot Breakfast!)

Many thanks also to The Industrial Jazz Group and the Joe Trainor Trio, whose albums kept me grinning and bopping throughout the writing process.

Most importantly, I need to thank my first teachers: my parents and my brother. My dad Jay encouraged me to be curious and to reason things out, to dive into technology and projects with a geeky fervor, that there's no such thing as too much horsepower, and to persevere even when the work I was tackling was difficult. My mom Jo-Ann instilled in me a love of language, words, and communication. As my French teacher for three years in middle school, she is (without bias) the best teacher I've ever had. I love that I see her teaching style echoed in my own, and she is directly responsible for every positive student review I've ever received. I draw inspiration from her every day, both inside the classroom and out. My brother Jeff set the bar for coolness and comic timing; he taught me how to correctly use the GOSUB statement on our TI-99/4A, that being smart and capable is hip, owning your own business is do-able, and that there's no occasion that can't be made better with a sing-along around the piano.

We Want to Hear from You!

As the reader of this book, *you* are our most important critic and commentator. We value your opinion and want to know what we're doing right, what we could do better, what areas you'd like to see us publish in, and any other words of wisdom you're willing to pass our way.

As an associate publisher for Pearson Education, I welcome your comments. You can email or write me directly to let me know what you did or didn't like about this book—as well as what we can do to make our books better.

Please note that I cannot help you with technical problems related to the topic of this book. We do have a User Services group, however, where I will forward specific technical questions related to the book.

When you write, please be sure to include this book's title and author as well as your name, email address, and phone number. I will carefully review your comments and share them with the author and editors who worked on the book.

Email: feedback@pearsonitcertification.com

Mail: David Dusthimer
Associate Publisher
Pearson Education
800 East 96th Street
Indianapolis, IN 46240 USA

Reader Services

Visit our website and register this book at www.pearsonitcertification.com/title/9780789742599 for convenient access to any updates, downloads, or errata that might be available for this book.

Introduction

The ITIL V3 Foundation Exam is based on the five core books of the IT Infrastructure Library (ITIL) as released in 2007. To assist students in passing the exam, these five core books are quoted extensively in this *Video Mentor* set, just as they would be in any accredited training class.

As such, it is important to distinguish between the words of the *Video Mentor* author and the text of the ITIL books themselves, both for student comprehension purposes, but also for matters of copyright. Several diagrams in this *Video Mentor* set are taken directly from the ITIL books, and they have been credited as such.

To differentiate, text appearing in this font ("Normal") was written by the *Video Mentor* author, and text appearing in this font ("Quote") is quoted directly from the ITIL volumes and is reproduced under license from The Office of Government Commerce (OGC). Additionally, several diagrams in this *Video Mentor* set are taken directly from the ITIL books, and they have been credited as such.

The author and the publisher have made the best possible effort to ensure copyright compliance.

Additionally, APM Group, OGC's Official Accreditor, is the organization responsible for creating and maintaining the syllabus from which all accredited trainers must teach, and from which all students seeking certification must study. This *Video Mentor* book/DVD set is based on Version 4.3 of the *ITIL Foundation Certificate in IT Service Management* syllabus, which went live in May 2010. This syllabus version includes new material on which students will be tested, and therefore this *Video Mentor* set reinforces these topics. As of this printing, the course syllabus can be found online at http://tinyurl.com/V3FndSyllabus. This *Video Mentor* booklet contains endnotes that provide references to the syllabus sections satisfied by each book section, so you can be sure all material is covered.

Intended Audience

This book/DVD set is the perfect supplement for students learning about the IT Infrastructure Library and preparing for the ITIL V3 Foundation exam via self-study or for students who seek extra clarification on topics not adequately covered in their instructor-led classroom experience.

Using This Book/DVD Set

Neither the book nor the DVD will provide a complete learning experience alone; these materials are meant to be used in tandem.

This printed book includes the formal ITIL language lifted directly from the five core ITIL publications, as well as additional prose. The DVD provides a more casual explanation along with anecdotes, analogies, occasional animations, and a few bad jokes.

To get the most from your purchase, it is recommended that this product be used in the way it was intended to be consumed: by watching the DVD while following along in the book.

This printed book was designed to tackle every bullet point in the latest version of the ITIL Foundation Exam syllabus. You will see footnotes throughout the book directing you to the syllabus points covered in that section.

As of this printing, the course syllabus can be found online at http://tinyurl.com/V3FndSyllabus. If this link is no longer valid, search using the following string: "The ITIL Foundation Certificate in IT Service Management Syllabus." You should choose the search result from the http://www.itil-officialsite.com domain.

Official sample exam questions from ITIL's official accreditor APMG Group (APMG) are available online from EXIN, one of ITIL's official examination institutes. You can access the sample exam here: http://tinyurl.com/ITILFndSampleExam. In addition, other companies have created their own sample exam questions, and the fabulous Rob "The IT Skeptic" England has compiled a sample exam directory on his website: http://www.itskeptic.org/itil-version-3-certification-eight-sources-free-it. While there, please be sure to look around the IT Skeptic's site, sign up for his newsletter, and give him your business; he is required reading for all Knapp I.T. students!

On the Knapp I.T., Inc., website (http://www.knapp-it.com), you can also download an additional lesson that provides another 40 rapid-fire questions and answers, as well as test-taking tips and tricks. Please use the password **VideoMentor** (case sensitive) to download the lesson.

Congratulations on choosing this *Video Mentor* set, which will prepare you for the latest version of the ITIL Foundation Certificate in IT Service Management examination. Good luck!

Chapter 1

Laying the ITIL Groundwork

Lesson 1: ITIL: An Overview

ITIL History

Back in the 1980s, the UK government realized that it was relying heavily on IT and needed guidance to manage it more effectively. In conjunction with consultants from IBM, suppliers, users, and other experts, the UK central government's IT department (back then called the Central Computer and Telecommunications Agency [CCTA]; today known as the Office of Government Commerce [OGC]) collected information on how various organizations were controlling their IT infrastructures and teams.

After analyzing and filtering this information, the CCTA/OGC chose the practices that would work best for them and their customers. Other organizations found the information helpful (even those in the public sector), and a set of books called *Government Information Technology Infrastructure Management* was born in 1985; this ultimately became the IT Infrastructure Library (ITIL).

Originally published as a set of 31 books, ITIL was not widely embraced by the industry until the mid 1990s. To make ITIL more accessible, ITIL was revised and condensed in 1999 and released as ITIL Version 2 ("V2"), which significantly reduced the amount of books to nine. Two books, *Service Support* and *Service Delivery*, became the most used.

In 2005, the OGC started an effort to further improve ITIL. A major refresh project was started, and authors from throughout the industry were appointed to develop Version 3 of ITIL ("V3"), which now consists of five books, as well as several complementary publications and additional information found online.

Today, the OGC owns the copyright to ITIL and has a contract with APM Group (APMG) to be the commercial partner for all certifications. APMG works with other certification agencies (APMG-International, BCS-ISEB, CSME, DANSK IT, DFC, EXIN, LCS, and TÜV SÜD Akademie) to create exams and certifications for both V2 and V3 in several languages.

ITIL practices are not based on any particular technology platform or industry type and do not provide prescriptive, specific guidance. It is a framework, and it is intended to be adapted. Its processes and counsel are applicable to virtually all organizations regardless of size or industry.

What's Better? "Best" or "Good?"[1]

ITIL has long been considered to be a set of IT Service Management best practices, so you need to understand what the term "best practice" means.

A best practice is defined as "an industry-accepted way of doing something that works" and "the best identified approach to a situation based upon observation from effective organizations in similar business circumstances."

However, there is some criticism that says that ITIL is not best practice, it is *good practice*.

Best practices are a book on a shelf; but good practice is how your organization implements them, by combining the guidance provided by best practice, along with proprietary knowledge, public frameworks, standards, academic research, training, and anything else that makes your implementation work for you. For example, Dell's ITIL implementation will be different from HP's ITIL implementation. Even though they are PC manufacturers, they are two different organizations, with different approaches, needs, challenges, proprietary knowledge, and ideas.

The good practices of today become the best practices of tomorrow.

One of the sources of *good practice* is *proprietary knowledge*. Proprietary knowledge is the deeply-embedded, internal (and often poorly documented) knowledge of an organization, and naturally these organizations are not seeking to share this knowledge with others for free. Unless the requesting organization had a near-identical circumstance, using another organization's proprietary knowledge would not be particularly effective. Thus, using publicly available frameworks (such as ITIL) and standards (such as ISO/IEC 20000) is much more attractive because they are validated across a diverse set of environments and conditions, rather than the limited experience of a single organization. Also, public frameworks are more likely to be widely distributed through training or through professional communities.

Governance²

In general, Governance *ensures that policies and strategy are actually implemented and that required processes are correctly followed*. Governance includes defining roles and responsibilities, measuring and reporting, and taking actions to resolve any issues identified. Governance ensures *transparency and fairness* in all transactions.

You might remember back in 2002 when a few corporate giants were behaving unethically, which spawned the Sarbanes-Oxley Act (SOX), which demands corporate transparency and holds executives accountable for any material deficiencies.

Governance comes in many different flavors; Enterprise Governance, Corporate Governance, Financial Governance, and of course, IT Governance. *IT Governance* is "an integral part of enterprise governance and consists of the leadership, organizational structures, and processes that ensure that the organization's IT sustains and extends the organization's strategies and objectives."

The Two Components of ITIL V3

ITIL Version 3 has two main components:

- **The ITIL Core Publications:** Best practice guidance that is applicable to all types of organizations who provide services to a business. There are five core publications (*Service Strategy*, *Service Design*, *Service Transition*, *Service Operation*, and *Continual Service Improvement*), and each of these five books corresponds to one of the five phases of ITIL's service lifecycle.

- **The ITIL Complementary Guidance:** An additional set of publications with guidance specific to industry sectors, organization types, operating models, and technology architectures. Study guides, process templates, and implementation guidance for small companies are also available as part of these complementary materials.

  Some of these complementary materials are printed books, and others are only found online on the ITIL online portal called "ITIL Live."

What makes ITIL V3 different from prior versions of the framework is the availability of these additional, complementary publications.

Note

The contents of these complementary materials are not part of the ITIL V3 Foundation Exam; however, candidates are expected to know that these complementary publications exist and that they contain guidance specific to particular markets and industries.

The Service Lifecycle[3]

From your own study, you already know the five phases of the service lifecycle, beginning with *Service Strategy*, feeding into *Service Design*, which creates a Service Design Package to be handed off to *Service Transition*, where the service is built, tested, and installed. *Service Operation* is the fourth phase and is responsible for keeping our services up and running, as well as providing operational metrics. It is important to reinforce that the *Continual Service Improvement* phase does not necessarily happen last; rather, it is *constantly happening*, as illustrated in Figure 1-1.

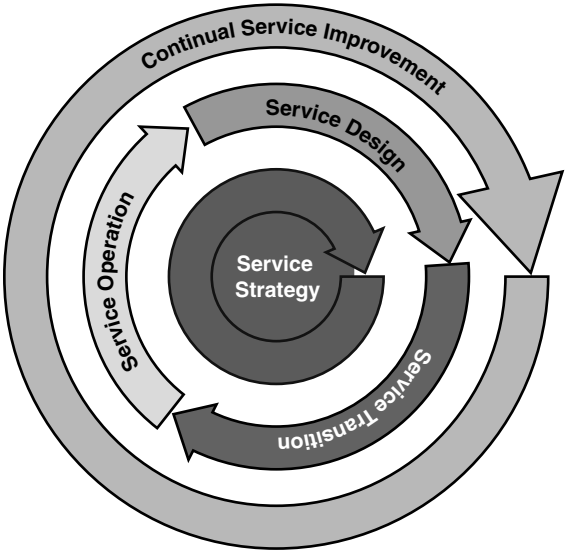

Figure 1-1 Service Lifecycle

There is some debate among ITIL practitioners and experts as to how many processes are truly identified in ITIL V3. For purposes of this *Video Mentor*, we will go with the commonly accepted numbers of **24 processes** and **four functions**.

Eight of the 24 processes are called *Lifecycle Processes* because their activities span all five phases of the service lifecycle. For example, Financial Management is a lifecycle process, because we are always thinking about budgets, accounting, return on investment (ROI), total cost of ownership (TCO), and chargebacks, no matter what phase of the lifecycle you're in or which processes you're executing.

These eight lifecycle processes are

- Service Portfolio Management
- Financial Management
- Capacity Management
- Availability Management
- Supplier Management
- Change Management
- Service Asset and Configuration Management
- Knowledge Management

For purposes of the exam, it is important to remember in which book these processes are first introduced. For example, you might be asked, "Which book contains the processes of Availability Management, Capacity Management, and Supplier Management?" Even though these processes contain activities that are happening throughout the lifecycle, they are introduced and detailed in *Service Design*, so Service Design would be the correct answer.

Earning Your ITIL Certification[4]

As of this writing, there are currently four levels of certification, as described in the list that follows and as illustrated in Figure 1-2. For more depth (which is not needed for the exam), go to http://tinyurl.com/ITILQualificationScheme.

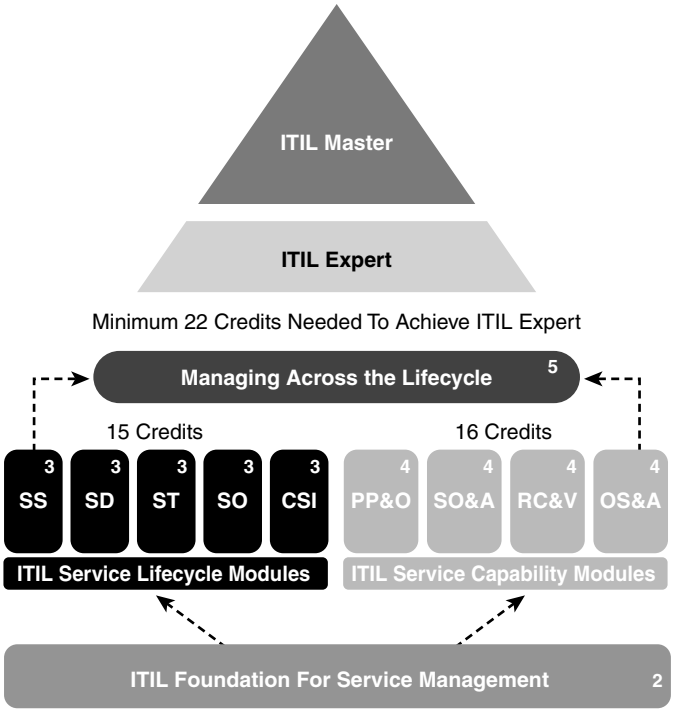

Figure 1-2 Levels of ITIL Certification

1. **ITIL Foundation Certificate in IT Service Management:** Completing this certification earns the candidate two credits toward ITIL Expert status. Please note that the ITIL Foundation certificate in Service Management is *not* intended to enable the holders of the certificate to *apply* the ITIL practices for Service Management without further guidance.
2. **ITIL Intermediate Level:** The Intermediate level classes provide more detail than what can be covered in an ITIL Foundation course. Intermediate classes come in two flavors: Lifecycle Classes and Capability Classes:
   - **Lifecycle Stream:** Each Lifecycle class focuses on only one of the five ITIL books. Lifecycle classes typically are three days in length and are geared more toward students who want to teach, consult, or speak authoritatively on that particular book's contents.

     Each of these certifications are worth three credits toward ITIL Expert status; upon completion of all five certifications in this category, a candidate will have earned 15 credits. The following Lifecycle classes are offered:

     - **SS:** Service Strategy
     - **SD:** Service Design

- **ST:** Service Transition
- **SO:** Service Operation
- **CSI:** Continual Service Improvement

- **Capability Stream:** Capability classes bundle together related processes, even if they span more than one book. These classes are typically four to five days in length (depending on the training provider), and the content is geared more toward practitioners and students who need to implement the processes covered in class.

  Each of these certifications are worth four credits toward ITIL Expert status; upon completion of all four certifications in this category, a candidate will have earned a total of 16 credits. This stream includes four individual certificates, each focusing on detailed process management and implementation:

  - **PP&O—Planning, Protection, and Optimization** (Capacity Management, Availability Management, IT Service Continuity Management, Security Management, Demand Management, and Risk Management).
  - **SO&A—Service Offerings and Agreements** (Service Portfolio Management, Service Level Management, Service Catalogue Management, Demand Management, Supplier Management, and Financial Management).
  - **RC&V—Release, Control, and Validation** (Change Management, Release & Deployment Management, Service Validation & Testing, Service Asset & Configuration Management, Knowledge Management, Request Fulfillment, and Evaluation).
  - **OS&A—Operational Support and Analysis** (Event Management, Incident Management, Request Fulfillment, Problem Management, Access Management, Service Desk, Technical Management, IT Operations Management, and Application Management).

  You may mix and match Lifecycle and Capability classes to earn your credits; however, students aiming for the ITIL Expert certification must ensure that their coursework sufficiently covers all lifecycle phases. The following website (also known as the "ITIL Credit Profiler") provides a handy tool to guide students toward the shortest route to obtaining ITIL Expert status guidance: http://tinyurl.com/ITILQualificationScheme.

  Any student who wants to earn the ITIL Expert status must also take a capstone course called *Managing Across the Lifecycle* and pass the exam as well. The MALC exam is worth five credits toward ITIL Expert status and also proves that the student's knowledge sufficiently covers all five lifecycle phases, handover activities, and process interdependencies.

3. **ITIL Expert:** ITIL Expert Certificate in IT Service Management: The ITIL Expert certification is automatically awarded when a student has earned 22 ITIL credits that show a balanced course of education and passes the capstone *Managing Across the Lifecycle* exam. There is no "ITIL Expert" class or exam. When students have satisfied the requirements, an ITIL Expert certificate is automatically mailed to the student.
4. **ITIL Master:** This highest-level diploma is just now entering a small pilot phase by APMG and is not publically available or attainable as of this writing. Information about attaining

this certification will be posted on the ITIL official website (http://www.itil-officialsite.com) when it is finalized.

It is also important to note that although *individuals* can get certified in ITIL, *organizations cannot*.

There is no organizational certification granted by APMG (ITIL's certifying body). Instead, many organizations strive for **ISO/IEC 20000** certification, which is an organizational certification in IT Service Management based on ITIL.

If you have already earned certifications in ITIL V2, some of your V2 credits can count toward your ITIL Expert certification. Visit this website for an interactive tool called the ITIL Credit Profiler: www.itil-officialsite.com/itilservices/v1/map.asp.

Lesson 2: ITSM/ITIL Key Concepts

Getting Started: Who's Who

Some people casually use the word "customer" instead of using the term "end user" (as in "I have to replace the customer's laptop"). However, the ITIL V3 books make a sharp distinction between these two concepts, with the Customer and a User serving two different roles, as follows:

- **Customer:** Someone who has the authority to request and purchase goods or Services. The Customer of an IT Service Provider is the person or group who defines and agrees to the Service Level Targets in the SLA; perhaps a head of a line of business in an organization.
- **Service Provider:** An Organization supplying Services to one or more Internal or External Customers. The term "Service Provider" is often used as an abbreviation for IT Service Provider.

Remember

The customer has the money. The customer has the freedom to choose the service provider they like best. The service provider must keep the customer happy.

- **Supplier:** A third party responsible for supplying goods or services that are required to deliver IT services. Examples of suppliers include hardware and software vendors, network and telecom providers, and outsourcing organizations.[5]
- **User:** A person who uses the IT Service on a day-to-day basis. They are not paying for the service, they are just using it to do their job. (e.g., Sally in Marketing, and Matt in Human Resources.)

What Is a Service?[6]

In its simplest definition, the word "service" means "doing something for someone else."

Here we see the official ITIL definition of a service:

> Services are a means of delivering value to customers by facilitating the outcomes customers want to achieve without the ownership of specific costs and risks.

You can break this down to its constituent components and apply them to the real-world situation of getting a haircut at a salon:

If your hair is in need of a trim, you will go to a hair salon. By making an appointment at the salon, you are requesting the service, and you are agreeing to pay for that service as well. This makes you the **customer**. You are seeking the **outcome** of shorter hair. Your shorter hair will be of **value** to you if you did not pay three million dollars for the haircut and if it looks good when you leave the salon. The customer does not want to worry about the **costs and risks** of providing the service, which is why she came to a salon instead of cutting her own hair. The customer did not want to invest in attending beauty school, nor did she want the risk of chopping off her ear while she tries to cut her own hair with sharp scissors.

You can also apply this concept to IT. Customers want a specific service such as email, which provides the outcome of fast and reliable written electronic communication. A customer doesn't want the hassle of learning how to manage hardware, maintaining software, and ensuring there is sufficient capacity on the network. Instead, the customer chooses a service provider who has the skills and tools to provide that service, and then pays them for it.

What Is Service Management?[7]

The official ITIL definition of Service Management is

> Service Management is a set of specialized organizational capabilities for providing value to customers in the form of services." Service Management is also "a professional practice supported by an extensive body of knowledge, experience, and skills.

The text goes on to clarify:

> Service Management aims to achieve common understanding between the customer and service provider through managing service level expectations and delivering and supporting desired results.

IT Provides Services, Too

IT Service Management (ITSM) is how to manage the services IT provides to the business.

Remember

Businesses do not buy IT products; they buy IT Services (or solutions).

Why does IT exist? IT is simply an *enabler* for business processes; it helps the business do what the business does in a faster, easier way.

Business services are the services the business provides to its own paying customers. If your business is a gas station, your services might include gas for cars, oil changes, and perhaps a car wash. If your business is a bank, your services might include checking accounts, savings accounts, and mortgages.

Business processes are the internal processes the business uses to make its business work. In a gas station, the gas station manager has a process to follow to get the car wash fixed when it is broken. In a bank, there are processes that need to be followed to see if a new customer has a solid credit history before their mortgage will be approved.

For these business processes to function efficiently and effectively, businesses rely on IT. The gas station manager might send an email to the car wash repair company to send in a maintenance request. A bank loan officer might use the Internet to check a customer's credit score. Email and Internet access are both *IT Services.*

IT provides IT Services to the business by leveraging *IT Components:* servers, routers, PCs, processes, administrators, software, documentation, and so on. In ITIL vocabulary, these *IT Components* are called **Configuration Items**.

Three Types of Service Providers[8]

As you've already learned, a **customer** is defined as *"someone who buys goods or services."* For IT, the customer (the head of a line of business who has the budget and authority to request services from IT) wants to buy IT Services. A typical large company often has multiple business units or departments, which have a different need for IT Services. In this case, there are multiple customers that are looking for services.

Services can be acquired from a service provider, and a service provider can provide any type of service. Within ITIL, the definition of a service provider is

> An organization supplying services to one or more internal or external customers.

This definition is not IT specific; for example, other services can be Human Resources or Payroll. The important part is that a service provider provides services, which differ significantly from the more traditional (tangible) goods.

The ITIL books identify three types of service providers, as illustrated in Figure 1-3 and described in the list that follows:

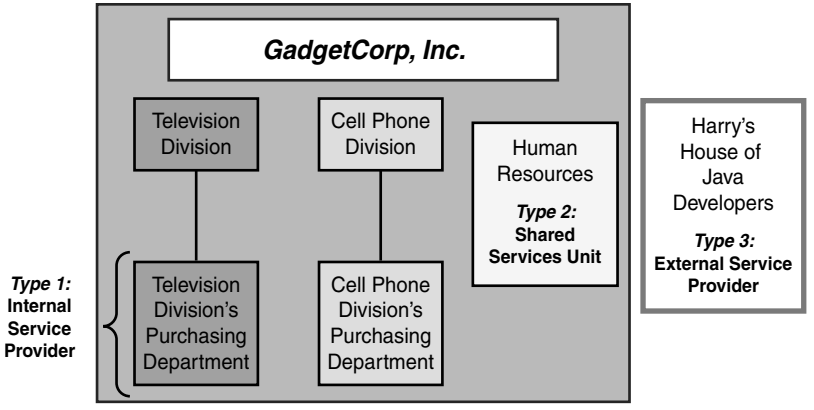

Figure 1-3 Service Provider Types

- **Internal Service Provider:** An Internal Service Provider is established close to the business and is defined as "A Service Provider that is part of the same Organization as its Customer." As depicted in Figure 1-3, the Television Division's purchasing department provides services only to those in the Television Division. They are an internal service provider for those customers in the Television Division.
- **Shared Services Unit:** Many services or departments, such as Accounting, Payroll, and Human Resources, are not part of the core business of many organizations; they exist to support all employees of the company, regardless of what department or division those employees work. These are often consolidated into an autonomous special unit, which is called a *Shared Services Unit (SSU)*. In Figure 1-3, Human Resources is a department that provides services to everyone in GadgetCorp, Inc., regardless of which division or department they work in.
- **External Service Provider:** Sometimes organizations buy goods or services that are provided by external vendors, suppliers, or companies. *External Service Providers* usually provide services to more than one organization. For the example shown in Figure 1-3, Harry's House of Java Developers is not a part of GadgetCorp, Inc., and probably provides Java Development services to many companies around the region, not just to GadgetCorp, Inc.

Where does IT reside in your organization? Depending on the company, IT can live in any one of these three structures.

Process Model[9]

A simple definition: A process is a bundle of logical activities combined to achieve a certain goal (result).

The ITIL definition: A process can be defined as a structured set of activities designed to accomplish a specific objective. A process takes one or more inputs and turns them into defined outputs. A process includes all of the roles, responsibilities, tools, metrics (measurements) and management controls required to reliably deliver the outputs.

Figure 1-4 shows a generic process diagram, with Process Inputs on the left, the process activities itself in the center, and the Process Outputs on the right. Every process requires **process enablers** and is regulated by a **control mechanism**. Figure 1-4 also shows the two major roles in the process: the **process owner** and the **process manager**.

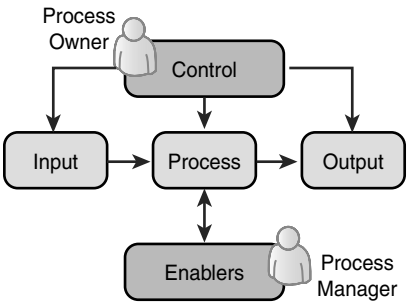

Figure 1-4 Process Diagram

Each process should be owned by a **process owner** who is responsible for documenting the process, educating relevant parties on the process' usage, measuring the process against key performance indicators (KPIs) and critical success factors (CSFs), and using those measurements and metrics to continually improve the process. The objectives of any process should be defined in measurable terms.

In larger organizations, processes might also have a **process manager** assigned who handles the day-to-day management of the process. In smaller organizations, it's normal to combine the roles of process owner and process manager.

Tip

The term "process manager" will not be on the exam.

Process control can be defined as "The activity of planning and regulating a process, with the objective of performing a process in an effective, efficient, and consistent manner."

Process enablers are the process assets—the Resources and Capabilities. Think of enablers as the tangible and intangible "things" that help a process work more efficiently or effectively.

Process Characteristics

Processes have the following characteristics:

- **They are measurable:** Processes must be measured in some relevant manner. "How much did it cost to run this process?" "How many new employees did we enable successfully last month?" "How many incidents did we have last week that were related to new employees having trouble logging in?"
- **They have specific results:** The reason a process exists is to deliver a specific result, and this result must be individually identifiable and countable. "When this process has been completed, a new employee will have a desk assignment, a properly configured laptop that is ready for use, a telephone, an email address, and a network ID."
- **They deliver to customers:** Every process delivers its primary results to a customer or stakeholder; these customers or stakeholders might be internal or external to the organization, but the process must meet their expectations. "The New Employee Enablement Process delivers its results to the new employee, as well as the hiring manager."
- **They respond to a specific event:** Although a process might be ongoing or iterative, it should be traceable to a specific trigger. "The New Employee Enablement Process is kicked off by a hiring manager submitting a completed New Employee Enablement Form to the *newhires* mailbox."

Processes must be measured in terms of their

- **Progress:** What step of the process are we on? How well are we adhering to the process?
- **Effectiveness:** Is the process delivering the desired outcome or result?
- **Efficiency:** Does the process accomplish the goal in the smallest amount of steps possible?
- **Cost-effectiveness:** Are we wasting money as we execute the process activities?

What Is the Difference Between Functions, Roles, and Processes?[10]

Functions are units of organizations specialized to perform certain types of work and are responsible for specific outcomes. Think of **functions** as self-contained units of organizations or teams who share the same goals, typically use the same tools, and also usually have a common budget. ITIL V3 discusses four functions: the Service Desk, Technical Management, Application Management, and IT Operations Management.

Tip

If you see the term "self-contained" on the exam, you should think of the word "function."

Roles are a set of responsibilities defined in a process and assigned to a person or team. A role is not necessarily one's job title. Think of a role as the hat someone wears when they are performing a certain activity. For example, over the course of a workday, a deskside support technician might work on Sally's computer (Incident Management), might investigate the root cause of why a certain model of printer keeps failing (Problem Management), and might install a piece of new software for a user (Release and Deployment Management). This technician's business card says "Deskside Support Technician;" however, he wore many different hats (served in various roles) in just a few hours.

Processes are a logical group of activities performed to deliver a result to a customer or stakeholder. Processes are performed by one or more functions and may include any of the roles, responsibilities, tools, and management controls required to reliably deliver the defined outputs. Processes should always have a process owner.

Remember

- Processes = *What* gets done.
- Functions = *Who* does them.
- Roles = What *hat* you're wearing when you're executing a process.

Roles and Responsibilities: The RACI Model[11]

The RACI Model (sometimes also referred to as a RACI chart or an ARCI chart) is an example of a model that can be used to **assign roles and responsibilities for the activities within a process**.

RACI is an acronym for the four main roles of

- **Responsible:** Executes process and activities. The person or people who actually and physically get the job done. There must be *at least one* "R" allocated to an activity, so you can be sure someone is on point to actually do the work.
- **Accountable:** Ownership of quality and end result of process. *Only one person can be accountable for each task.* This eliminates finger-pointing.

- **Consulted:** The people who are consulted and whose opinions are sought. Involvement through input of knowledge and information. There can be as many people consulted as necessary; having no one consulted is also fine.
- **Informed:** The people that are kept up-to-date on progress, receiving information about process execution and quality. There can be as many people informed as necessary; having no one informed is also fine.

As demonstrated in Figure 1-5, RACI charts come in handy when creating or updating processes, and process owners should get in the habit of including completed RACI charts as part of their process documentation. This ensures that everyone involved in the process knows what he or she is specifically expected to deliver. Conflicts and confusion can be avoided if these roles are determined and documented in advance. Accurate and updated RACI charts ensure that you never hear or utter the phrase, "I didn't know I was supposed to do that."

Tip

Be sure to take note of the words "responsible" and "accountable" as roles and responsibilities are defined (both in this book, but also in your practice).

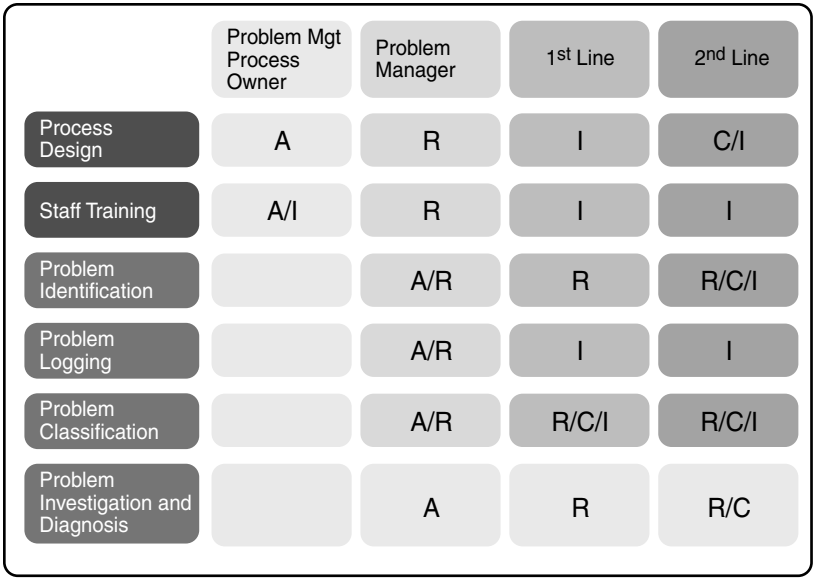

Figure 1-5 RACI Chart

Note

Only one "A'' per row is allowed. Also, at least one "R" is needed per row; this ensures that someone actually does the work.

Process Owners[12] Versus Service Owners[13]

Typically, a process spans several organizational boundaries or departments; therefore, it is important that each process has an owner who has oversight of the hand-offs between organizations and departments. The **process owner** is *accountable* for the overall success of the process. They are *responsible* for ensuring that everyone who is involved in the execution of the process is kept informed of any changes that occur. The process owner is also responsible for ensuring the continual improvement of the process, and as the business' needs change, the process is updated to accurately reflect those changes.

In a simple list, the **process owner**'s (simplified) responsibilities can be represented by the acronym **DEMI**:

- **D**ocumenting and publicizing the process they own.
- **E**ducating relevant staff on the process, **e**nsuring that participants are aware of their role in the process (the RACI model is handy here), and periodically checking in to **e**nsure that participants are still following the process.
- **M**easuring and **m**onitoring the process against the KPIs, CSFs, and other metrics the process owner has chosen (such as progress, effectiveness, efficiency, and cost).
- Continually **I**mproving the progress, effectiveness, efficiency, and cost of the process. (This is done with input and assistance from the Continual Service Improvement phase.)

The **service owner** is *accountable* for a specific service end-to-end. Their role is *responsible* for ensuring that a service is managed with a business focus, and therefore this role is often filled by an IT executive, or someone fairly high up on the organizational chart. The service owner is also responsible for representing the service to the business and can speak authoritatively about the service during Change Management meetings. Additionally, the service owner (with assistance from the Continual Service Improvement Manager) is responsible for the continual improvement of that service so that it is aligned to the changing needs of the business. The service owner is often the party who signs the SLA from the IT side.

Services require processes to make them work. For example, your organization probably offers "Email" as an IT service. You know that in order for "Email" to work, there are many processes that go on behind the scenes (for example, some kind of tape backup process, some kind of Exchange server preventative maintenance process, an archiving-the-logs process, Capacity Management, and so on). Each of these processes (whether ITIL-sanctioned or not) has a **process owner** who ensures that the process is **d**ocumented, that everyone is **e**ducated on how to use the process, that the process' results are **m**easured, and that the process is constantly **i**mproved. The ***service* owner** makes sure the *service as a whole* is working and delivering value to the business. In larger organizations, the service owner is typically an executive of some kind (for example, VP of Messaging) and probably is not the person rebooting the Exchange server at 3 a.m.

Remember

Owners are **R**esponsible for continually improving whatever they own. **Process** owners are responsible for continually improving the **processes** they own; **service** owners are responsible for continually improving the **services** they own.

Lesson 3: Sample Questions Based on Chapter 1

Answers can be found at the end of this chapter.

1. What are the two components of ITIL V3?
    a. The five core books and the itSMF
    b. The itSMF and the complementary publications
    c. The five core books and the complementary publications
    d. The complementary publications and ITIL Live
2. "Services are a means of delivering value to customers by facilitating the outcomes customers want to achieve without the ownership of specific costs and risks." Which entity owns the risks?
    a. The customer
    b. The IT organization
    c. The service provider
    d. The service desk function
3. Which of the following statements is correct?
    1. All processes should have an owner.
    2. A process takes one or more inputs and turns them into defined outputs, such as process reports and reviews.
    3. All processes' objectives must be defined in measurable terms.
    4. All processes must have an objective.
        a. 1 and 2 only
        b. 2 and 4 only
        c. All of the above
        d. 1, 2, and 4

Answers to Sample Questions Based on Chapter 1

1. **C is correct.**

    a. Incorrect. The five core books are correct; but the itSMF is the international user group of ITIL.

    b. Incorrect. The complementary publications are correct; but the itSMF is the international user group of ITIL.

    c. **Correct. The five core books and the complementary publications are the two components of ITIL V3.**

    d. Incorrect. The complementary publications are correct, but ITIL Live refers to the online portion of the complementary publications.

2. **C is correct.**

    a. Incorrect. The customer does not want to own the costs and risks; they want to pay to receive the outcome of the service.

    b. Incorrect. The definition in the first part of the question is the definition of a **service**. We are speaking in general service management terms, and this definition is too limited because it relates only to IT. Anyone can be a service provider, such as a gas station or a restaurant—not only IT organizations.

    c. **Correct. The service provider owns the specific costs and risks of providing a service to a customer. For example, if the customer is seeking a haircut, the service provider has paid to attend school and has earned a license to cut hair; they also own the risk of potentially doing a poor job in cutting the customer's hair.**

    d. Incorrect. This answer is not speaking in broad enough terms.

3. **C is correct.**

    a. Incorrect. Although statements 1 and 2 are correct, so are statements 3 and 4.

    b. Incorrect. Although statements 2 and 4 are correct, so are statements 1 and 3.

    c. **Correct. All statements above are correct.**

    d. Incorrect. All processes must be documented.

Endnotes/Syllabus Requirements

1. This section satisfies Syllabus Requirement ITILFND01-01-1.
2. This section satisfies Syllabus Requirement ITILFND03-03-5.
3. This section satisfies Syllabus Requirement ITILFND02-02-2.
4. This section satisfies Syllabus Requirement ITILFND09-09-1.
5. This section satisfies Syllabus Requirement ITILFND03-03-10.
6. This section satisfies Syllabus Requirement ITILFND01-01-2.
7. This section satisfies Syllabus Requirement ITILFND01-01-3.
8. This section satisfies Syllabus Requirement ITILFND03-03-9.
9. This section satisfies Syllabus Requirement ITILFND01-01-5.
10. This section satisfies Syllabus Requirement ITILFND01-01-4.
11. This section satisfies Syllabus Requirement ITILFND07-07-2.
12. This section satisfies Syllabus Requirement ITILFND07-07-1.
13. This section satisfies Syllabus Requirement ITILFND07-07-2.

Chapter 2

Service Strategy

Lesson 1: Service Strategy Overview[14]

Service Strategy Asks the Big Questions

The word *strategy* means "a long-term plan for success." To get you thinking in this long-term manner, you should start by asking these "big-picture" questions. You will notice these questions have a marketing feel to them:

- What services should we offer and to whom?
- How do we differentiate ourselves from competing alternatives?
- How do we truly create value for our customers?
- How do we capture value for our stakeholders?
- How can we make a case for strategic investments?
- How can Financial Management provide visibility and control over value creation?
- How should we define service quality?
- How do we choose between different paths for improving service quality?
- How do we efficiently allocate resources across a portfolio of services?
- How do we resolve conflicting demands for shared resources?

Service Strategy Scope

The Service Strategy book examines the Service Management practice and provides guidance on setting strategy. The Service Strategy book also aids in understanding service economics, including how to calculate total cost of ownership (TCO), return on investment (ROI), and other financial information. This also helps service providers determine how best to create value for customers by leveraging your resources and capabilities so your services will be chosen over those of your competitors. Finally, Service Strategy provides guidance for setting policies and objectives. Overall, the book aims to improve the strategic impact of Service Management by helping managers confront higher levels of complexity, uncertainty, and conflict.

Tip

If an exam question sounds like marketing or long-term planning (such as setting policies and objectives), think *Service Strategy*.

Service Strategy Processes

There are four processes found in the Service Strategy book. The first process, **Strategy Generation**, is no longer part of the May 2010 ITIL V3 Foundation Syllabus (syllabus version

4.3). No questions surrounding this process appear on the exam; therefore, it is not included in this *ITIL V3 Foundation Exam Video Mentor*.

The remaining three Service Strategy processes are covered here:

- **Service Portfolio Management:** Creating a Service Portfolio and managing it for value and risk.
- **Financial Management:** Understanding and controlling costs associated with IT.
- **Demand Management:** Understanding and predicting the customer's demand for services and providing that information to Capacity Management.

Service Strategy Deliverables

The outputs of Service Strategy are as follows:

- A Service Portfolio.
- A list of business requirements that you seek to satisfy or business challenges that you seek to solve. Specifically, any agreed, new, or changed business requirements.
- In addition, the outputs include any business strategies, policies, and constraints, so that Service Design can work within and around them.

It is important to note that Service Strategy is not the time to discuss *functional* requirements; functional requirements are dealt with in *Service Design*. *Service Strategy* deals only with gathering higher-level *business* requirements.

Creating Value[15]

To provide services that your customers actually want, you have to put on your marketing hat to determine what your customers find valuable.

Consider the example of a chain restaurant that most people have heard of—Applebee's—to describe what influences a customer's opinion of a service provider.

The value of a service to a customer is influenced by the following:

- **The attributes of the service:** These are the actual, objective characteristics of the service. Applebee's is a chain restaurant that serves lunch and dinner and also has a bar. It is not considered fine dining, but it's not a greasy-spoon truck stop either. These facts are not up for debate. Applebee's as a company has direct control over these attributes.
- **The customer's perceptions:** "My friends say that Applebee's doesn't have very much for vegetarians," or "Applebee's is the perfect way to start off a date night." Applebee's has *some* control over a customer's perceptions; advertising can be used to sway a customer's opinions and views.
- **The customer's pre-established preferences:** Customers have their own habits, lifestyles, likes, and dislikes. "I prefer to eat at restaurants with linen napkins," or "I prefer a quick,

unpretentious meal." Applebee's cannot do very much to change a customer's preferences; customers like what they like.

- **Actual business outcomes:** These business outcomes describe what a customer experiences when they actually use the service. "Applebee's provided me with a tasty meal for less than $15, and we got out of there in 45 minutes; it was solid." or "The server was snippy and he never brought out our appetizer." Applebee's has control over this as well.
- **The customer's self-image or position in the market:** How do customers feel when they think of themselves using the service? "I feel pretty hip when I'm sitting in an Applebee's with my all friends after work; they have great margaritas, and it's easy to meet interesting people there," or "I'd rather eat at the fancy bistro down the street, but Applebee's fits my budget a bit better."

Remember

A customer's perceptions of the service provider (or the services provided) can greatly influence the value they place on the service.

Calculating Value[16]

The formula for calculating value is Utility + Warranty.

Utility means that the service is **fit for purpose**. "Does the service do what I need it to do?" *Utility* is perceived by the customer from the attributes of the service that have a positive effect on the performance of tasks associated with desired outcomes. Removal or relaxation of constraints on performance is also perceived as a positive effect.

Warranty means that the service is **fit for use**. "Will the service be available and usable when I need to use it?" *Warranty* is derived from the positive effect being available when needed, in sufficient capacity or magnitude, and dependably in terms of continuity and security.

Utility is *what* the customer gets, and warranty is *how* it is delivered.

As an example, an IT organization provides an application to process invoices. This application is very effective; users love it because it has a great interface and it gets the job done quickly. However, the application is down quite often. You can say that the application has **high utility but low warranty** because the application does what it is supposed to do (provides the desired outcomes, which means *high utility*), but it is broken quite often (it is not working dependably in terms of availability, capacity, continuity, or security, which means *low warranty*).

Service Assets: Capabilities and Resources[17]

An asset is simply something that an organization *has*; it can be something tangible (a server) or intangible (skills or expertise). A more formal definition of a Service Asset is anything that could contribute to the delivery of a Service.[18]

Service assets can be one of the following types: Management, Organization, Process, Knowledge, People, Information, Applications, Infrastructure, and Financial Capital.

As illustrated in Figure 2-1, assets fall into two categories: **Capabilities** and **Resources**.

Organizations use them to create value in the form of goods and services.

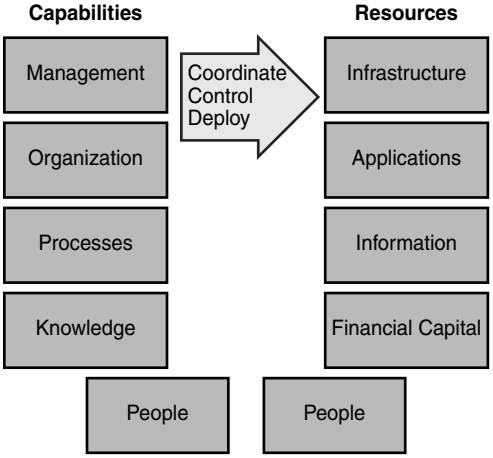

Figure 2-1 Resources and Capabilities Are Service Assets, Which Are the Basis for Value Creation

Capabilities

Capabilities represent an organization's ability to coordinate, control, and deploy resources to produce value. They are typically experience-driven, knowledge-intensive, information-based, and firmly embedded within an organization's people, systems, processes, and technologies. Capabilities are intangible.

Resources

Resources are direct inputs for production. Resources (Infrastructure, Applications, Information, Financial Capital, and People) are tangible.

Note

Note that "People" fall into both categories because people have capabilities (skills), but they are also considered a resource (they are tangible).

It is much easier to acquire resources compared to capabilities. You can walk into a computer store and purchase a piece of hardware (a resource), but you cannot simply purchase the knowledge (capability) to do something useful with that piece of hardware. A service provider must use their capabilities to differentiate themselves from competitors because their resources could very well be the same.

For example, if you are seeking a cup of coffee, you can go either to a gas station or to a fancy café. Both serve coffee (coffee being a resource; it is a tangible aspect of the service); however, only the café serves freshly ground, single-origin coffee prepared by skilled baristas. The *skills* of the barista and the *quality* of the coffee beans (both capabilities; both intangible) make most people agree that the café would serve "better" coffee. Better coffee is more valuable, which is why you pay $2.79 for a cup of this café coffee, but only $.69 for a cup of gas station coffee.

Lesson 2: Service Portfolio Management[19]

Service Portfolio Management spans across the service lifecycle.

The Service Portfolio is a **tool** used to represent services (and an organization's investments in them) in terms of their business value. It allows the business (and IT) to prioritize investments in services across the enterprise and manage them for value, just like a stock portfolio enables you to prioritize your investments in the stock market and manage them for value.

The Service Portfolio is created, managed, and supported through the **Service Portfolio Management process**.

The Service Portfolio has three components:

- Planned services are found in the **Service Pipeline**.
- The **Service Catalogue** contains all current, operational services, as well as those that are staged for implementation (that is, thoroughly built and tested, and simply awaiting their "go live" date).[20]
- Archived services are stored in the **Retired Services**.

The Service Portfolio helps to clarify the following strategic questions:

- Why should a customer buy these services?
- Why should they buy these services from us?
- What are the pricing and chargeback models?
- What are our strengths and weaknesses, priorities, and risks?
- How should our resources and capabilities be allocated?

The Service Portfolio represents the commitments and investments made by a service provider across all customers and market spaces.

Lesson 3: Financial Management[21]

Financial Management spans across the service lifecycle.

Remember

Every process owner's job is to report on their process' progress, effectiveness, efficiency, and *cost.* This means that every process (whether an ITIL process or your own company's internal process) has to be examined in a financial light. For example, if we apply this to the Problem Management process:

- How much does it cost to run this process?
- How much money can we save if we eliminate these recurring incidents?
- How much did it cost to implement this change?
- How can we improve the Problem Management process to reduce the cost of diagnosing problems?

One of the goals of Financial Management is to quantify the value of IT services in financial terms; this is called *Service Valuation*.

There are three main activities associated with Financial Management:

- **Budgeting:** The activity of predicting and controlling the spending of money. This consists of a periodic negotiation cycle to set budgets (usually annual) and the day-to-day monitoring of the current budgets.
- **IT Accounting:** The Process responsible for identifying actual costs of delivering IT Services, comparing these with budgeted costs, and managing variance from the Budget.
- **Charging:** Requiring payment for IT Services. Charging for IT Services is optional, and many Organizations choose to treat their IT Service Provider as a Cost Centre.

Business Case[22]

A business case is a decision support and planning tool that projects the likely consequences of a business action. The consequences can take on **qualitative and quantitative dimensions**. A financial analysis, for example, is frequently central to a good business case.

Intangible benefits (soft benefits) should not be the cornerstone for a business case, however. Instead, business cases should focus on the tangible, quantitative, or qualitative aspects.

For example:

"If we invest $50,000 in our service desk, our team morale will improve." Morale is not really measurable or tangible, even though it's important in a team. A better basis for a business case might be, "If we invest $50,000 in our service desk, our team will achieve a 30% increase in first call resolution rates." This 30% reduction is measurable, and therefore preferable for a business case.

Lesson 4: Demand Management[23]

The main objectives of Demand Management are to understand user demand for IT services, possibly influence their demand, and provide solid planning data to the Service Design process of Capacity Management. Demand Management also seeks to eliminate excess capacity because it's silly to pay for what you're not using.

The Demand Management key concepts are as follows:

- **Patterns of Business Activity (PBA):**[24] There may be certain times of the day/month/year the business behaves in a way that impacts IT. For example, if your employees get paid on the 15th and the 30th of the month, your payroll department (and payroll processing applications and servers) are going to be working extra hard on the 14th and the 29th of the month as it churns out paychecks and calculates remaining vacation time. IT can use this information to ensure that payroll-related services are not down for preventative maintenance on those days.
- **User Profiles (UP):**[25] Certain users may use services differently than other users. For example: Individuals who work in Marketing need access to color printing services. Individuals who work in Executive Sales require remote access, after-hours support, and higher-end laptops. Individuals who work in Finance need stable PCs and access to financial applications from 7 a.m. to 6 p.m. Monday through Friday.

Demand Management goes hand-in-hand with Capacity Management (which is part of *Service Design*). Demand Management identifies the PBAs here in the Service Strategy phase so Capacity Management can then design a solution to meet the demand.

Demand Management is challenging, mainly because services cannot be manufactured in advance, unlike widgets or goods. Services are being used and consumed while IT is providing them, so it can be difficult to measure the true demand for services.[26]

Lesson 5: Sample Questions Based on Chapter 2

Answers can be found at the end of this chapter.

1. Which of the following is *not* a primary concern of Service Strategy?
    a. Providing guidance on setting strategy
    b. Setting policies and objectives
    c. Understanding how to create value for customers
    d. Defining a Release Plan

2. Which of the following statements is *incorrect* about patterns of demand generated by the customer's business?

    a. Demand can be influenced by charging different rates at different times.

    b. They are delivered to the Capacity Management process so the capacity to deliver services at the agreed levels can be ensured.

    c. They are driven by patterns of business activity.

    d. Understanding patterns of business activity is unimportant.

3. What are the three elements of the Service Portfolio?

    a. Service Portfolio, Business Service Catalogue, Technical Services Catalogue

    b. Service Knowledge Management System, Service Portfolio, Service Lifecycle

    c. Service Pipeline, Service Catalogue, Retired Services

    d. Chartered, Operational, Retired

4. True or False? A customer's perceptions, customer's pre-established preferences, and actual business outcomes all influence the value of a service.

5. Which of the following is the correct description of "utility"?

    a. A customer or organization doing business with an electrical or water-services company.

    b. The service is fit for use.

    c. An assurance of certain levels of availability, capacity, continuity, and security.

    d. The attributes of the service that have a positive effect on the performance of activities, objects, and tasks associated with desired outcomes.

Answers to Sample Questions Based on Chapter 2

1. **D is correct.**

    a. Incorrect. Providing guidance on setting strategy is a primary concern of *Service Strategy*.

    b. Incorrect. *Service Strategy* is concerned with long-term planning, which includes setting policies and objectives.

    c. Incorrect. Creating value for customers is a primary concern of *Service Strategy.*

    d. **Correct. Release Plans would be defined in the Service Transition phase of the Lifecycle.**

2. **D is correct.**
    a. This option is a true statement, which means that it is the wrong answer, because this question is seeking the incorrect statement. Customers' usage can be influenced by how much customers need to pay at certain times of day. (Think about how your cell phone company provides free nights and weekends.)
    b. This option is a true statement, which means that it is the wrong answer, because this question is seeking the incorrect statement. Capacity Management and Demand Management go hand in hand.
    c. This option is a true statement, which means that it is the wrong answer, because this question is seeking the incorrect statement. PBA are based on patterns of demand generated by the customer's business.
    d. **This option is a false statement, which means that it is the correct answer. Understanding PBA is critical to the success of Demand Management and to ITSM as a whole.**
3. **C is correct.**
    a. Incorrect. The Business Service Catalogue and the Technical Service Catalogue are the two aspects of the Service Catalogue, not the Service Portfolio.
    b. Incorrect. This answer does not contain any valid elements of the Service Portfolio.
    c. **Correct. The Service Pipeline, the Service Catalogue, and the Retired Services are the three elements of the Service Portfolio.**
    d. Incorrect. These are not the official ITIL names of the subsections of the Service Portfolio, but rather the descriptions of them.
4. **True.** In addition, the attributes of the service, the actual business outcomes, and the customer's self-image or position in the market also influence the value of a service.
5. **D is correct.**
    a. Incorrect. This definition of utility is unrelated to ITIL.
    b. Incorrect. This is a description of "warranty."
    c. Incorrect. This also describes "warranty."
    d. **Correct. This is the description of utility, which means the service is fit for purpose.**

Endnotes/Syllabus Requirements

14. This section satisfies Syllabus Requirement ITILFND02-02-3.

15. This section satisfies Syllabus Requirement ITILFND04-04-2.

16. This section satisfies Syllabus Requirement ITILFND03-03-1.

17. This section satisfies Syllabus Requirement ITILFND03-03-2.

18. This section satisfies Syllabus Requirement ITILFND03-03-34.

19. This section satisfies Syllabus Requirement ITILFND03-03-3.

20. This section satisfies Syllabus Requirement ITILFND03-03-4.

21. This section satisfies Syllabus Requirement ITILFND05-05-22.

22. This section satisfies Syllabus Requirements ITILFND05-05-22 and ITILFND03-03-6.

23. This section satisfies Syllabus Requirement ITILFND05-05-21.

24. This section satisfies Syllabus Requirement ITILFND05-05-21.

25. This section satisfies Syllabus Requirement ITILFND05-05-21.

26. This section satisfies Syllabus Requirement ITILFND05-05-21.

Chapter 3

Service Design

Lesson 1: Service Design Overview

It is important to remember that this phase of the lifecycle is only concerned with **designing** services (or aspects of services). You do not buy or build anything in this phase. Think of Service Design as the phase where you use the whiteboard to make a lot of flowcharts, documentation, and infrastructure diagrams, but you're not getting your hands dirty otherwise. This phase is all about careful and patient designing.

Main Goals and Objectives of Service Design[27]

Some of the goals and objectives of Service Design are to:

- Design services to satisfy business objectives, based on the quality, compliance, risk and security requirements, delivering more effective and efficient IT and business solutions and services aligned to business needs by coordinating all design activities for IT services to ensure consistency and business focus
- Design services that can be easily and efficiently developed and enhanced within appropriate timescales and costs and, wherever possible, reduce, minimize or constrain the long-term costs of service provision
- Design efficient and effective processes for the design, transition, operation and improvement of high-quality IT services, together with the supporting tools, systems and information, especially the Service Portfolio, to manage services through their lifecycle
- Identify and manage risks so that they can be removed or mitigated before services go live
- Design secure and resilient IT infrastructures, environments, applications and data/information resources and capability that meet the current and future needs of the business and customers
- Design measurement methods and metrics for assessing the effectiveness and efficiency of the design processes and their deliverables
- Produce and maintain IT plans, processes, policies, architectures, frameworks and documents for the design of quality IT solutions, to meet current and future agreed business needs
- The assembly of a Service Design Package (SDP) for the subsequent transition, operation, and improvement of the new or changed service solution

Tip

In a nutshell, if something needs to be designed, it is designed in this *Service Design* phase.

Value to the Business[28]

The following business benefits are a result of a careful and conscientious Service Design practice:

- To ensure the achievement of business objectives after the service goes live in the Service Operation phase
- Implementation of new or changed services is easier because the services are designed well
- More effective Service Management and IT processes because you take the time to carefully design them here in Service Design
- To ensure the services you ultimately deliver in Service Operation have a means to be measured because you make sure you design the ability to pull the right metrics
- Reduced Total Cost of Ownership (TCO): If all aspects of services, processes, and technology are designed properly (and subsequently implemented, of course), you can ultimately reduce TCO

The Five Aspects of Service Design

The five aspects of Service Design describe what items actually get designed in this phase of the lifecycle. As you can see, it's a pretty comprehensive list, which is why I always tell my students to keep it simple: "We design *everything* in the Service Design phase. Period."

Tip

For the exam, an easy way to remember the Five Aspects of Service Design is that the key words of each aspect spell out **STAMP** if you change the order a little bit (otherwise, it spells "STAPM," which is just silly).

The five aspects of Service Design are as follows:

- **Designing the *S*ervice solutions for new or changed services**, which entails identifying business requirements and defining Service Requirements and the design of services, including all the *functional requirements*, resources, and capabilities needed and agreed.
- **Designing the Service Management systems and *t*ools, especially the Service Portfolio and the Service Catalogue**, for the management and control of services through their lifecycle. (This also includes other tools that assist with the "big picture" of managing your ITIL / Service Management initiative, such as your Service Desk tool.)
- **Designing the technology *a*rchitectures and management systems** to provide and manage the services.
- **Designing the required *p*rocesses** to ensure that the processes, roles, responsibilities, and skills have the capability to operate, support, and maintain the new or changed service. This includes all IT and Service Management processes, not just the key Service Design processes; for example, processes needed to design, transition, operate and improve the services.

- **Designing the *m*easurement methods and metrics** to ensure that the existing measurement methods can provide the required metrics on the new or changed services, architectures, constituent components, CIs, and processes when we reach Service Operation.

The most effective IT service providers integrate all five aspects of design rather than design them in isolation. [...] This integrated design ensures that when a new or changed service is implemented, it not only provides the functionality required by the business, but also meets and continues to meet all its service levels and targets in all areas. This minimizes rework.

The Service Design Package[29]

A Service Design Package (SDP) can be thought of as a blueprint, containing everything Service Transition will need to build, test, and implement this new, changed, or retired service. It also contains everything necessary for this service's subsequent operation and improvement as well.

A Service Design Package is created during the Service Design phase of the lifecycle and is passed directly to the Service Transition phase, but it will also be referred to during Service Operation and CSI, too.

The Service Design Package:

- Details of all aspects of a service
- Details requirements through each lifecycle stage
- Is based on SLRs (Service Level Requirements) passed on from Service Strategy
- Is passed on to Service Transition for implementation

The SDP contains the following:

- Requirements:
  - Business Requirements
  - Service applicability
  - Service contacts
- Service Design details:
  - Service functional requirements
  - Service Level Requirements
  - Service and operational management requirements
  - Service Design and topology
- Organizational Readiness Assessment
- Service Lifecycle plan:
  - Service Program
  - Service Transition Plan

- Service Operational Acceptance Plan
- Service Acceptance Criteria

An SDP is produced for each new service, major change, or IT service retirement.

Tip

For the exam, keep it easy. If you are asked what goes into a Service Design Package, just remember that the SDP contains everything including the kitchen sink. If you're given a list of items that might be included, look for an "All of the above" option for your answer.

The Service Design Manager

The Service Design Manager has a key role to play within Service Design.

They are responsible for the overall coordination and deployment of quality solution designs for services and processes. Responsibilities of the role over and above those of line management of all people involved in Service Design roles include:

- Taking the overall Service Strategies and ensuring they are reflected in the Service Design practice as well as the Service Designs that are produced to meet and fulfill the documented business requirements
- Designing the functional aspects of the services as well as the infrastructure, environment applications and data management
- Producing quality, secure and resilient designs for new or improved services, technology architecture, processes or measurement systems that meet all the agreed current and future IT requirements of the organization
- Producing and maintaining all design documentation, including designs, plans, architectures and policies
- Producing and maintaining all necessary Service Design Packages
- Measuring the effectiveness and efficiency of the Service Design process

The Four Ps of Service Design[30]

Many designs, plans, and projects fail through a lack of preparation and management.

The implementation of ITIL Service Management as a practice is about preparing and planning the effective and efficient use of the Four Ps. Ensure you attend to the:

- People
- Processes
- Products (technology, tools, and services)
- Partners (suppliers, manufacturers, and vendors)

Your design should consider each of these Four Ps carefully.

Automation Considerations

Automation can have particularly significant impact on the performance of service assets such as management, organization, people, process, knowledge, and information. Applications by themselves are a means of automation, but their performance can also be improved where they need to be shared between people and process assets.

Advances in artificial intelligence, machine learning, and rich-media technologies have increased the capabilities of software-based service agents to handle a variety of tasks and interactions.

Automation is considered to improve the utility and warranty of services. It might offer advantages in many areas of opportunity, including the following:

- The capacity of automated resources can be more easily adjusted in response to variations in demand volumes.
- Automated resources can handle capacity with fewer restrictions on time of access; they can therefore be used to serve demand across time zones and during after hours.
- Automated systems present a good basis for measuring and improving service processes by holding constant the factor of human resources. Conversely, they can be used to measure the differential impact on service quality and costs due to varying levels of knowledge, skills, and experience of human resources.
- Many optimization problems such as scheduling, routing, and allocation of resources require computing power that is beyond the capacity of human agents.

Service Management can benefit from automation in the following areas: [31]

- Design and modeling
- Service catalogue updates
- Pattern recognition and analysis (Problem Management, Event Management)
- Classification, prioritization, and routing (Incident, Change, and Problem Management)
- Detection and monitoring (Event Management, Incident Management)
- Optimization

Lesson 2: Service Catalogue Management

The **Service Catalogue** is a subset of the Service Portfolio and contains the services currently available to customers, including the details of all operational services being provided *or those being prepared for operational running*. In addition, it has information on the type of customers who are likely to get the service and what they might use it for.

Here are the objectives:

- Create and manage an accurate Service Catalogue that provides a single source of information about all services, and ensure that it is available to anyone approved to access it.
- Ensure that the Service Catalogue reflects the current details, status, interfaces, and dependencies of all services that are being run, *or being prepared to run*, in the live environment.

Two Aspects of the Service Catalogue[32]

The Service Catalogue has two aspects:

- **The Business Service Catalogue**: Containing details of all the IT services delivered to the customer, together with relationships to the business units and the business process that rely on the IT service. This is the customer view of the Service Catalogue.
- **The Technical Service Catalogue**: Containing details of all the IT services delivered to the customer, together with relationships to the supporting services, shared services, components, and CIs necessary to support the provision of the service to the business. This should underpin the Business Service Catalogue and not form part of the customer view.

Some organizations only maintain either a Business Service Catalogue or a Technical Service Catalogue.

Role: The Service Catalogue Manager

The Service Catalogue Manager is the **process owner** of the Service Catalogue Management process.

As the process owner, this person is responsible for the following tasks (DEMI):

1. **D**ocumenting the Service Catalogue Management process.
2. **E**ducating process participants on how to use the Service Catalogue Management process correctly and ensuring that process participants are complying with the process.
3. **M**easuring the success of the process against key performance indicators (KPIs), critical success factors (CSFs), and other targets.
4. Continually **I**mproving the process. (This is done with input and assistance from the Continual Service Improvement Manager.)

In addition to those tasks, the Service Catalogue Manager is also responsible for the following:

- Producing and maintaining the Service Catalogue
- Ensuring that all the information within the Service Catalogue is accurate and up-to-date
- Ensuring all operational services and those being prepared for operational running are recorded within the Service Catalogue
- Ensuring all information in the Service Catalogue is accurate, up to date and consistent with the Service Portfolio
- Ensuring all information is adequately protected and backed up

Lesson 3: Service Level Management

If "Service Management aims to achieve common understanding between the customer and service provider through managing service level expectations and delivering and supporting desired results," then Service Level Management is at the heart of Service Management. Service Level Management (SLM) negotiates, agrees to, and documents IT service targets with the business during the Service Design phase of the lifecycle, and then produces reports on the service provider's ability to deliver the agreed level of service during Service Operation and as part of Continual Service Improvement (CSI).

Highlighted objectives of Service Level Management are as follows:[33]

- Define, document, agree, monitor, measure, report, and review the level of IT services provided
- Provide and improve the relationship and communication with the business and customers
- Ensure that specific and measurable targets are developed for all IT services
- Monitor and improve customer satisfaction
- Ensure that both IT and the customers have a clear and unambiguous expectation of the level of service to be delivered

The Scope of Service Level Management[34]

Service Level Management provides a point of regular contact and communication to the customers and business managers of an organization. It represents the IT service provider to the business and the business to the IT service provider. The Service Level Manager works with customers to ensure that expectations and service quality match while the service is being designed and also after the service goes live; this includes new and existing services.

In addition, the Service Level Management process establishes and maintains Service Level Agreements (SLAs) for all current, live services and reviews them at least annually.

Service Level Requirements[35]

When the business needs to request a new service or change an aspect of an existing service, a business representative contacts the Service Level Manager with a list of business requirements and objectives. Together, the Service Level Manager and the business representative work out a set of Service Level Requirements (SLRs). Think of Service Level Requirements as the first draft of what will eventually become a Service Level Agreement (SLA).

The business representative and the Service Level Manager begin negotiating the Service Level Targets within the SLA—targets such as service uptime, maintenance windows, details surrounding what exactly is to be provided, who is allowed to use the service, how the service will be supported, how much the business will pay for the service, and so on. This negotiation process might be iterative (meaning, it might go through many rounds of revisions before it's finished) and might also take a substantial amount of time.

Service Level Agreements[36]

It is a common misunderstanding that an SLA is only an expression of "how much time a team has to resolve a ticket." There is *much* more to an SLA.

A Service Level Agreement (SLA)[37] is 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 both the IT Service Provider and the Customer. A single SLA may cover multiple IT Services or multiple customers.

SLAs are binding contracts in which agreements between the IT organization and the customer are recorded regarding the services to be delivered. During the Service Operation phase, the SLA serves as the official parameters within which the service must be provided.

The SLA's contract language should reflect that IT has an obligation to the business to provide the service as agreed, but the business also has an obligation to IT to pay for the service and to use the service in the expected manner. Targets in the SLA might represent the minimum acceptable, worst case, expected, or target service levels; either way, it should be clearly stated and unambiguous.

Even though SLAs are binding contracts and must have signatures, they should be written in clear, concise, but easy-to-read language. Steer clear of overly technical language or legalese, and instead choose language that the customer can easily understand.

Finally, it is imperative that any Service Level Target in your SLA be measurable. Never put anything in your SLA that cannot be measured, or disputes and conflict will undoubtedly occur.

Three Types of Agreements

A **contract**[38] is a generic term that describes any binding agreement between two or more parties. **All contracts must be signed in order to be valid.** An unsigned contract is unenforceable and worthless.

Each of the following items are contracts:

- **Service Level Agreement (SLA):** An agreement between a service provider and a customer.[39]
- **Operational Level Agreement (OLA):** An agreement between an IT service provider and another part of the same organization[40].
- **Underpinning Contract (UC):** A contract made between Service Level Management and External Service Providers (suppliers) in support of agreed to SLAs.

These contracts should be reviewed (and revised, if necessary) at least annually by the Service Level Manager and whichever other parties are governed by the contract.

Refresh Your Memory: The Service Owner

Service owners play an important role in Service Level Management, as it is the **service owner** who is accountable for the success of the service as a whole—*not* the Service Level Manager.

As an example: Your organization might offer email as one of the services it provides to the business. For email to work, there are many processes that go on behind the scenes (for example, some kind of tape backup process, an archiving-the-logs process, Capacity Management, and so on). Each of these processes (whether ITIL-issued or not) has a **process owner** who ensures that the process is documented, everyone is educated on how to use the process, the process' results are measured, and the process is constantly improved. The **service owner**, however, makes sure the *end-to-end service as a whole* is working and delivering value to the business. The service owner will attend change management meetings if a change to their service is up for review or discussion. The service owner is typically an executive of some kind (for example, the VP of Messaging), and is not necessarily the person rebooting the Exchange server at 3 a.m. or doing other day-to-day technical tasks.

SLA Structures

Service Level Agreements aren't usually one-size-fits-all contracts. Instead, organizations might need to structure their SLAs in different ways, depending on the needs of the customers.

The different types of SLA structures are as follows:

- **Service Based:**[41] Service-based SLAs cover one or more services for all the users of that service. For example, an organization might have one SLA for the service of Internet Access, meaning that every user in an entire organization uses the Internet Access service the exact same way. If certain users have restricted Internet access, whereas others have unlimited Internet access, a Service-based SLA may not be the right fit, or you may need to create separate targets within one agreement.
- **Customer Based:** A Customer-based SLA is an agreement with an individual customer group, covering all the services they use. For example, agreements might be reached with an organization's Finance Department covering, say, the Finance System, the Accounting System, the Payroll System, the Billing System, the Procurement System and any other IT systems that they use. Customers often prefer such an agreement, as all of their requirements are covered in a single document. Only one signatory is normally required, which simplifies this issue.
- **Multi-level SLAs:**[42] Some organizations have chosen to adopt a multiple level SLA structure. For example, a three-layer structure as follows:
  - **Corporate Level:** Covering all the generic SLM issues appropriate to every customer throughout the organization. These issues are likely to be less volatile and so updates are less frequently required.
  - **Customer Level:** Covering all SLM issues relevant to the particular customer group, regardless of the service being used.

- **Service Level:** Covering all SLM issues relevant to the specific service, in relation to this specific customer group (one for each service covered by the SLA).

The Multi-Level SLA structure allows SLAs to be kept to a manageable size, avoids unnecessary duplication, and reduces the need for frequent updates. However, it does mean that extra effort is required to maintain the necessary relationships and links within the Service Catalogue and the CMS.

The Service Review and the SLAM Chart[43]

It is up to the Service Level Manager to initiate **service reviews** that measure how well services (and any contributing processes) are performing and documenting the results in a service report that is presented to the customer. Some customers might expect a service report every month; others might take a "no news is good news" approach. Some customers might require the report to be in a fancy presentation format, and others might be satisfied with a few lines in an email. Different services and customers might require different reporting schedules; for this reason, it is important to specify the report format, reporting frequency and cycle, and distribution list in the SLA.

It is good practice to create an "at-a-glance" chart to present service level achievements as compared to the agreed Service Level Targets as the front page of a service report. This is called a Service Level Agreement Monitoring chart, or **SLAM chart**. The supporting details and data should be provided on the subsequent pages of the service report.

SLAM charts are typically color-coded for easy viewing, following a standard "red, amber, green" convention.

Service Improvement Plan (SIP)[44]

If a Service Level Target is missed or some other performance deficiency is found during service measurement and reporting, the Service Level Manager initiates a **Service Improvement Plan (SIP)**, in partnership with the Service Owner and the Continual Service Improvement Manager. The SIP is drawn only when there is a need. If all Service Level Targets are being met, no SIPs are needed. If 14 Service Level Targets are consistently falling short, there might be a need for 14 SIPs.

It is important not to get SIPs confused with the CSI phase of the lifecycle. SIPs are drawn up only when there is a need, much like a bandage for a broken bone. The CSI phase of the lifecycle is always occurring, even when all targets are being met successfully, and things are working well.

Service Level Management Activities[45]

Service Level Management's main activities are as follows:

- Working with customers to define their Service Level Requirements.
- Negotiating, agreeing to, and formally documenting SLAs, Operation Level Agreements (OLAs), and Underpinning Contracts (UCs), and ensuring that these are reviewed at least annually.

- During service operation, monitoring the performance of the services.
- Creating service reports and reviewing them with the customer, at whatever interval is specified in the SLA.
- Maintaining positive relationships with the business.
- Translating business requirements into IT terms and translating IT challenges into business terms.
- Measuring customer satisfaction and addressing complaints if necessary.
- Championing service improvement initiatives with assistance from the service owner and the CSI Manager.

The Service Level Manager Role

The **Service Level Manager** is a critical role in the building of a professional image of IT. Therefore, it is important to consider the skills and background of the person(s) in this role.

Consider this in light of the business customers with whom they will meet. The Service Level Manager needs to be able to communicate comfortably and effectively with any level of customer.

The necessary skills that a Service Level Manager must possess are as follows:

- Negotiation skills
- Relationship building and relationship management
- Very organized and detail-oriented
- Excellent communicator who is able to translate between business terms and technical terms
- Trustworthy, because they might be perceived as a "double-agent" or a "spy in both camps" because they represent IT to the business and the business to IT

The Service Level Manager is the **process owner** of the Service Level Management process.

As the process owner, this person is responsible for the following tasks (DEMI):

1. **D**ocumenting the Service Level Management process.
2. **E**ducating process participants on how to use the Service Level Management process correctly, and ensuring that process participants are complying with the process.
3. **M**easuring the success of the process against KPIs, CSFs, and other targets.
4. Continually **I**mproving the process. (This is done with input and assistance from the Continual Service Improvement Manager.)

Lesson 4: Capacity Management[46]

Rewinding a bit, remember that Demand Management is a process found in the Service Strategy phase of the lifecycle. Demand Management's job is to understand, predict, and influence what the customer's demand is going to be for a given service and to hand off that information to Capacity Management, here in Service Design.

Capacity Management ensures that there is sufficient capacity to meet that demand, by creating a design that will support the business requirements as captured by Demand Management.

Remember

Demand Management and Capacity Management go hand-in-hand.

Capacity Management ensures that there is cost-justifiable capacity in all areas of IT: applications, network bandwidth, server disk space, CPU utilization, teams, and so on. Capacity Management spans across the service lifecycle.

Capacity Management Overview

Figure 3-1 shows an overview of Capacity Management, its three subprocesses, as well as key outputs and tools.

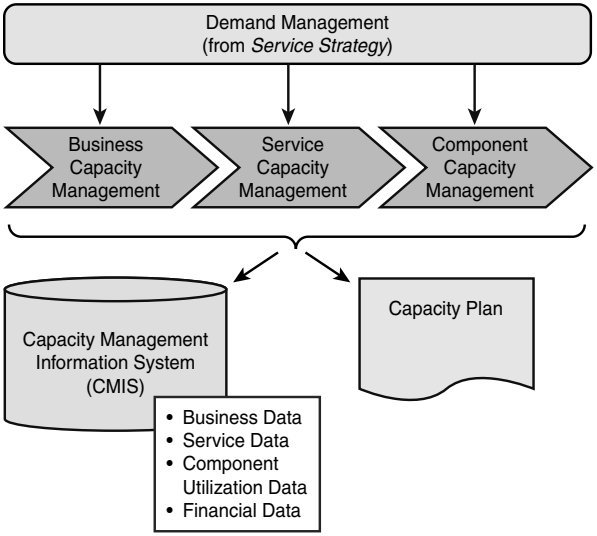

Figure 3-1 Capacity Management Subprocesses, Output, and Tools

The Three Subprocesses of Capacity Management[47]

There are many similar activities that are performed by each of the Capacity Management subprocesses, but each subprocess has a very different focus:

- **Business Capacity Management:** Ensures that the future *business requirements* (customer outcomes) for IT services are considered and understood and that sufficient IT capacity to

support any new or changed services is planned and implemented within an appropriate timescale.

- **Service Capacity Management:** Identifies and understands the IT services, their use of resources, working patterns, and peaks and valleys; ensures that the *services* meet their SLA targets.
- **Component Capacity Management:** Identifies and understands the performance, capacity, and utilization of each of the *individual components* within the technology used to support the IT services.

Remember that Demand Management (from Service Strategy) works closely with Capacity Management to influence user and customer demand for IT services and manage the impact on IT components.

The Capacity Plan[48]

One of the outputs of the Capacity Management process is the production of an annual Capacity Plan that outlines the IT resources and funding needed to support the business plan, together with a cost justification of that expenditure. The Capacity Plan is typically published annually, though it might need to be revised more often, especially if there are many changes being proposed or implemented.

The Capacity Management Information System (CMIS)[49]

The Capacity Management Information System (CMIS) holds the information needed by all subprocesses within Capacity Management. For example, the data monitored and collected as part of Component and Service Capacity Management is used in Business Capacity Management to determine what infrastructure components or upgrades to components are needed, and when.

The CMIS will not typically be a single database and likely will exist across several physical locations.

The CMIS stores four different types of data:[50]

- **Business data:** Information on the current and future needs of the business; this comes from the Business Capacity Management subprocess.
- **Service data:** Service performance data (e.g., transaction rates); this comes from the Service Capacity Management subprocess.
- **Component utilization data:** Resource data consisting of utilization, threshold, and limit information on all of the technological components supporting the services; this comes from the Component Capacity Management subprocess.
- **Financial data:** Financial information associated with various scenarios in the Capacity Plan; this is important because Capacity Management's job is to provide cost-justifiable IT capacity. You need to understand the cost of things, which is why the CMIS needs to able to access and store financial information.

The CMIS is part of the Configuration Management System (CMS).[51]

Capacity Management Roles

The Capacity Manager is the **process owner** of the Capacity Management process.

As the process owner, this person is responsible for the following tasks (DEMI):

1. **D**ocumenting the Capacity Management process.
2. **E**ducating process participants on how to use the Capacity Management process correctly, and ensuring that process participants are complying with the process.
3. **M**easuring the success of the process against KPIs, CSFs, and other targets.
4. Continually **I**mproving the process. (This is done with input and assistance from the Continual Service Improvement Manager.)

In addition, other roles participate in Capacity Management, including the following:

- **Service Level Manager:** Negotiates capacity requirements with existing customers.
- **Various Business Managers:** Provides demand patterns for existing, new, and potential future customers and services.
- **Technical and Application Management:**
  - Day-to-day capacity management activities.
  - React to capacity-related incidents and problems.

Lesson 5: Availability Management

Availability Management spans across the service lifecycle.

Availability Management's main objective is to ensure that service availability achievements meet (or even exceed) all of their agreed availability-related Service Level Targets. These Service Level Targets are documented in the SLA.

Availability Management should look to continually optimize and proactively improve the availability of the IT infrastructure, the services, and the supporting organization, in order to provide cost-effective availability improvements that can deliver business and customer benefits.[52]

Availability Management Activities

Because Availability Management spans the service lifecycle, it has both proactive and reactive activities. Proactive activities are performed in the "pre-game show" phases of the lifecycle: Service Strategy, Service Design, and Service Transition. Reactive activities happen in Service Operation, which is when the service goes live.

Tip

For the exam, you'll need to identify the difference between reactive and proactive activities of Availability Management. To answer these questions, just ask yourself: "Does this sound like something that happens before a service goes live (proactive) or after a service goes live (reactive)?"

The outputs of these activities are stored in the Availability Management Information System, or AMIS. The AMIS is part of the Configuration Management System (CMS).

Figure 3-2 illustrates both the proactive and reactive activities of the Availability Management process, as well as the types of data stored in the AMIS.

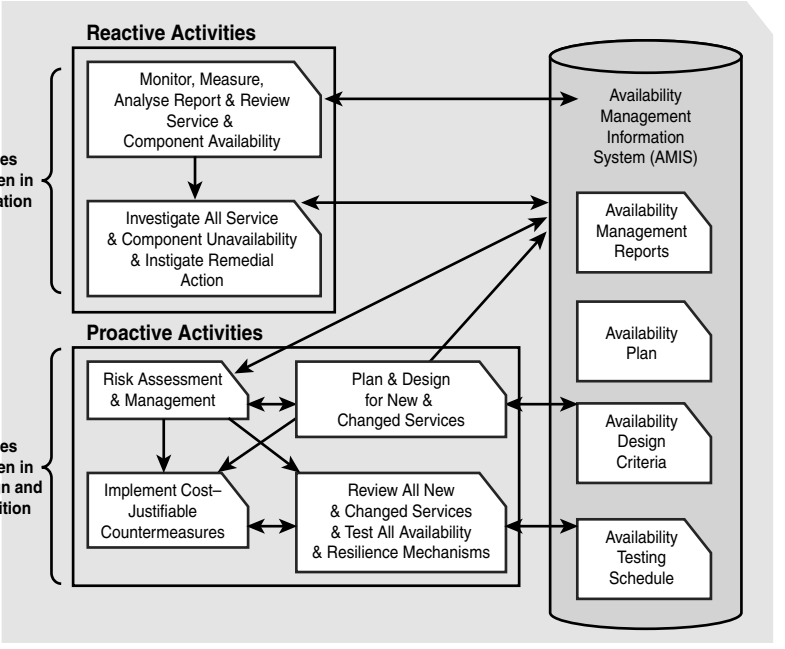

Figure 3-2 Availability Management Activities and the AMIS

What Does the Availability Management Process Measure?

After the service goes live in Service Operation, the Availability Management process switches gears and goes into reactive mode, where it measures the availability (uptime) of both **services** and **components**:

- **Service Availability:**[53]
  - Measures the **end-to-end service**. (How long has the *service of email* been available?)
  - How long has this service been up and running without interruption?

    - When it went down, how long was it down for?
    - What will we do to ensure that it doesn't go down again?
- **Component Availability:**[54]
    - Measures **individual components**. (How long has *this one server* been available?)
    - How long has this component been up and running without interruption?
    - When it went down, how long was it down for?
    - What will we do to ensure that it doesn't go down again?

Services are comprised of components, so to calculate Service Availability, the availability of all the constituent components will need to be tallied.

Availability Management Terms

There are several vocabulary words that are associated with the Availability Management process, and you'll need to know these for the exam:

- **Availability:**[55] The ability of a component or an IT Service to perform its agreed function when required. Also referred to as "uptime" or "Mean Time Between Failures (MTBF)." Availability numbers are often reported as a percentage. A service is considered **available** when the service is delivered to the Customer as stated in the SLA.
- **Reliability:**[56] A measure of how long a service or component can perform its agreed function without interruption. Also referred to as "Mean Time Between System Incidents (MTBSI)." This is a measure of how often a component breaks. (Is your car reliable? Not if it breaks down every other day.)
- **Maintainability:**[57] A measure of how quickly and effectively a service or component can be restored to normal working after a failure. Also referred to as "downtime" or, if services are being measured, "Mean Time to Restore Service (MTRS)."
- **Serviceability:**[58] The ability of a third-party supplier to meet the terms of their contract. It might seem strange to have this term mixed in with these more number-based terms, however, contracts will often include agreed levels of Availability, Reliability, and/or Maintainability for supporting a service or component.

Availability Management Roles

The Availability Manager is the **process owner** of the Availability Management process.

As the process owner, this person is responsible for the following tasks (DEMI):

1. **D**ocumenting the Availability Management process.
2. **E**ducating process participants on how to use the Availability Management process correctly and ensuring that process participants are complying with the process.

3. **M**easuring the success of the process against KPIs, CSFs, and other targets.
4. Continually **I**mproving the process. (This is done with input and assistance from the Continual Service Improvement Manager.)

Note

Availability Management is closely related to Information Security Management and Access Management. This will be discussed in more detail in the section, "Lesson 7: Information Security Management," later in this chapter.

Lesson 6: IT Service Continuity Management[59]

IT Service Continuity Management focuses on understanding and remediating events **the business** considers significant enough to be a disaster. What counts as a disaster for one organization might not count as a disaster for another, so be sure to plan for your unique circumstances. The business should have a clear idea of what constitutes a disaster and what services they will need quickly restored in the event of a catastrophic failure. As such, IT Service Continuity Management exists to underpin and support the business process called **Business Continuity Management**.

The objectives of IT Service Continuity Management are as follows:[60]

- Maintain a set of IT Service Continuity Plans and Recovery Plans.
- Complete regular Business Impact Analysis (BIA) exercises to ensure continuity plans are aligned with changing business impacts and requirements.
- Conduct regular Risk Analysis and Risk Management exercises.
- Negotiate contracts with suppliers for the provision of recovery capability.
- Assess the impact of all changes on the Service Continuity / Recovery plans.

IT Service Continuity Management doesn't happen in a vacuum; it gets its direction from the business. The business, through their process called Business Continuity Management, performs a **Business Impact Analysis** and identifies their potential risks; from there, an appropriate **Business Continuity Plan** is created. The business gives this plan to IT, and IT builds their IT Service Continuity Management strategy and plan to support and underpin the business' needs. These terms are defined as follows:

- **Business Continuity Management (BCM):**[61] The business process responsible for managing risks that could seriously affect the business. BCM safeguards the interests of key stakeholders, reputation, brand, and value-creating activities. The BCM process involves reducing risks to an acceptable level and planning for the recovery of business processes should a disruption to the business occur. BCM sets the objectives, scope, and requirements for IT Service Continuity Management.

- **Business Continuity Plan:**[62] 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.
- **Business Impact Analysis (BIA):**[63] BIA is the Activity in Business Continuity Management that identifies Vital Business Functions and their dependencies. These dependencies can include suppliers, people, other business processes, IT services, etc. BIA defines the recovery requirements for IT Services. These requirements include minimum Service Level Targets for each IT Service (e.g., "This service must be restored within 3 hours in the event of a disaster.").

IT Service Continuity Management Activities

IT Service Continuity Management has several activities as part of its process. You are not required to know these activities for the exam, but they are provided here to illustrate that IT Service Continuity Management cannot happen without the business giving direction to IT.

Figure 3-3 illustrates the activities of the IT Service Continuity Management process and how it gets its direction from the Business Continuity Management process.

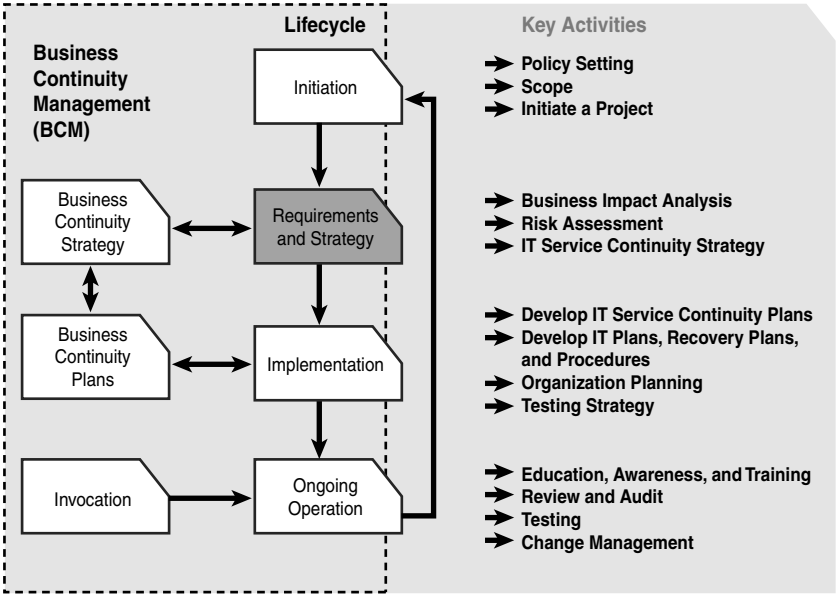

Figure 3-3 The IT Service Continuity Management Process Activities

Risk Management

Figure 3-4 illustrates a simple Risk Management model.

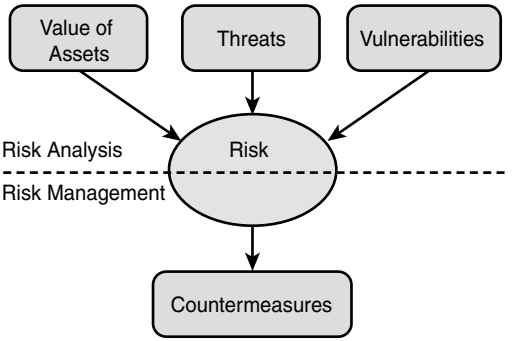

Figure 3-4 Risk Analysis and Management

People and organizations face risks every day. A judiciously applied Risk Management effort can identify and reduce those risks.

Broadly speaking, the generic term *risk management* is comprised of two main activities: Risk Analysis, which happens first, and Risk Management, which happens in reaction to the risk analysis.[64]

In the Risk Analysis stage, you first calculate the value of your assets, and then determine what vulnerabilities might be exploited by the threats to which you might be exposed.

A **threat** is anything that might exploit a vulnerability. Any potential cause of an incident can be considered to be a threat. For example, a fire is a threat that could exploit the vulnerability of flammable floor coverings.

A **vulnerability** is a weakness that could be exploited by a threat. For example an open firewall port, a password that is never changed, or a flammable carpet.

Risks can never be eliminated, of course, but they can be reduced.

Tip

A risk is simply something that *might* happen.[65]

Risk Management plays an important part in many ITIL processes, most notably Availability Management, IT Service Continuity Management (ITSCM), Information Security Management, and Supplier Management and the Service Transition phase of the lifecycle.[66]

IT Service Continuity Management Roles

The IT Service Continuity Manager is the **process owner** of the IT Service Continuity Management process.

As the process owner, this person is responsible for the following tasks (DEMI):

1. **D**ocumenting the IT Service Continuity Management process.
2. **E**ducating process participants on how to use the IT Service Continuity Management process correctly and ensuring that process participants are complying with the process.
3. **M**easuring the success of the process against KPIs, CSFs, and other targets.
4. Continually **I**mproving the process. (This is done with input and assistance from the Continual Service Improvement Manager.)

The IT Service Continuity Manager is part of the overall Business Continuity team.

In addition, the IT Service Continuity Manager does the following:

- Performs BIAs for all existing and new services
- Responsible for producing, testing and maintaining continuity plans
- Performs risk assessment and risk management
- Invokes the Continuity plan and manages it while it is in operation
- Communicates and maintains awareness
- Helps negotiate and manage contracts with 3rd party recovery service providers
- Assesses changes for impacts on continuity plans
- Part of overall Business Continuity team

Lesson 7: Information Security Management[67]

The primary objective of Information Security Management is to protect organizations, their data, and communications from harm that are caused by failures of *confidentiality*, *integrity*, and *availability* (CIA).

It is important to note that the *business* defines the level of protection that Information Security will provide because the business is the one paying for it. Information Security Management simply *provides* that level of protection.

Key Definitions

Three vocabulary words are associated with Information Security Management: **confidentiality**, **integrity**, and **availability**:

- **Confidentiality:** Information is disclosed or visible only to individuals who have a right to access it.

- **Integrity:** Information is complete, accurate, and will not get corrupted during transfer. It is also protected against unauthorized modification (such as hackers).
- **Availability:** Information is accessible, available, and usable when needed, and the systems on which this information resides can resist attacks and remain stable. (You might notice that this aligns with the definition of "availability," as learned in Availability Management.)

Tip

For the exam, you'll need to remember that Information Security Management is closely related to Availability Management and Access Management. See the section, "Information Security Management Interfaces with Other ITIL Processes," for details, as well as a list of other processes that interface with Information Security Management.

Framework for Managing IT Security[68]

The framework for managing IT security consists of an Information Security Policy and an Information Security Management System (ISMS).

The Information Security Policy[69]

Information Security Management activities should be focused on and driven by an overall Information Security Policy and a set of underpinning specific security policies. The policy should cover all areas of security, be appropriate, meet the needs of the business, and should include the following:

- An overall Information Security Policy
- Use and misuse of IT assets policy
- **An access control policy***
- A password control policy
- An e-mail policy
- An Internet policy
- An anti-virus policy
- An information classification policy
- A document classification policy
- A remote access policy
- A policy with regard to supplier access of IT service, information and components
- An asset disposal policy

These policies should be widely available to all customers and users, and their compliance should be referred to in all SLRs, SLAs, contracts, and agreements.

Note

The Access Control Policy lists which users (or groups of users) are permitted to access certain services, devices, folders, resources, and so on. Information Security sets this policy here in *Service Design*; however, this Access Control Policy is executed via the Access Management process in *Service Operation.*

The Information Security Management System (ISMS)[70]

The ISMS, as illustrated in Figure 3-5, is a tool that contains the standards, management procedures and guidelines supporting the information security policies.

For the exam, you'll be expected to know what ISMS stands for, and that all SLAs, OLAs, and UCs must have security-related information documented in them.

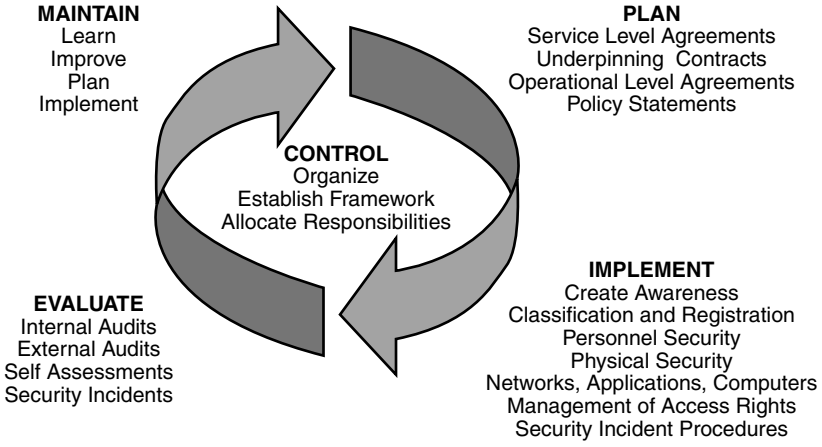

Figure 3-5 Framework for Managing IT Security

Note

First-print editions of the *Service Design* book call the ISMS by the term "SMIS" (Security Management Information System) in a few places. This is a typo in the *Service Design* book itself. The exam, however, calls this tool only by the name "ISMS," which is also the name we use in our book/DVD set.

Information Security Management Interfaces with Other ITIL Processes

Rarely a week goes by where we don't hear about a data security breach in the news. Laptops are stolen, Social Security Numbers are compromised, and our privacy settings for social networking sites are ignored. A vigilant approach to Information Security Management is more important than ever.

This critical process touches every area of IT, and virtually all ITIL processes have some kind of security consideration.

For the exam, you'll need to remember that Information Security Management is most closely related to Availability Management and Access Management:

- Security is often seen as an element of **Availability Management**, with *Confidentiality, Integrity, and Availability (CIA)* being the essence of both Availability Management and Information Security Management.
- **Access Management:** This process from *Service Operation* is responsible for granting or denying users the access to certain systems, tools, or services. Access Management executes the policies defined by Information Security Management.

In addition, these other processes also have security considerations:

- **ITSCM:** This *Service Design* process assesses risk, as well as how resilience, fail-over, and recovery mechanisms will be provided in the event of a catastrophic failure. Security is a major issue when continuity plans are tested or invoked.
- **Service Level Management:** This process gathers security requirements from the business and documents these within SLRs and SLAs during the Service Design phase. During Service Operation, SLM will also provide reports back to the Customer regarding the investigation and resolution of service and component security breaches.
- **Incident and Problem Management:** These Service Operation processes provide assistance with the resolution and subsequent justification and correction of security incidents and problems. The Incident Management process must provide the capability to identify and deal with security-related incidents. Service Desk and Service Operation staff must be trained to recognize a security incident as well.
- **Change Management:** ISM should assist with the assessment of every change for impact on information security. Also ISM can provide information on unauthorized changes that may have been performed.
- **Service Asset and Configuration Management** will provide the ability to provide accurate asset information to assist with security classifications. Having an accurate CMS is therefore an extremely useful ISM input.
- **Capacity Management** must consider security implications when selecting and introducing new technology. Security is an important consideration when procuring any new technology or software.
- **Financial Management** should provide adequate funds to finance security requirements.
- **Supplier Management** should assist with the joint management of suppliers and their access to services and systems, and the terms and conditions to be included within contracts concerning supplier responsibilities.

Information Security Management Roles

The Information Security Manager is the **process owner** of the Information Security Management process.

As the process owner, this person is responsible for the following tasks (DEMI):

1. **D**ocumenting the Information Security Management process.
2. **E**ducating process participants on how to use the Information Security Management process correctly and ensuring that process participants are complying with the process.
3. **M**easuring the success of the process against KPIs, CSFs, and other targets.
4. Continually **I**mproving the process. (This is done with input and assistance from the Continual Service Improvement Manager.)

In addition, the Information Security Manager performs the following duties:

- Develops and maintains the Information Security Policy.
- Communicates security awareness and policy.
- Performs security risk analysis and risk management exercises.
- Monitors and manages security breaches and incidents.
- Assesses changes for any impact on security.
- Ensures that CIA is maintained as agreed in SLAs.

Lesson 8: Supplier Management[71]

Supplier Management spans across the service lifecycle.

The purpose of the Supplier Management process is to obtain value for money from suppliers and to ensure that suppliers perform to the targets contained within their contracts and agreements. In addition, the Supplier Management process provides assistance to Service Level Management in periodically reviewing underpinning contracts and managing them for value.[72]

The Supplier and Contracts Database (SCD)

Supplier Management also maintains a Supplier and Contracts Database (SCD),[73] which stores supplier-related reports, contract details and information, along with the details of the services or products provided by each supplier.

The Supplier and Contracts Database (SCD) is part of the CMS.

Supplier Management Roles

The Supplier Manager is the **process owner** of the Supplier Management process.

As the process owner, this person is responsible for the following tasks (DEMI):

1. **D**ocumenting the Supplier Management process.
2. **E**ducating process participants on how to use the Supplier Management process correctly and ensuring that process participants are complying with the process.
3. **M**easuring the success of the process against KPIs, CSFs, and other targets.
4. Continually **I**mproving the process. (This is done with input and assistance from the Continual Service Improvement Manager.)

In addition, the Supplier Manager performs the following duties:

- Ensures that value for money is received from suppliers.
- Assists in development and review of SLAs, contracts, and agreements.
- Reviews and manages underpinning contracts.
- Maintains a Supplier and Contract database (SCD).
- Maintains processes for dealing with contractual disputes and for expected end, early end, or transfer of a service.
- Assesses changes for impact on suppliers, supporting services, and contracts.

Lesson 9: Sample Questions Based on Chapter 3

Answers can be found at the end of this chapter.

1. For which of the following is the Service Catalogue Manager responsible?
    1. Ensuring that information within the Service Pipeline is accurate and up to date.
    2. Ensuring that information in the Service Catalogue is consistent with information in the Service Pipeline.
    3. Ensuring that all operational services are recorded in the Service Catalogue.
    4. Ensuring that the information in the Service Catalogue is accurate and backed up.
        a. 1 and 2 only
        b. All of the above
        c. 2, 3, and 4 only
        d. 3 and 4 only

2. Which of the following list is a valid type of SLA?
    a. Priority-based SLA
    b. Technology-based SLA
    c. Location-based SLA
    d. Customer-based SLA
3. What types of data are stored in the CMIS?
    1. Change Management process metrics
    2. Component utilization data
    3. Business data
    4. Financial data and reports
        a. All of the above
        b. 1 only
        c. 2, 3, and 4 only
        d. 2 and 3
4. Capacity Management goes hand in hand with what process?
    a. Strategy Generation
    b. Service Level Management
    c. Financial Management
    d. Demand Management
5. Which of the following Availability Management activities are considered to be reactive, as opposed to proactive?
    1. Performing risk assessment and management exercises
    2. Monitoring service availability
    3. Monitoring component availability
    4. Testing of resilience mechanisms
        a. 1 and 2 are proactive; 3 and 4 are reactive.
        b. 1 and 4 are proactive; 2 and 3 are reactive.
        c. 1 and 4 are reactive; 2 and 3 are proactive.
        d. 1, 2, and 3 are reactive; 4 is proactive.

6. What does availability measure?
    a. The ability of a Configuration Item (a service component) to perform its agreed function when required.
    b. The amount of time a service or component experienced a reduced capacity.
    c. The amount of time a service or component can perform its agreed function without failing or interruption.
    d. A measure of how quickly and effectively a service or component can be restored to normal working after a failure.
7. A risk is something that
    a. Will definitely happen
    b. Has already happened
    c. Will not happen
    d. Might happen
8. Which processes(es) must adhere to security policies?
    a. Financial Management
    b. Availability Management
    c. Supplier Management
    d. All of the above
9. Which process must consider Business Continuity Plans as a major part of its own planning?
    a. Disaster Recovery
    b. IT Service Continuity Management
    c. Capacity Management
    d. Supplier Management
10. Who compiles the Service Design Package and ensures that it is complete?
    a. The Service Transition Manager
    b. The Availability Manager
    c. The Service Design Manager
    d. The Capacity Manager

11. Which of the five major aspects of Service Design is missing from the list below?
    - The design of services
    - The design of service management systems and tools
    - The design of technology architecture and management systems
    - ?
    - The design of measurement systems, methods, and metrics

    a. The design of functions

    b. The design of Service Level Agreements (SLAs)

    c. The design of applications

    d. The design of processes

12. How often should Service Level Management present reports back to the customer?

    a. At least annually

    b. Weekly

    c. Monthly

    d. According to the schedule specified in the SLA

13. Information Security Management is closely related to what other process(es)?

    a. Availability Management only

    b. Access Management only

    c. Availability Management and Access Management

    d. Incident Management and Service Portfolio Management

14. The Four Ps of Service Design are People, Processes, Products, and Partners. What is meant by “Products?”

    a. Tools, technology, and services

    b. Off-the-shelf software

    c. Servers only

    d. Necessary documentation to support our technology

Answers to Sample Questions Based on Chapter 3

1. **C is correct.**

    a. Incorrect. Only the Service Portfolio Manager ensures that information within the Service Pipeline is accurate and up to date. The Service Catalogue Manager is responsible only for the Service Catalogue. Option 2 falls within the SCM scope.

    b. Incorrect. Only the Service Portfolio Manager ensures that information within the Service Pipeline is accurate and up to date. The Service Catalogue Manager is responsible only for the Service Catalogue. The remaining three options fall within the SCM scope.

    c. **Correct. This answer eliminates option 1 as a possibility because only the Service Portfolio Manager can make changes to the Service Portfolio as a whole. The Service Catalogue Manager has control only over the Service Catalogue. Option 2 states that the Service Catalogue Manager ensures that the information in the Service Catalogue is consistent with the information in the Service Pipeline, which is true. Option 3 states that the Service Catalogue Manager ensures that all operation services are recorded in the Service Catalogue; this is also a true statement. Option 4 states that the Service Catalogue Manager ensures that the information in the Service Catalogue is accurate and backed up, which is also part of the Service Catalogue Manager's duties.**

    d. Incorrect. This answer erroneously avoids option 2, which is part of the Service Catalogue Manager's job duties, along with options 3 and 4. This answer is incomplete.

2. **D is correct.**

    a. Incorrect. Priority-based SLA is not a valid type of SLA.

    b. Incorrect. Technology-based SLA is not a valid type of SLA.

    c. Incorrect. Location-based SLA is not a valid type of SLA.

    d. Correct. Customer-based SLA is the only type of valid SLA on this list.

3. **C is correct.**

    a. Incorrect. Change Management process metrics data are compiled by the Change Management process owner and are stored in the CMS. The remaining three answers are correct.

    b. Incorrect. Change Management process metrics data are compiled by the Change Management process owner and are stored in the CMS.

    c. **Correct. The CMIS stores business data, component utilization data, and financial data. In addition, the CMIS also stores service data.**

d. Incorrect. Financial data is also stored in the CMIS, as the objective of Capacity Management is to provide *cost-justifiable* IT Capacity. Information about those costs must be tracked.

4. **D is correct.**

   a. Incorrect. Strategy Generation is a process found in the Service Strategy book and is unrelated to Capacity Management. (Strategy Generation is also not part of the ITIL Foundation syllabus or exam.)

   b. Incorrect. Although Capacity Management might provide input and get feedback from Service Level Management, they are not closely related.

   c. Incorrect. Although Capacity Management might use data supplied by Financial Management, they are not as closely related as Capacity Management and Demand Management. Demand Management provides a direct input into Capacity Management; you cannot have one process without the other.

   d. **Correct. Demand Management provides the patterns of business activity, user profiles, and capacity requirements directly to the Capacity Management process. Capacity Management designs and supplies the capacity to meet the demand. Capacity Management cannot provide one of its main outputs without the input Demand Management provides.**

5. **B is correct.**

   a. 1 and 2 are proactive; 3 and 4 are reactive.

   b. **1 and 4 are proactive; 2 and 3 are reactive.**

   c. 1 and 4 are reactive; 2 and 3 are proactive.

   d. 1, 2, and 3 are reactive; 4 is proactive.

6. **A is correct.**

   a. **Correct. The ITIL definition of availability is the ability of a Configuration Item or IT Service to perform its agreed function when required.**

   b. Incorrect. This would be a helpful thing to measure, however.

   c. Incorrect. This measures reliability.

   d. Incorrect. This measures maintainability.

7. **D is correct.**

   a. Incorrect. Although risks can't be completely eliminated, they also aren't guaranteed to occur either.

   b. Incorrect. Although this may be true of some risks, it is not true for all risks.

   c. Incorrect. It is impossible to completely eliminate risk even with the best planning.

   d. **Correct. This is one of the characteristics of a risk.**

8. **D is correct.**

    a. Incorrect. Financial Management must adhere to Information Security Policies, but the other options must also. This answer is incomplete.

    b. Incorrect. Availability Management must adhere to Information Security Policies, but the other options must also. This answer is incomplete.

    c. Incorrect. Supplier Management must adhere to Information Security Policies, but the other options must also. This answer is incomplete.

    d. **Correct. All processes, whether they are ITIL processes or processes that are unique to your organization, must adhere to security policies.**

9. **B is correct.**

    a. Incorrect. Disaster Recovery is not the proper, official term for this process.

    b. **Correct. IT Service Continuity Management underpins Business Continuity Management, which creates Business Continuity Plans.**

    c. Incorrect. Capacity Management should consider ITSCM plans as part of its capacity planning, but this is not a major component of this process.

    d. Incorrect. Supplier Management might provide input and assistance into contingency plans and contracts with external suppliers in the event of a disaster, but it is not a major component of the process.

10. **C is correct.**

    a. Incorrect. It is the Service Design Manager who compiles the Service Design package and ensures that it is complete, not the Service Transition Manager. (*Note:* There is a role identified within the Service Transition book called the Service Transition Manager; however, that role is not part of the ITIL Foundation exam syllabus. You will never be asked a question about that role on the exam. If you see "Service Transition Manager" as a possible answer on the ITIL Foundation exam, you can safely assume it is the wrong answer.)

    b. Incorrect. The Availability Manager may contribute design data to the SDP as it relates to the availability of components and services, but they do not do the official SDP compilation.

    c. **Correct. The Service Design Manager compiles the SDP and ensures that it is complete.**

    d. Incorrect. The Capacity Manager might contribute design data to the SDP as it relates to the capacity of components and services, but they do not do the official SDP compilation.

11. **D is correct.**

    a. Incorrect. The five aspects of Service Design spell STAMP. The list is missing the letter "p," which stands for the design of processes. This answer, however, is discussing the design of functions, which is not part of the five aspects of Service Design.

    b. Incorrect. The five aspects of Service Design spell STAMP. The list is missing the letter "p," which stands for the design of processes. This answer, however, is discussing the design of SLAs, which is not part of the five aspects of Service Design.

    c. Incorrect. The five aspects of Service Design spell STAMP. The list is missing the letter "p," which stands for the design of processes. This answer, however, is discussing the design of applications, which is not specifically mentioned as part of the five aspects of Service Design.

    d. **Correct. The design of processes is missing from the list.**

12. **D is correct.**

    a. Incorrect. There are several other documents that must be reviewed "at least annually," which include SLAs, OLAs, UCs, the Availability Plan, and the Capacity Plan. However, SLM's reporting schedule is dictated by what is documented and agreed to in each SLA.

    b. Incorrect. The reporting schedule will be documented in the SLA and may vary from customer to customer or agreement to agreement.

    c. Incorrect. The reporting schedule will be documented in the SLA and may vary from customer to customer or agreement to agreement.

    d. **Correct. In each service's SLA, the reporting schedule should be clearly stated and subsequently followed.**

13. **C is correct.**

    a. Incorrect. Availability Management is closely related to Information Security Management, but Access Management is as well.

    b. Incorrect. Access Management is closely related to Information Security Management, but Availability Management is as well.

    c. **Correct. Information Security Management is responsible for ensuring data confidentiality, integrity, and availability. The word "Availability" here corresponds with Availability Management. Information Security Management is also responsible for creating an Information Security Policy, which contains an Access Control Policy. Access Management executes this exclusively in the Service Operation phase of the lifecycle.**

    d. Incorrect. Although all processes must follow Information Security policies, Availability Management and Access Management are the most closely related. Security is often seen as an element of Availability Management, with *confidentiality*, *integrity*, *and availability (CIA)* being the essence of both Availability Management

and Information Security Management. Access Management executes the policies defined by Information Security Management.

14. **A is correct.**

    a. **Correct. The term "Products" refers to the tools, technology, and services that must be considered during the Service Design phase, along with the remaining three Ps.**

    b. Incorrect. Although "Products" can certainly include off-the-shelf software, this is not a complete definition.

    c. Incorrect. Although "Products" can certainly include servers, this is not a complete definition.

    d. Incorrect. Documentation is important, but it is not what is being described here.

Endnotes/Syllabus Requirements

27. This section satisfies Syllabus Requirement ITILFND02-02-4.
28. This section satisfies Syllabus Requirement ITILFND02-02-5.
29. This section satisfies Syllabus Requirement ITILFND03-03-14.
30. This section satisfies Syllabus Requirement ITILFND04-04-3.
31. This section satisfies Syllabus Requirement ITILFND08-08-2.
32. This section satisfies Syllabus Requirement ITILFND03-03-4.
33. This section satisfies Syllabus Requirement ITILFND05-05-31.
34. This section satisfies Syllabus Requirement ITILFND05-05-31.
35. This section satisfies Syllabus Requirement ITILFND05-05-31.
36. This section satisfies Syllabus Requirement ITILFND03-03-11.
37. This section satisfies Syllabus Requirement ITILFND03-03-11.
38. This section satisfies Syllabus Requirement ITILFND03-03-13.
39. This section satisfies Syllabus Requirement ITILFND03-03-11.
40. This section satisfies Syllabus Requirement ITILFND03-03-12.
41. This section satisfies Syllabus Requirement ITILFND05-05-31.
42. This section satisfies Syllabus Requirement ITILFND05-05-31.
43. This section satisfies Syllabus Requirement ITILFND05-05-31.
44. This section satisfies Syllabus Requirement ITILFND05-05-31.

45. This section satisfies Syllabus Requirement ITILFND05-05-31.

46. This section satisfies Syllabus Requirement ITILFND05-05-45.

47. This section satisfies Syllabus Requirement ITILFND05-05-45.

48. This section satisfies Syllabus Requirement ITILFND05-05-45.

49. This section satisfies Syllabus Requirement ITILFND05-05-45.

50. This section satisfies Syllabus Requirement ITILFND05-05-45.

51. This section satisfies Syllabus Requirement ITILFND05-05-45.

52. This section satisfies Syllabus Requirement ITILFND05-05-42.

53. This section satisfies Syllabus Requirement ITILFND05-05-42.

54. This section satisfies Syllabus Requirement ITILFND05-05-42.

55. This section satisfies Syllabus Requirements ITILFND05-05-42 and ITILFND03-03-15.

56. This section satisfies Syllabus Requirement ITILFND05-05-42.

57. This section satisfies Syllabus Requirement ITILFND05-05-42.

58. This section satisfies Syllabus Requirement ITILFND05-05-42.

59. This section satisfies Syllabus Requirement ITILFND05-05-46.

60. This section satisfies Syllabus Requirement ITILFND05-05-42.

61. This section satisfies Syllabus Requirement ITILFND05-05-42.

62. This section satisfies Syllabus Requirement ITILFND05-05-42.

63. This section satisfies Syllabus Requirement ITILFND05-05-42.

64. This section satisfies Syllabus Requirement ITILFND05-05-46.

65. This section satisfies Syllabus Requirement ITILFND03-03-7.

66. This section satisfies Syllabus Requirement ITILFND03-03-7.

67. This section satisfies Syllabus Requirement ITILFND05-05-43.

68. This section satisfies Syllabus Requirement ITILFND05-05-43.

69. This section satisfies Syllabus Requirement ITILFND05-05-43.

70. This section satisfies Syllabus Requirement ITILFND05-05-43.

71. This section satisfies Syllabus Requirement ITILFND05-05-44.

72. This section satisfies Syllabus Requirement ITILFND05-05-44.

73. This section satisfies Syllabus Requirement ITILFND05-05-44.

Chapter 4

Service Transition

Lesson 1: Service Transition Overview

The Service Transition phase of the lifecycle is where things start to get exciting for IT because this is the phase where IT buys, builds, tests, and ultimately installs and deploys services. This is where the action happens; up until this point, IT hasn't been able to tinker with gadgets like servers, routers, switches, circuits, applications, and the like. Service Transition is where IT gets its hands dirty.

Tip

Need a handy way to remember that Service Transition is the lifecycle phase where techies get to do their testing and tinkering? "Transition," "test," and "tinker" all start with the letter T.

The Goals and Scope of Service Transition

Business environments are in a constant state of transition, and as such, so are the services required from IT. To ensure these services are being implemented properly, an effective Service Transition practice is critical.

Service Transition is a very exciting phase in the service lifecycle, because in this phase you begin the building process. In the Service Strategy and Design phases, your work was limited to brainstorming and conceptualizing, but in Service Transition you can finally get your hands dirty.

Service Transition focuses on how to ensure that the requirements that were developed in Service Strategy and carefully set out in Service Design are successfully built, tested, and implemented in Service Transition for use by the business in Service Operation. It truly is a phase of *transition*.

The goals of Service Transition include the following:[74]

- Introducing new (or changed) services in the production environment, with a focus on customer expectations, as well as efficiency, cost, and safety.
- Moving services from the Design phase into the production environment, while ensuring that there is minimal impact on existing services.
- Ensuring that there are clear and comprehensive transition plans.

Service Transition's scope includes the following:

- Managing the complexity associated with changes to services.
- Introduction of new services and changes to existing services.
- The retiring of services no longer needed.
- The transfer of service to an external provider or bringing a previously outsourced service back in-house.

Service Transition's Value to the Business[75]

As the business reacts to changes the marketplace, their business processes will change as well. This is normal and healthy; it means the business is staying agile in a changing world. The fallout of these business changes will ultimately warrant adjustments to the services IT provides.

Service Transition provides value to the business by enabling the service provider to handle high volumes of change and releases across its customer base.

In addition, Service Transition adds value to the business by improving the following:

- The ability to adapt quickly to new requirements and market developments ('competitive edge')
- Transition management of mergers, de-mergers, acquisitions and the transfer of services
- The success rate of changes and releases
- The predictions of service levels and warranties for new and changed services
- Confidence in the degree of compliance with business and governance requirements during change
- The productivity of business and customer staff in the planning and use of new and changed services

Lesson 2: Service Asset and Configuration Management (SACM)

Service Asset and Configuration Management (SACM) spans across the service lifecycle.

The Service Asset and Configuration Management process manages service assets and configuration items in order to support the other Service Management processes. Its main objective is to define and control the components of services and infrastructure and maintain accurate configuration information on the historical, planned, and current state of the services and infrastructure.

The primary purpose of SACM[76] is to:

- Define and control Configuration Items (CIs)
- Provide accurate configuration records

- Identify, control, record, report, audit, and verify service assets and configuration items, including versions, baselines, constituent components, their attributes, and relationships
- Maintain an accurate and complete Configuration Management Database (CMDB) and Configuration Management System (CMS)

SACM Key Terms

Asset Management covers service assets across the whole service lifecycle. *Configuration Management* ensures that selected components of a complete service, system, or product are identified, baselined, and maintained and that changes to them are controlled.

Tip

A **Service Asset**[77] is anything that could contribute to the delivery of a service. They come in two flavors: Capabilities and Resources. (Refer to Lesson 1 in Chapter 2, "Service Strategy," for more information.)

A **Configuration Item (CI)**[78] is "Any item under the control of Configuration Management." This means, "If you feel like calling it a CI, it's a CI. But if you're going to commit to calling it a CI, you're also committing to managing it through the Configuration Management process and the Configuration Management Database (CMDB) and controlling it through the Change Management process. Choose wisely."

Some of the key terms related to Service Asset and Configuration Management are as follows:

- **The Configuration Management Database (CMDB)**: The CMDB is a set of one or more connected databases that provide a logical model of the IT infrastructure. It captures Configuration Items (CIs) and the relationships between them. This logical model is called a "configuration model." An organization might have one CMDB, or several CMDBs that work in concert as one federated CMDB. Either way, the CMDB(s) is/are part of the CMS.
- **The Configuration Model:** A **Configuration Model**[79] is a mock-up of a service or a group of related CIs. Change Management uses the Configuration Model to perform risk assessments and simulations when evaluating a change. The Service Design phase of the lifecycle uses it to plan and design new or changed services. Release and Deployment Management uses it to plan release and deployment packages. Incident and Problem Management also use the configuration model to assess the impact and cause of outages, plan desktop refreshes, and so on. A configuration model records the relationships between Assets, the Infrastructure, and Services.[80]
- **The Configuration Baseline:** A **Configuration Baseline**[81] is the first measurement of a particular CI or logical group of CIs. Baselines are used for later comparison and also as a possible rollback point. You gather a baseline (and all subsequent measurements) by taking a **snapshot**. Baselines are also stored as records in the CMDB.
- **Definitive Media Library (DML):**[82] Official, approved versions of all electronic media Configuration Items (software [both off-the-shelf and home-grown], official versions of documentation, software licenses, activation keys, and so on) are securely stored in and released from the Definitive Media Library (DML). The DML is a single logical storage area

even if there are multiple locations. All software in the DML is under the control of Change Management and is recorded in the Configuration Management System. Only software from the DML is acceptable for use in a Release.

To clarify: The DML is officially maintained by Service Asset and Configuration Management, and it is controlled by Change Management. It is used primarily by Release and Deployment Management, as this is the only location from where software releases are deployed. **It is part of the CMS.**

The section, "Lesson 4: Release and Deployment Management," later in the chapter covers the DML in more detail.

The Configuration Management System (CMS)[83]

The Configuration Management System (CMS) is defined as:

A set of tools and databases that are used to manage an IT Service Provider's Configuration data. The CMS also includes information about Incidents, Problems, Known Errors, Changes and Releases; and may contain data about employees, Suppliers, locations, Business Units, Customers and Users. The CMS is maintained by Configuration Management and is used by all IT Service Management Processes.

The CMS is a federation of many constituent databases and data sources, as illustrated in Figure 4-1. Components can include the DML, the Known Error Database (KEDB), the CMDB(s), the CMIS, the Availability Management Information System (AMIS), the Supplier and Contract Database (SCD), and so on. Even non-ITIL-related data sources can be included in the CMS, such as HR or personnel data, data about various branch locations of your business, and so on.[84]

The CMS stores relationships between data from different data sources, whether "officially ITIL-sanctioned" or not.

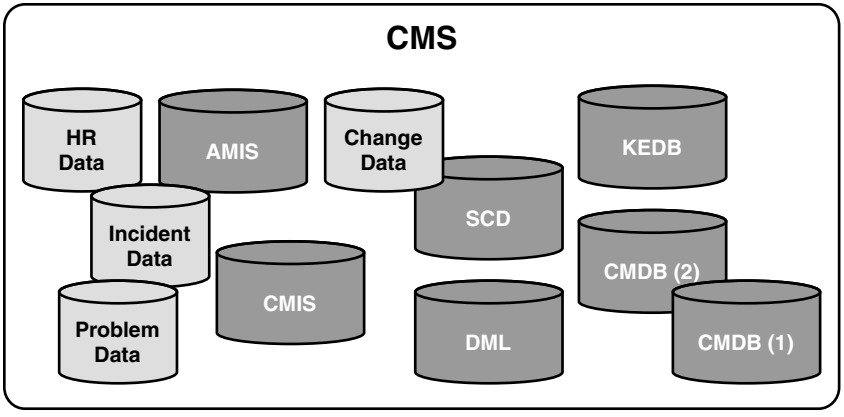

Figure 4-1 CMS Components

In Figure 4-1, the darker-shaded databases are databases specified in the ITIL books. The data sources in the lighter color (Incident data, Change data, Problem data, and even HR data) represent repositories of data that do not have specific "ITIL titles" in the ITIL publications; however, students should understand that this data needs to be tracked *somewhere*, and it needs to be accessible via the CMS in order for the CMS to do its job.

For purposes of the Foundation exam, this type of information (Incident data, Change data, Problem data, and HR data) is generically found "in the CMS."

Tip

When you see the word "relationships" on the exam, your mind should either go to the SACM process itself or to the tools described in the SACM process (the CMDB and the CMS). Of course, if the word "relationships" is being used in the context of building and maintaining good working relationships between the customer and IT, you should think of Service Level Management.

SACM Activities[85]

The main activities of Service Asset and Configuration Management are as follows:

- **Management and Planning:** Determining how your organization is going to "do" Service Asset and Configuration Management—creating policies, objectives, and so on.
- **Configuration Identification:** Determining the scope and detail of your CMDB by deciding what counts as a CI and which attributes will be stored about each CI. Does your organization want to track telephones as CIs? What about keyboards?

  Every organization will have its own approach to defining CIs. You might choose to label services as CIs first and then break them down into their constituent parts, or you might choose an alternate scheme that makes more sense for your organization.

  CIs and the relationships (parent/child or peer-to-peer) between them are stored as records in the Configuration Management Database (CMDB). These records contain information about each CI (called *attributes*) as well as the history of the CI (called *status*).

  Examples of CI *attributes* include the following:

  - Serial numbers
  - Physical location
  - Owner
  - Asset tag number
  - Manufacturer

  Examples of CI *status* include the following:

  - Ordered
  - In production

- Down for maintenance
- In storage
- Retired

- **Configuration Control:** Ensuring that only authorized and identifiable CIs are recorded and that no CI is added, removed, modified, or replaced without being authorized by Change Management.
- **Status Accounting and Reporting:** Being able to track and report on the current and historical data for each CI as it changes status throughout its individual lifecycle (for example, "on order," "being tested," "in production," or "retired").
- **Verification and Audit:** Auditing your CMDB(s) is vital to determining if your CMDB accurately reflects reality. Whether automated tools are used or if a manual audit is performed, this is the only way to ensure CMDB integrity.

SACM Roles

The Configuration Manager is the **process owner** of the Service Asset and Configuration Management process.

As the process owner, this person is responsible for the following tasks (DEMI):

1. **D**ocumenting the Configuration Management process.
2. **E**ducating process participants on how to use the Configuration Management process correctly and ensuring that process participants are complying with the process.
3. **M**easuring the success of the process against KPIs, CSFs, and other targets set.
4. Continually **I**mproving the process. (This is done with input and assistance from the Continual Service Improvement Manager.)

Other SACM-related roles might be necessary, too:

- Configuration administrator/librarian
- CMS/tools administrator

The **Change Manager** also plays a role in SACM. The Change Manager ensures that after a change has been implemented, a list of the changed CIs gets populated into the CMDB/CMS. The Change Manager will not input this information into the CMDB/CMS himself, but instead will ensure that the Configuration Administrator/Librarian has done it correctly and in a timely fashion.

Lesson 3: Change Management

Change Management spans across the service lifecycle.

Note

A convenient rule of thumb: No changes to any CI may be made without going through Change Management. Bear this in mind as you continue through the rest of the chapter; this rule will always hold true.

The most important thing to remember about Change Management is that this process is responsible for managing, coordinating, and facilitating changes. (Notice that this process does not include actually *implementing* the change.) Change Management is simply the mechanism for ensuring that changes are recorded and then evaluated, authorized, prioritized, planned, tested, implemented, documented, and reviewed in a controlled manner.[86]

It is up to Release and Deployment Management to actually execute and implement the change. Change Management ensures that Release and Deployment Management has done its job.

Change Management Vocabulary

The Change Management process is one of the more vocabulary-intensive processes in ITIL. Because the Change Management process spans across the service lifecycle, the following terms will be used throughout the five ITIL books:

- **Service Change:**[87] Often referred to as just a "change," this word simply means to alter a CI in some way, whether it's adding a CI, modifying a CI, or even removing a CI.
- **Request for Change:**[88] The form (electronic, paper, or otherwise) upon which the change is written. Submitting an RFC is how a change enters the Change Management process.
- **Post-Implementation Review (PIR):**[89] A meeting held after the change implementation to determine its success. A **PIR** should be carried out to confirm that the Change has met its objectives, that the initiator and stakeholders are happy with the results, and that there have been no unexpected side effects.

Note

Sometimes the PIR is simply referred to as a "change review" in the ITIL books. You can use these terms interchangeably.

- **Change Advisory Board (CAB):**[90] The CAB is a committee of technical and business personnel that convenes to assist in the assessment, prioritization, and scheduling of changes. This board is typically made up of representatives from all areas within the IT organization, representatives from the Business and third-party suppliers when necessary. The CAB might change from meeting to meeting, depending on the nature of the changes on the agenda. The Change Manager determines who needs to attend.

  The CAB needs to include members who have a clear understanding of Customers' and users' business requirements, along with knowledge of technical and support functions for the specific changes on the agenda. RFCs are typically circulated for review prior to the meeting to keep meetings efficient.

- **Emergency CAB (ECAB):**[91] When true emergencies occur, there might not be time to convene a formal and complete CAB. Instead, an **Emergency CAB (ECAB)** will be brought together to assist in the assessment and authorization of emergency changes.

Both the CAB and the ECAB are advisory bodies only; it is up to the proper change authority (which might change depending on the size, complexity, and scope of a change) to provide the final stamp of approval. Remember that the Emergency Change designation should be reserved for true emergencies.

Role: The Change Manager

The Change Manager is the **process owner** of the Change Management process.

As the process owner, this person is responsible for the following tasks (DEMI):

1. **D**ocumenting the Change Management process.
2. **E**ducating process participants on how to use the Change Management process correctly and ensuring that process participants are complying with the process.
3. **M**easuring the success of the process against KPIs, CSFs, and other targets he/she has set.
4. Continually **I**mproving the process. (This is done with input and assistance from the Continual Service Improvement Manager.)

In addition, the Change Manager does the following:

- Monitors process adherence.
- Runs CAB meetings and produces change schedule.
- Coordinates the change build, test, and implementation.
- Reviews changes upon completion.
- Determines, documents, and enforces what constitutes a normal, standard and emergency change.
- Authorizes changes, based on input and guidance from CAB/ECAB.
- Is accountable for the success of a change.

Where Do Changes Come From?[92]

Changes can come from many different sources. Some examples include the following:

- An RFC document (a network admin needs to change a router configuration).
- A call to the service desk (a user would like a flat-panel monitor instead of a CRT monitor).
- A project initiation document (the finance department is implementing a new payroll system).
- A change proposal (for very large changes, such as outsourcing the service desk).

Note

Changes to *business processes* do not fall under the scope of Change Management. Change Management is concerned with changes to IT services, IT processes, IT infrastructure, IT components, and so on. Changes to business processes are handled by the business; of course, the "fallout" from those changes will most likely trickle down to IT.

Three Types of Changes

Changes come in three types, and it is easy to get two of these terms confused. The words "normal" and "standard" have similar meanings in day-to-day conversation, but in ITIL, they are quite different. The third type of change, an *Emergency Change*, is straightforward.

- **Normal changes:**[93] Every organization's definition of "normal change" is going to be different. For purposes of the Foundation exam, it suffices to say that a normal change is one that goes through the typical Change Management process of requiring assessment by the CAB and to have the change's implementation managed and coordinated by a formal process.
- **Standard changes:**[94] Standard changes are *pre-authorized changes* to a service or infrastructure that has an accepted and established procedure. Examples might include reinstalling an application, getting a new PC set up for a new employee, or moving a PC for a single user.

  Standard changes must have the following:

  - A defined trigger to initiate the RFC
  - Tasks that are well known, documented, and proven
  - Authority that is effectively given in advance
  - Budgetary approval made in advance
  - Low and well-understood risk

  Some standard changes will be addressed via the Request Fulfillment process (part of Service Operation).
- **Emergency changes:**[95] When true emergencies arise, there must be a streamlined assessment and authorization process so that implementation can happen as quickly as possible. However, it is important to save this designation for true emergencies because emergency changes do not have time to be thoroughly tested. There is a significantly higher degree of risk when implementing an emergency change, and that risk must be weighed because the untested change implementation may cause more damage than what it is trying to solve. Emergency changes are assessed by the ECAB.

NOTE:

ITIL no longer uses the V2 phrase "urgent change." The proper V3 term is "emergency change."

Who Really Authorizes Changes?

Formal authorization is obtained for each change from a **change authority** that might be a *role, person, or a group of people*. The change authority may differ from change to change, as illustrated in Figure 4-2, depending on the size and scope of the change.

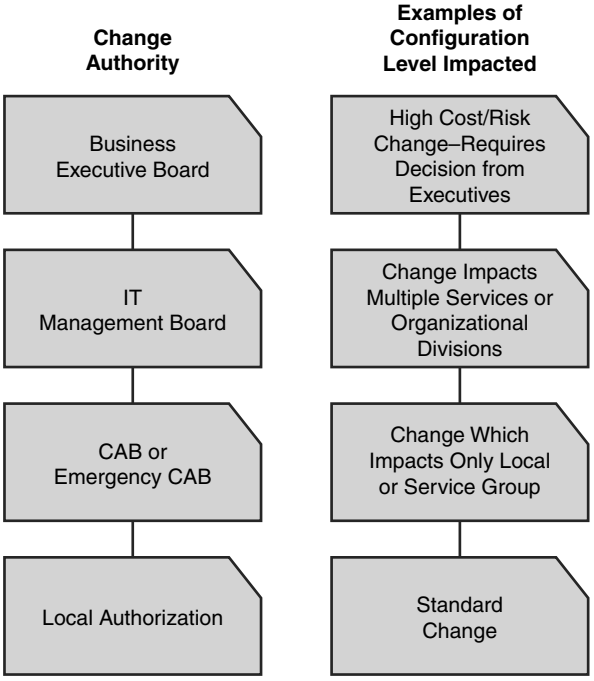

Figure 4-2 Change Authority

The levels of authorization for a particular type of change should be judged by the type, size, or risk of the change, e.g. changes in a large enterprise that affect several distributed sites may need to be authorized by a higher-level change authority such as a global CAB or the Board of Directors.

Remediation (the Backout Plan)[96]

Every change must have some type of action plan in the event the change needs to be backed out. In the event the change cannot be backed out once it has begun, a plan must be created for remediation in the event the change fails. Changes should not be authorized unless the remediation plan is deemed solid by the appropriate change authority.

The Seven Rs of Change Management[97]

When evaluating a proposed change, it is important to ask enough questions to ascertain whether the change should be attempted.

These Seven Rs are questions to be asked prior to a change's implementation to assist in evaluating the change. The Seven Rs are as follows:

- Who **raised** the change?
- What is the **reason** for the change?
- What is the **return** required from the change?
- What are the **risks** involved in the change?
- What **resources** are required to deliver the change?
- Who is **responsible** for the build, test, and implementation of the change?
- What is the **relationship** between this change and other changes?

Change Management Activities[98]

Figure 4-3 illustrates the high-level activities of the Change Management process:

Step 1: Create and record RFCs: RFCs can come from any person or team in the organization, whether from the business side or from IT.

Step 2: Review RFC: In this step, the change manager reviews the RFC to make sure the form is filled out correctly, has the required information, and so on. The change is also logged in the CMS. Changes that do not have the required information or that may have been accidentally misrouted are filtered out.

Step 3: Assess and evaluate the change: The change manager determines the appropriate level of change authority needed to authorize the change, and then decides who should be involved in CAB given the type of change. Next, usually with assistance from the CAB, the change is assessed and evaluated for its cost, benefits, and potential impact to both the business as well as other IT systems.

Step 4: Authorize the change: The change is authorized by the appropriate change authority, and the initiator of the Request for Change is notified.

Step 5: Coordinate Change implementation: This is where the Change Management process manages/coordinates/oversees what is built, tested, and implemented by Release and Deployment Management.

Step 6: Review and Close the Change: After the change has been implemented by the Release and Deployment Management process, the Change Manager reviews the change and its change documentation, and then closes the change record in the CMS when all actions are completed.

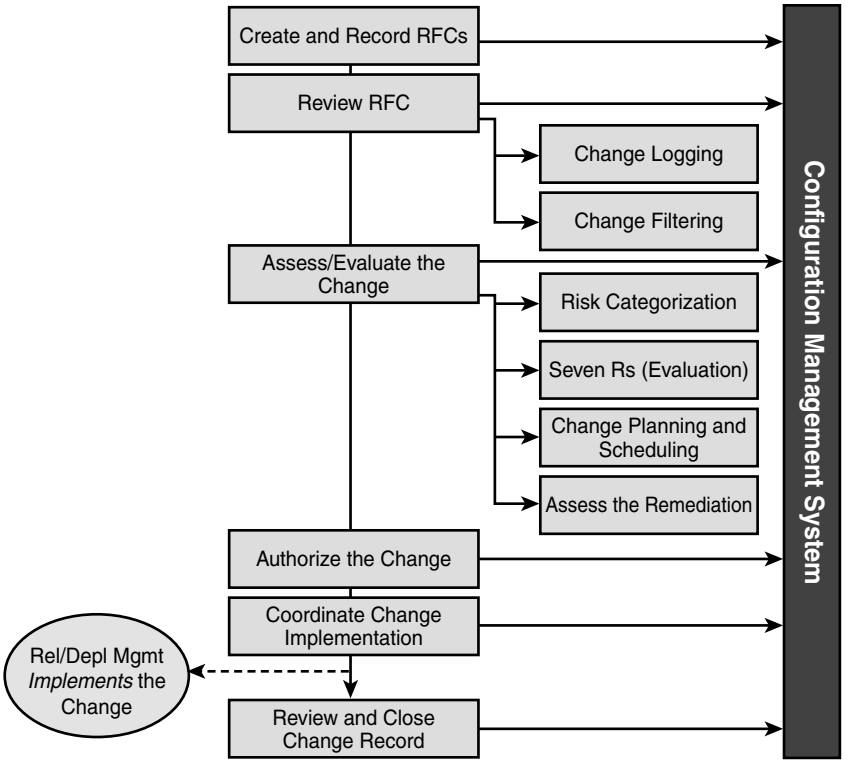

Figure 4-3 Change Management Process Activities

Note

There is no officially named "Change Management Database." Therefore, all changes are tracked within the CMS.

Remember

Change Management manages and coordinates the change.

Release and Deployment Management builds, tests, and implements the change.

Service Asset and Configuration Management tracks the changes to the CIs in the CMDB/CMS.

Lesson 4: Release and Deployment Management

If Change Management *manages* and *coordinates* changes, Release and Deployment Management *builds*, *tests*, *delivers*, *installs,* and *implements* changes.[99]

Release and Deployment Management ensures the following:

- There are clear and comprehensive release and deployment plans.
- All components of the release are capable of delivering the agreed service requirements.
- There is minimal unpredicted impact on production services when changes are released into the operational environment.
- The business is satisfied with all *Service Transition practices.* This might not seem intuitive; however, Release and Deployment Management is where the activities of Service Transition "touch" and affect the customers and users. All other Service Transition processes are largely invisible to the business.

Release and Deployment Management Concepts and Key Terms[100]

A ***release*** is a collection of authorized changes and must be accompanied by an RFC which effectively defines it. The new and changed CIs that make up the release are tested and introduced into the live environment together.

The official ITIL definition of **release** is as follows: A release is defined as the collection of hardware, software, documentation, processes or other components required to implement one or more approved changes to IT services.

A **release unit**[101] describes the portion of a service or IT infrastructure that is normally released at a time. A release unit typically includes sufficient components to perform a useful function. For example, one release unit could be a laptop, which includes the hardware, the operating system, a word processing application, and licenses. Each individual component is not very useful on its own, but combining them provides a usable unit.

A **release package** can be a single release unit or a structured set of release units. Where possible, release packages should be designed so that some release units can be removed if they cause issues in testing.

A **release policy**[102] document for an organization should be produced to clarify the roles and responsibilities for Release Management. There may be one document per organization, or an umbrella set of guidelines and specific details for each supported system or IT service. The Release policy covers Release numbering, frequency, and the level in the IT infrastructure that will be controlled by definable Releases. A Release policy may say, for example, that only strict "emergency fixes" will be issued in between formally planned Releases of enhancements and non-urgent corrections.

The Definitive Media Library (DML) and Definitive Spares[103]

The Definitive Media Library (DML) is the secure library in which definitive, authorized versions of all media CIs are stored and protected. It is both the container and the distribution point for master copies of both off-the-shelf software as well as software built in-house. Master copies of controlled (official) documentation are also stored in the DML in electronic form.

Typically, the DML consists of more than one physical library or location, especially if an organization has many sites or locations. In addition to software, associated documentation and license agreements and activation keys ("media CIs") should also be stored. *Backups are never stored in the DML.*

All items in the DML must be registered as CIs in the CMDB and ultimately in the CMS, and regular audits must be carried out to ensure that the two remain synchronized.

Definitive Spares:[104] An area should be set aside for the secure storage of definitive hardware spares. These are spare components and assemblies that are maintained at the same level as the comparative systems within the live environment. Details of these components and their respective builds and contents should be comprehensively recorded in the CMDB and ultimately the CMS. These can then be used in a controlled manner when needed for additional systems or in the recovery from incidents. Once their (temporary) use has ended, they should be returned to the Definitive Spares storage area or replacements obtained.

DML, CMDB, and CMS Relationship

The CMDB contains *information about* CIs.

The DML contains *the actual media CIs* (the actual .exe, .msi, .pdf, and .doc files).

The CI record for a given piece of software (for example) would contain the name of the software title, version information, and where the installation file is physically located. That physical location is where Release and Deployment Management will install from—the DML.

Both the CMDB and the DML are part of the larger CMS.

Figure 4-4 illustrates the relationship between the CMS, DML, and CMDB.

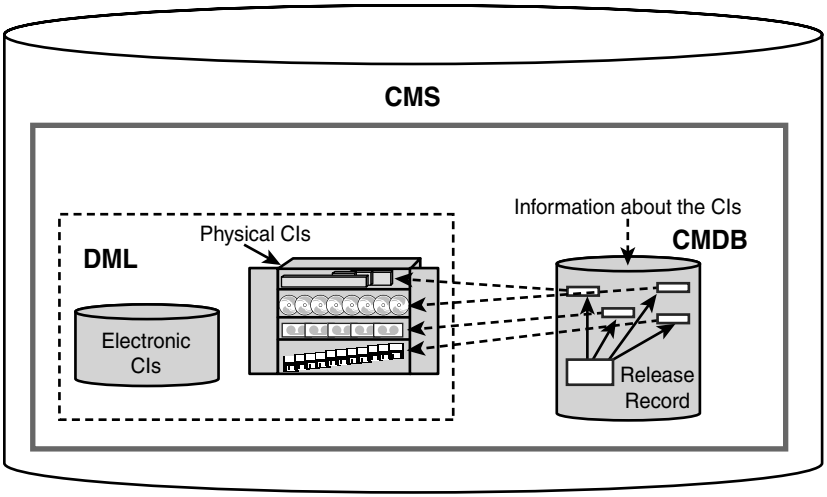

Figure 4-4 The Relationship Between the DML, CMDB, and the Larger CMS

The Change, Release, and SACM Trifecta

The Change Management, Release and Deployment Management, and Service Asset and Configuration Management processes are very closely related because their process' activities constantly intertwine:

- **Change Management** is the process you use to manage and coordinate changes.
- **Release and Deployment Management** is the process you use to build, test, and install/execute the changes.
- **Service Asset and Configuration Management** is the process you use to track and control the changes to services and CIs, using the CMS and the CMDB.

Applying the RACI model, Change Management is *accountable* for the success of all changes, whereas Release and Deployment Management is *responsible* for the success of all changes. SACM is *consulted* and *informed* of all changes.

Roles in Release and Deployment Management

The Release and Deployment Manager is the **process owner** of the Release and Deployment Management process.

As the process owner, this person is responsible for the following tasks (DEMI):

1. **D**ocumenting the Release and Deployment Management process.
2. **E**ducating process participants on how to use the Release and Deployment Management process correctly and ensuring that process participants are complying with the process.

3. **M**easuring the success of the process against KPIs, CSFs, and other targets set.
4. Continually **I**mproving the process. (This is done with input and assistance from the Continual Service Improvement Manager.)

Also, some organizations might choose to segregate certain job duties based on skill set and authority, for instance:

- **Release Package and Build Manager** builds and tests the final release.
- **Deployment Manager** (or deployment staff) physically installs the release.

Lesson 5: Knowledge Management[105]

Knowledge Management spans across the entire service lifecycle.

Often, decisions are made based on a gut feeling rather than hard and fast facts and numbers ("I think" versus "I know"). The goal of Knowledge Management is to ensure that decision-makers have the ability to make informed decisions based on accurate data and careful analysis of trends.

The DIKW Model[106]

Every leader knows that it is important to make decisions based on sound facts. Yet, so many organizations have no practical way to capture the data churned out by various systems and tools, let alone turn that data into something meaningful and useful. Many leaders are then forced to make decisions based on their gut feeling, rather than on the results of careful analysis.

The Data, Information, Knowledge, Wisdom (DIKW) model shows a hierarchy of how data is turned into information, which can then be transformed into useful and actionable knowledge. In the best case, knowledge becomes wisdom.

Figure 4-5 illustrates the Data, Information, Knowledge, Wisdom hierarchy, where:

- **Data** is a set of discrete facts about events.
- **Information** comes from finding relationships between data points, and providing context to data.
- **Knowledge** is composed of tacit experiences, ideas, insights, values, and judgments of individuals. People gain knowledge both from their own and from their peers' expertise, as well as from the analysis of information (and data). Through the synthesis of these elements, new knowledge is created. Decisions cannot be made without knowledge.
- **Wisdom** gives the ultimate discernment of the material and having the application and contextual awareness to provide strong common sense judgment.

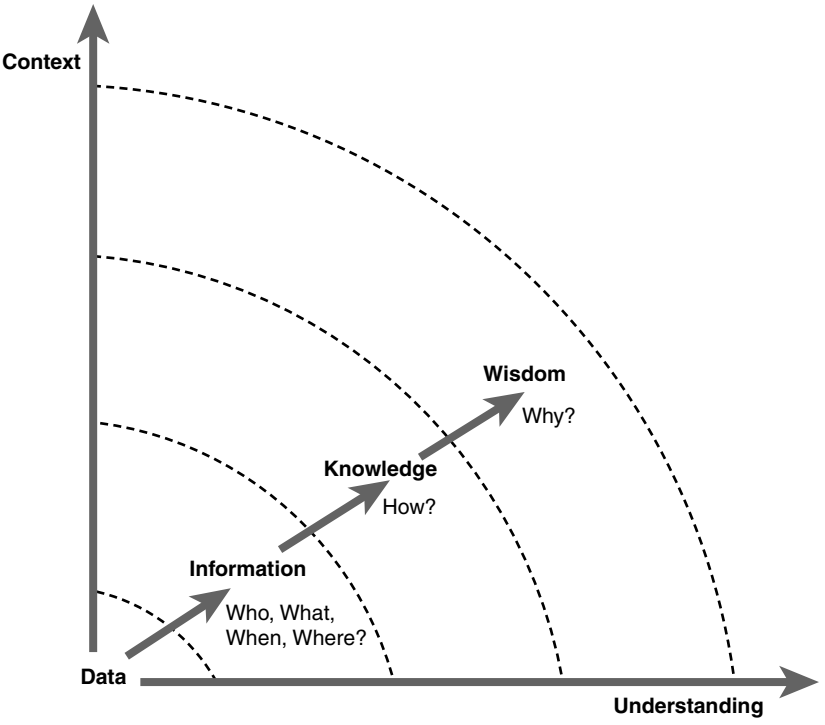

Figure 4-5 DIKW Model

The Service Knowledge Management System (SKMS)[107]

Knowledge Management is controlled in and facilitated by the Service Knowledge Management System (SKMS), which is illustrated in Figure 4-6.

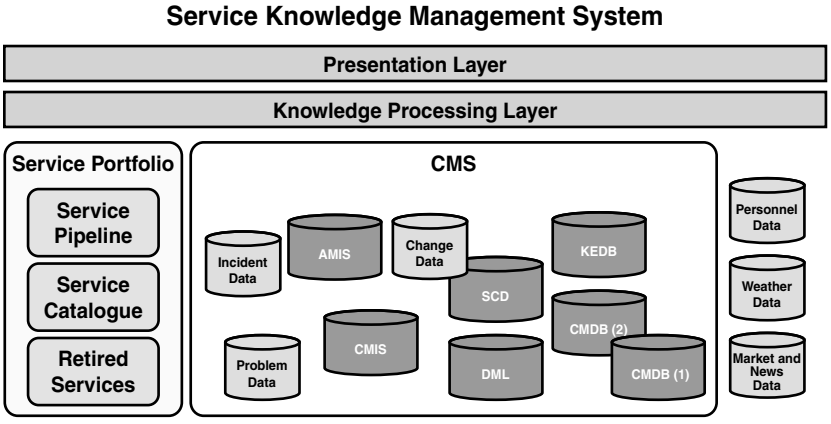

Figure 4-6 SKMS Components

This knowledge in the system will be supported and underpinned by a considerable quantity of data, which will be held in the CMS, and the constituent components of the CMS (the CMDB, the CMIS, SCD, and so on).

The SKMS covers a wide base of knowledge, such as the following:

- The experience of staff
- Peripheral topics, such as weather reports, user headcounts, and important news impacting the market
- User skill levels

This extra (and seemingly irrelevant) data help provides the biggest and most accurate picture possible for the SKMS user.

Knowledge Management Tools Mimic the DIKW Model[108]

The Service Knowledge Management System and its constituent components follow the DIKW model, as illustrated in Figure 4-7:

- **Data** is stored in any database or data source (for example, the CMDBs, the SCD, and so on).
- **Information** is created when trends and relationships are drawn between data; therefore, information is stored in the CMS.
- **Knowledge** is needed to make an actionable decision and to guide the direction of the organization. Knowledge is stored in the SKMS.
- **Wisdom** cannot be stored in a tool.

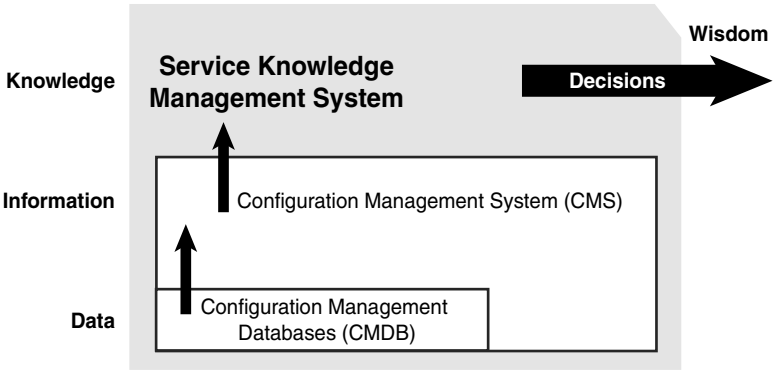

Figure 4-7 The Relationship Between the CMDB, the CMS, and the SKMS

Lesson 6: Sample Questions Based on Chapter 4

Answers can be found at the end of this chapter.

1. Which process is responsible for tracking and maintaining relationships between pieces of data?
    a. Service Asset and Configuration Management
    b. Service Level Management
    c. Change Management
    d. Release and Deployment Management
2. The objective of the Service Asset and Configuration Management process is most accurately described as:
    a. To track changes throughout their lifecycle
    b. To manage service assets and CIs day-to-day
    c. To define and control the components of services and infrastructure and maintain accurate configuration records
    d. To ensure that assets and CIs meet their availability targets as outlined in the SLAs

3. Which phrase is missing from the following sentence?

   "A logical _____ records the relationships between assets, the infrastructure, and services."

   a. Configuration Model

   b. Knowledge Management System

   c. Service Asset Database

   d. Release Package

4. What is the best description of a release unit?

   a. A team that builds, tests, and implements releases into the live environment

   b. The part of a service or infrastructure that is rolled back after a failure during implementation

   c. The portion of a service or IT infrastructure that is changed by a specific release

   d. The portion of a service or IT infrastructure that is normally released together

5. What is the best description of a release package?

   a. The 7 Rs of Change Management

   b. A single release unit, or a structured set of release units

   c. A tool used for software deployment

   d. The portion of a service or IT infrastructure that is normally released together

6. Which ITIL process formally "owns" the Definitive Media Library (DML)?

   a. Release and Deployment Management

   b. Change Management

   c. Service Asset and Configuration Management

   d. Service Level Management

7. Which list shows these items in order from smallest to largest?

   a. CMS, CMDB, SKMS

   b. SKMS, CMDB, CMS

   c. CMDB, CMS, SKMS

   d. Service Portfolio, CMS, CMDB

8. Which of the following cannot be stored in a tool?
    a. Data
    b. Information
    c. Knowledge
    d. Wisdom
9. What type of changes is the ECAB responsible for reviewing prior to authorization?
    a. Urgent changes
    b. Standard changes
    c. Normal changes
    d. Emergency changes
10. Which of the following would be stored in the Definitive Media Library (DML)?
    1. Software developed in-house
    2. Software purchased off the shelf
    3. Relevant license keys and license documentation
    4. Backup copies of software
    a. All of the above
    b. 1 and 2 only
    c. 2, 3, and 4 only
    d. 1, 2, and 3 only

Answers to Sample Questions Based on Chapter 4

1. **A is correct.**
    a. **Correct. Service Asset and Configuration Management uses the CMDB to track relationships between CIs; the CMS is used to track relationships between different data types and data sources.**
    b. Incorrect. Service Level Management is responsible for building maintaining positive relationships between the customer and IT, but this question isn't asking about interpersonal relationships; it is asking about relationships between relationships between pieces of data.
    c. Incorrect. Change Management uses the CMS to assist with risk management when evaluating the change, but the CMS is maintained by SACM.

d. Incorrect. Release and Deployment Management uses the CMS to track releases and uses the DML (which is part of the CMS) to deploy releases into the live environment, but SACM maintains both.

2. **C is correct.**

   a. Incorrect. This is an activity of Change Management.

   b. Incorrect. Managing service assets and CIs day-to-day (or an "operational perspective") would be an activity of one of the processes within Service Operation.

   c. **Correct. The objective of SACM is defined as "To define and control the components of services and infrastructure and maintain accurate configuration information on the historical, planned, and current state of the services and infrastructure."**

   d. Incorrect. This is an activity of Availability Management.

3. **A is correct.**

   a. **Correct. A configuration model records the relationships between assets, infrastructure, and services.**

   b. Incorrect. There is no such tool in ITIL as the Knowledge Management System.

   c. Incorrect. There is no such tool in ITIL as the Service Asset Database.

   d. Incorrect. A release package is a structured set of release units bundled together.

4. **D is correct.**

   a. Incorrect. A release unit is not a team of people.

   b. Incorrect. A release unit describes the portion of a service or IT infrastructure that is normally released together.

   c. Incorrect. A release unit describes the portion of a service or IT infrastructure that is normally released together.

   d. **Correct. The definition of a release unit is the portion of a service or IT infrastructure that is normally released together. An example of a release unit is a PC with an operating system on it and standard software. Those items independently do not deliver much value, so they are normally released together at one time.**

5. **B is correct.**

   a. Incorrect. This describes how we evaluate a change prior to its authorization.

   b. **Correct. The definition of a release package is "a single release unit or a structured set of release units."**

   c. Incorrect. ITIL does not mention specific tools that should be used during deployment.

   d. Incorrect. This describes a release unit, not a release package.

6. **C is correct.**
    a. Incorrect. Release and Deployment Management deploys media CI releases from the DML, but the DML is owned by Service Asset and Configuration Management.
    b. Incorrect. Change Management helps track and control changes to the DML, but SACM owns it.
    c. **Correct. SACM formally owns and manages the DML; however, other processes use it.**
    d. Incorrect. The Service Level Management process has little to do with the DML.
7. **C is correct.**
    a. Incorrect. The CMDB is the smallest, followed by the CMS, which is then part of the SKMS.
    b. Incorrect. The CMDB is the smallest, followed by the CMS, which is then part of the SKMS.
    c. **Correct. The CMDB is the smallest, followed by the CMS, which is then part of the SKMS.**
    d. Incorrect. The CMDB is the smallest, followed by the CMS, which is then part of the SKMS. The Service Portfolio forms part of the SKMS.
8. **D is correct.**
    a. Incorrect. Data is stored in a database or a document.
    b. Incorrect. Information is stored in the CMS.
    c. Incorrect. Knowledge is stored in the SKMS.
    d. **Correct. Wisdom cannot be stored in a tool.**
9. **D is correct.**
    a. Incorrect. The term "urgent change" is no longer a term used in ITIL V3. It is strictly an ITIL V2 term.
    b. Incorrect. Standard changes are pre-authorized changes and do not require approval each time.
    c. Incorrect. Normal changes are not emergencies.
    d. **Correct. The "E" in "ECAB" stands for "Emergency" because it evaluates Emergency Changes only.**
10. **D is correct.**
    a. Incorrect. Backup copies (#4) are never stored in the DML.
    b. Incorrect. Items 1 and 2 are correct, but license keys and license documentation would also be stored in the DML.

c. Incorrect. Backup copies (#4) are never stored in the DML, and in-house developed software would be stored in the DML.

d. **Correct. Items 1, 2, and 3 are correct; however, backup copies are never stored in the DML.**

Endnotes/Syllabus Requirements

74. This section satisfies Syllabus Requirement ITILFND02-02-6.

75. This section satisfies Syllabus Requirement ITILFND02-02-07.

76. This section satisfies Syllabus Requirement ITILFND05-05-52.

77. This section satisfies Syllabus Requirement ITILFND03-03-34.

78. This section satisfies Syllabus Requirements ITILFND03-03-17 and ITILFND05-05-52.

79. This section satisfies Syllabus Requirement ITILFND05-05-52.

80. This section satisfies Syllabus Requirement ITILFND05-05-52.

81. This section satisfies Syllabus Requirement ITILFND05-05-52.

82. This section satisfies Syllabus Requirements ITILFND03-03-19 and ITILFND05-05-52.

83. This section satisfies Syllabus Requirements ITILFND03-03-18 and ITILFND05-05-52.

84. This section satisfies Syllabus Requirements ITILFND03-03-18 and ITILFND05-05-52.

85. This section satisfies Syllabus Requirement ITILFND05-05-52.

86. This section satisfies Syllabus Requirement ITILFND05-05-51.

87. This section satisfies Syllabus Requirement ITILFND03-03-20.

88. This section satisfies Syllabus Requirement ITILFND05-05-51.

89. This section satisfies Syllabus Requirement ITILFND05-05-51.

90. This section satisfies Syllabus Requirement ITILFND05-05-51.

91. This section satisfies Syllabus Requirement ITILFND05-05-51.

92. This section satisfies Syllabus Requirement ITILFND05-05-51.

93. This section satisfies Syllabus Requirement ITILFND03-03-21.

94. This section satisfies Syllabus Requirements ITILFND05-05-51 and ITILFND03-03-21.

95. This section satisfies Syllabus Requirement ITILFND03-03-21.

96. This section satisfies Syllabus Requirement ITILFND05-05-51.

97. This section satisfies Syllabus Requirements ITILFND03-03-23 and ITILFND05-05-51.

98. This section satisfies Syllabus Requirement ITILFND05-05-51.

99. This section satisfies Syllabus Requirement ITILFND05-05-61.

100. This section satisfies Syllabus Requirement ITILFND05-05-61.

101. This section satisfies Syllabus Requirement ITILFND03-03-22.

102. This section satisfies Syllabus Requirement ITILFND03-03-35.

103. This section satisfies Syllabus Requirement ITILFND03-03-19.

104. This section satisfies Syllabus Requirement ITILFND05-05-61.

105. This section satisfies Syllabus Requirement ITILFND05-05-62.

106. This section satisfies Syllabus Requirement ITILFND05-05-62.

107. This section satisfies Syllabus Requirements ITILFND05-05-62 and ITILFND03-03-16.

108. This section satisfies Syllabus Requirements ITILFND05-05-62 and ITILFND03-03-16.

Chapter 5

Service Operation

Lesson 1: Service Operation Overview

Although each stage in the ITIL service lifecycle provides value to the business, Service Operation provides the most, as this is where the strategy and design have finally been transitioned into the operational environment. In this phase, the business can finally *use* the service! In addition, now that your service is up and running, you can measure it against the targets in your Service Level Agreements (SLAs) for use in your service reporting back to the customer, and to find opportunities for improvement.

The Purpose and Scope of Service Operation[109]

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

Service Operation embodies five processes and four functions, as outlined in Table 5-1. Service Operation is the only core publication that describes functions.

Table 5-1 Service Operation Processes and Functions

Processes	Functions
Event Management	Service Desk
Incident Management	Technical Management
Request Fulfillment	Application Management
Problem Management	IT Operations Management
Access Management	

Processes alone will not result in effective Service Operation. A stable infrastructure and appropriately skilled people are needed as well. To achieve this, Service Operation relies on several groups of skilled people (called **Functions**), all focused on using processes to match the capability of the infrastructure to the needs of the business.

Remember

Processes are what gets done; functions are who does them.

In this Service Operation phase, you do the following:

- Manage the users' support requests (via the service desk *function* and Request Fulfillment *process*).
- Monitor operational events and alerts (via the Event Management *process*).
- Restore the service after disruptions (via the Incident Management *process*).
- Find the root cause of incidents and prevent their recurrence, as well as reduce incident duration (via the Problem Management *process*).
- Grant and deny access to services (via the Access Management *process*).

You have teams dedicated to

- Answering calls from users (via the service desk *function*)
- Maintaining the software (via the Application Management *function*)
- Executing the day-to-day "behind-the-scenes" activities (via the IT Operations Management *function*)
- Supporting the infrastructure (via the Technical Management *function*)

Communication in *Service Operation*[110]

Good communication is needed with other IT teams and departments, with users and internal customers and between the Service Operation teams and departments themselves. Issues can often be prevented or mitigated with appropriate communication.

An important principle is that all communication must have an intended purpose or a resultant action. Information should not be communicated unless there is a clear audience.

The following types of communication are common in the Service Operation phase:

- Routine operational communication
- Communication between shifts
- Performance reporting
- Communication in projects
- Communication related to changes
- Communication related to exceptions
- Communication related to emergencies

- Training on new or customized processes and service designs
- Communication of strategy and design to Service Operation teams

Lesson 2: ITIL's Four Functions[111]

Functions are self-contained units of organizations that are specialized to perform certain types of work and responsible for specific outcomes. They have the necessary resources and capabilities (tools, budget, skills, and so on) to perform those types of work and provide the expected outcomes.

The Service Operation functions described in this section are needed to manage the "steady state" operational IT environment. These are logical functions and do not have to be performed by an equivalent organizational structure. This means that Technical and Application Management can be organized into any combination and into any number of departments.

The second-level groupings in Figure 5-1 (Mainframe, Server, Network, etc.) are examples of typical groups of activities performed by Technical Management and again, are not a suggested organizational structure.

As Figure 5-1 illustrates, the service desk is a free-standing function; however, there is some overlap between the Technical Management, IT Operations Management, and Application Management functions. This is partly because IT Operations Management often takes their direction from Technical Management and Application Management. Also, some of the typical IT Operations Management duties might be handled by either Technical Management or Application Management, depending on the skill level of your IT Operations Management team.

Technical Management[112]

Technical Management refers to the groups, departments, or teams that provide technical expertise and overall management of the IT Infrastructure:

- Technical Management is the custodian of technical knowledge and expertise related to managing the IT infrastructure.
- Technical Management provides the actual resources to support the IT Service Management Lifecycle. Technical Management ensures that resources are effectively trained and deployed to design, build, transition, operate and improve the technology required to deliver and support IT Services.

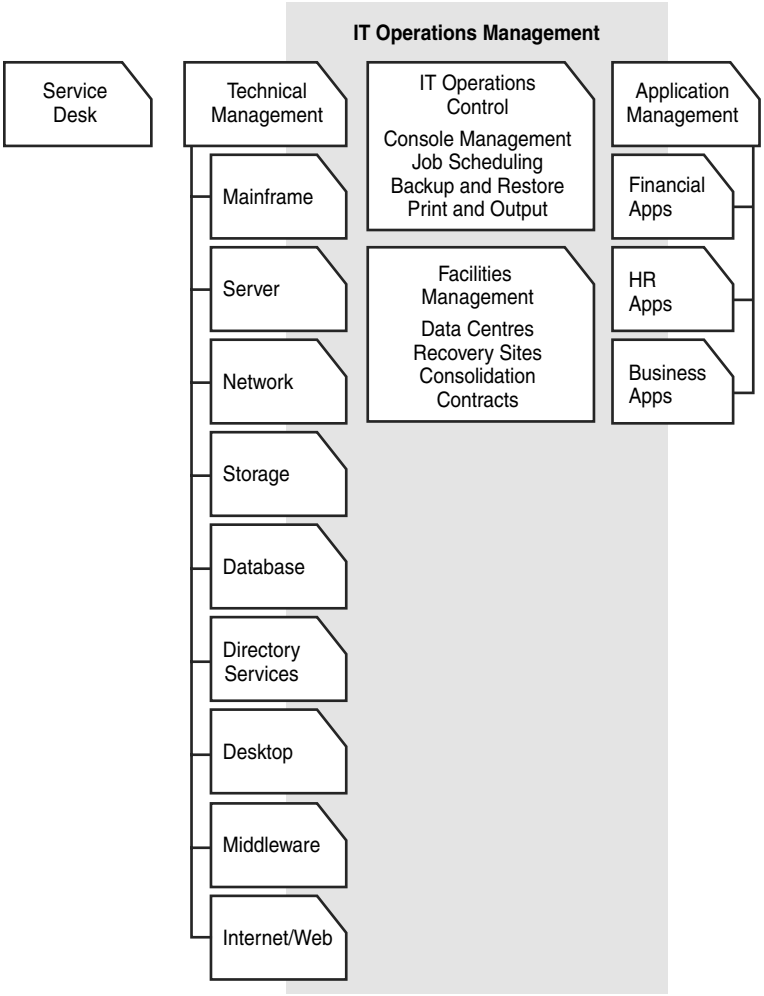

Figure 5-1 The Four Functions of ITIL

Application Management[113]

The next function is **Application Management**, which manages applications throughout their lifecycle. It supports and maintains production applications and also plays a role in the design, testing, and improvement of applications. During the Service Design phase, it helps answer the question: "Should we buy or build an application?"

Note

Application Management members are not always application *developers*. Application Management simply supports the applications used in your organization.

Application Management, working together with Technical Management, ensures that the knowledge required to design, test, manage and improve IT Services is identified, developed, and refined. It provides the actual resources to support the IT Service Management Lifecycle. Furthermore, Application Management provides guidance to IT Operations Management about how best to carry out the ongoing operational management of applications.

IT Operations Management[114]

IT Operations Management is made up of two components: *IT Operations Control* and *Facilities Management*. IT Operations Control is responsible for many "behind-the-scenes" tasks: tape backups, copy/print, job scheduling, and manning the IT Operations Bridge (sometimes referred to as a Network Operations Center, or NOC). Facilities Management is responsible for data centers, HVAC, cabling, and so on, as it relates to IT.

IT Operations Management is the function responsible for the daily operational activities needed to manage the IT Infrastructure. In some organizations this is a single, centralized department, while in others some activities and staff are centralized and some are provided by distributed or specialized departments. IT Operations Management has two functions that are unique and which are generally formal organizational structures. These are:

- **IT Operations Control**,[115] which is generally staffed by shifts of operators and which ensures that routine operational tasks are carried out. IT Operations Control will also provide centralized monitoring and control activities, usually from an IT Operations Bridge or Network Operations Center (NOC).
- **Facilities Management**[116] refers to the management of the physical IT environment, usually data centers or computer rooms. In many organizations Technical and Application Management are co-located with IT Operations in large data centers.

Note

On the exam, you may find the "IT" omitted, thus calling these groups "Operations Management" and "Operations Control."

Service Desk[117]

Note

Many organizations use the term "Help Desk" as a synonym for "Service Desk." For purposes of the ITIL V3 Foundation exam, there is no such thing as a Help Desk.

The service desk serves as a single point of contact (SPOC) for users to get information to and from IT. Having all communication flowing solely through the service desk gives users and IT staff confidence in knowing whatever the issue or request is, it will be managed in a timely and satisfactory way. This also frees up second- and third-tier support personnel from interfacing with users and enables them instead to focusing on the technical challenges at hand. Having a well-trained service desk saves money by allowing IT personnel to perform more technical duties instead of addressing issues that can be solved by the service desk.[118]

Service desk personnel handle a wide array of technical issues over the course of a typical day. Because of this, service desk technicians are often promoted to other IT support functions as a logical career path.

Service Desk Objectives

The objectives of the service desk are as follows:

- Logging all relevant incident/service request details
- Providing first-line investigation and diagnosis
- Resolving those incidents/ fulfilling those service requests they are able; escalating those they cannot within agreed timescales
- Keeping users informed of progress
- Closing all resolved incidents and service requests
- Conducting user satisfaction surveys and callbacks
- Update the CMS under the direction and approval of Configuration Management (if so agreed)

Service Desk Structures

Service desks may be structured in one of several ways, or even a hybrid of two or more of these approaches:

- **Local Service Desk:**[119] Simply speaking, a local service desk has a one-to-one relationship between user locations and service desks—if your organization has 12 separate locations housing users, there will be 12 separate service desks, all working independently of each other. Users often call an extension to get technical support as opposed to calling a number outside the building. Local service desks usually are independently operated; each most likely will have its own freestanding CMS.
- **Centralized Service Desk:**[120] A centralized service desk has a many-to-one relationship between user locations and the service desk. If your organization has 12 separate locations housing users, you will have one service desk servicing them all. Users will typically call a toll-free number to get technical support. Service desk personnel in this structure must use the same CMS.
- **Virtual Service Desk/Follow the Sun:**[121] A virtual service desk harnesses the power of the Internet and advanced phone technology by allowing service desk personnel to work anywhere in the city, country, or world but still appearing as if they are working from a single location (if, of course, that is a desired effect). Users call a single toll-free number, and the call will be routed according to the logic in the phone switch. Service desk personnel in this structure absolutely must use the same CMS.

  Virtual service desks can be structured so calls will **Follow the Sun**. If a user based in North America requires technical support at 3:00 a.m., a service desk agent in Europe or India may take their call because it is daytime there.

A Virtual or Follow the Sun approach can be challenging to implement due to difficulties in streamlining escalation and handover procedures.

Service Desk Roles[122]

In larger organizations where the Service Desk is of a significant size, a **Service Desk Manager** role may be justified with the Service Desk Supervisor(s) reporting to him or her. In such cases this role might perform the following activities:

- Manage the overall desk activities, including the supervisors
- Act as a further escalation point for the supervisor(s)
- Take on a wider customer-services role
- Report to senior managers on any issue that could significantly impact the business
- Attend Change Advisory Board meetings
- Take overall responsibility for incident and Service Request handling on the Service Desk. This could also be expanded to any other activity taken on by the Service Desk; for example, monitoring certain classes of event.

In very small desks, it is possible that the senior Service Desk Analyst will also act as the Supervisor; however, in larger desks it is likely that a dedicated **Service Desk Supervisor** role will be needed. Where shift hours dictate it, there might be two or more post-holders who fulfill the role, usually on an overlapping basis. The Supervisor's role is likely to include:

- Ensuring that staffing and skill levels are maintained throughout operational hours by managing shift staffing schedules, etc.
- Undertaking HR activities as needed
- Acting as an escalation point where difficult or controversial calls are received
- Production of statistics and management reports
- Representing the Service Desk at meetings
- Arranging staff training and awareness sessions
- Liaising with senior management
- Liaising with Change Management

The primary **Service Desk Analyst** role is that of providing first-level support through taking calls and handling the resulting incidents or Service Requests using the Incident Management and Request Fulfillment processes, in line with the objectives described earlier.

Lesson 3: Event Management

Event Management is the process responsible for managing events throughout their lifecycle. *An event can be defined as any detectable or discernible occurrence that has significance for the management of the IT Infrastructure or the delivery of IT services and evaluation of the impact a deviation might cause to the services.*[123] Events are typically notifications created by an IT service, Configuration Item (CI), and/or passive or active monitoring tool.

Purpose/Goal/Objective:[124] The ability to detect events, make sense of them, and determine the appropriate control action is provided by Event Management. Event Management is therefore the basis for Operational Monitoring and Control. It also provides a way of comparing actual performance and behavior against design standards and SLAs which becomes an input for Continual Service Improvement activities.

Event Types

Event Management is also responsible for defining thresholds related to these events, and when these *thresholds* are exceeded, an **alert**[125] is issued to draw specific attention to this/these event(s). An alert requires a person or a team to respond.

Some events are related to a failure and will be reported as an **incident**, which is handled by the Incident Management process.

There are three types of events:[126]

- **Informational:** Signifies *regular* operation ("All is well! Just a heads up that this normal thing has happened!"):
  - A user has successfully logged into an application.
  - Notification that a batch job has completed.
  - An email was read by its intended recipient.
- **Warning:** Signifies *unusual* operation ("Be on the lookout– things could get ugly soon. You might want to take a look at this."):
  - A user attempts to log in three times with an incorrect password.
  - A routine scan has detected unauthorized software.
  - A device's CPU is above its acceptable utilization rate but is still functional.
- **Exception:** Signifies an *abnormality* ("Yikes! Someone needs to jump on this now!"):
  - A server is down.
  - A transaction is taking 15% longer than normal.

Each organization needs to define what constitutes "regular" versus "unusual" versus "exception."

Event Management Roles

It is unusual for an organization to appoint an Event Manager, as events tend to occur in multiple contexts and for many different reasons. However, it is important that Event Management procedures are coordinated to prevent duplication of effort and tools.

The **service desk** is typically not involved in Event Management, unless an event requires something that your organization has deemed within the scope of the service desk.

Technical Management and **Application Management** performs Event Management for the systems under their control; they also help resolve incidents and problems related to events. Additionally, **Technical Management** and **Applications Management** also define what constitutes an event, and what control action must be taken if an event occurs.

IT Operations Management performs event monitoring and provide first-line support, typically from an IT Operations Bridge or a Network Operations Center (NOC).

Lesson 4: Incident Management

The primary goal of Incident Management is to restore **normal service operation as quickly as possible** and minimize the adverse impact on business operations, thus ensuring that the best possible levels of service quality and availability are maintained.

It is critical that your SLA defines "normal."

Take a look at some different incident scenarios in the sections that follow and how each is handled via the Incident Management process.

Scenario 1

Sally in Marketing calls the service desk to report she cannot print. The service desk asks her where she normally prints, and she reports "I normally print to PrinterA; it happens to be right near my desk here on the first floor." The service desk remotes into her PC and tries to fix her issue, but they can't fix the problem. The service desk agent looks at the SLA, which states that "All users must be able to print during normal service hours," but gives no specification as to *where* they must be able to print. To resolve the issue, the service desk agent changes Sally's default printer to PrinterB, which is up on the third floor. Sally prints a test page successfully, and Sally's incident is now ***closed.***

Explanation:

If the SLA states that Sally must be able to print *somewhere* without specifying to which specific printer, you can *close* the incident when Sally is able to print *someplace*. The service has been restored according to what is normal in the SLA.

The objective of Incident Management is to restore the *service of* ***printing*** for Sally, not to restore a specific printing device.

You might be thinking, "Wow, Sally isn't going to be very happy about that," and you might be right. But Incident Management isn't about making people happy; it's about delivering what is stated in the SLA. This is why SLAs must be written well!

In the meantime, 14 more people have called to report that they cannot print to PrinterA. The service desk has opened 14 *more* incident tickets and will reroute those users' print jobs over to PrinterB, and will then close all 14 incidents—just like they did with Sally. This brings the total

number of people affected by the PrinterA outage to 15. As of right now, the *service of **printing*** has been restored for a total of 15 people.

You're probably thinking, "Why doesn't someone just go fix the printer already? There are 15 people who can't print to PrinterA." This is where the **Problem Management** process kicks in, because Problem Management's job is to find the root cause and the solution to major or multiple incidents. The service desk notifies the Problem Manager of the trend, and the Problem Manager opens *one problem ticket that is linked to all 15 incidents***.**

Scenario 2

Matt in HR calls the service desk to report that he cannot print. The service desk asks Matt where he normally prints, and he reports "The printer is called HRPrint01; it's our only printer. It's located back here in our secure area because we print private information." The service desk agent looks up the SLA and discovers that there is an HR-specific SLA (called a "customer-based SLA" in ITIL-speak), which states that "All HR employees must be able to print to that one HR-specific printer called HRPrint01 during normal service hours." Because there is only one printer in the entire HR department, the service desk cannot close the incident because there is no workaround available; there is no way to restore the *service of **printing*** to Matt. This incident must remain open until the HR printer is repaired.

Explanation:

Here, the SLA gives specific direction for users in the HR department. Because HR personnel print confidential documents, they cannot print to the public printers in the hallway. If the HR printer is unavailable, the *service of **printing*** cannot be restored because there is no backup printer in the HR area.

Just like in the previous scenario, the service desk notifies the Problem Manager that Matt in HR can't print to HR's sole printer. The Problem Manager opens a problem ticket and links Matt's open incident ticket to this single problem ticket. In this scenario, there is an incident and a problem open at the same exact time for the same issue. After a technician fixes the printer, both the incident ticket and the problem ticket can be closed simultaneously.

Remember

Incident Management restores the *service*. Problem Management restores the *device*.

Note

Lesson 6 in this chapter covers the Problem Management process in more detail.

Incident Management Scope

Incident Management includes any event that disrupts or could disrupt a service.

Incidents are communicated to the service desk by users, IT staff, and event monitoring tools.

Note

Not all events are incidents!

Incident Management Key Terms

Some of the key Incident Management terms are as follows:

- Incident:[127] An unplanned interruption to an IT service or reduction in the quality of an IT service. *Failure of a configuration item that has not yet impacted service is also an incident.*
- **Timescales**: Timescales describe how quickly an incident must be resolved. These naturally vary by priority. Timescales must be documented in the SLA.
- **Incident Models**: A **model** is a predefined way of handling a repetitive task. An Incident Model is simply a predefined way to handle repetitive incidents.
- **Major Incidents**: A major incident usually affects a large number of users or severely impacts a critical service and is given higher priority. Major incidents have their own separate procedures and shorter timescales. It is up to your organization to determine what counts as a major incident and what does not; these will vary from organization to organization.
- **Service Request**:[128] A user needs *something* from IT, but nothing is broken. ("Where can I find the RFC form?" "I have a new employee starting in my department next week and need to get him set up." "Do we have any color printers in this building?"). *Service requests are not incidents*. Service requests are handled through the Request Fulfillment process, which is covered in the next lesson.

Incident Prioritization[129]

The formula for calculating priority is **Priority = Urgency + Impact.** This formula can be used to calculate the priority of incidents, problems, changes, or anything else:

- **Priority:** Simply means "the order in which we will handle these items." In order to prioritize incidents, we must consider the incident's impact and urgency.
- **Impact:** The effect of the incident upon the business. (How much is this incident hurting the business?)
- **Urgency:** How quickly the incident needs to be resolved.

The service desk, in consultation with the user, determines the incident's priority by calculating the impact and the urgency.

Routing: Escalation[130]

If the service desk is unable to resolve an incident on their own, they must escalate the ticket to another group or team.

If the service desk requires someone with more knowledge, the ticket should undergo a **Functional Escalation**. For example, if the incident is related to a database error, the service desk might escalate the incident to someone with *more knowledge* in that area, such as a database administrator.

If the service desk discovers a major incident or possibly an incident that might breach an SLA, they must perform a **Hierarchic Escalation**; this means someone with *more authority* must get involved so they can direct their resources appropriately.

The Incident Management Process Flow[131]

Figure 5-2 illustrates a flowchart of the Incident Management process, the steps for which are described in the list that follows.

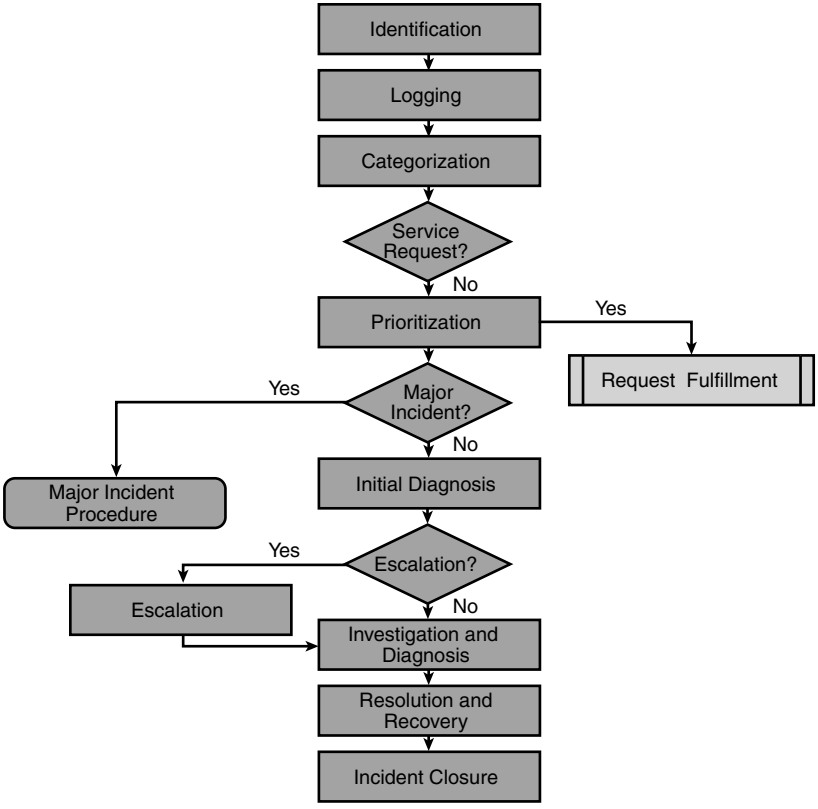

Figure 5-2 Incident Management Process

1. **Identification:** Obviously, an incident cannot be investigated until you learn that an incident has actually occurred. Incidents can be identified via users, IT staff, or event monitoring tools.

2. Logging: Incidents must be fully logged and date/time stamped, regardless of whether they are raised through a Service Desk telephone call or automatically detected via an event alert.

3. **Categorization:** Categorization might be several levels deep (some organizations use a *SCIM* approach: System, Component, Item, Module). Placing an incident in the proper category means grouping them by type, and possibly by which support group will address them. Proper incident categorization is important so Problem Management (and other processes) can find trends.

   If the call is determined to be a service request and not an incident, the service request is addressed by the Request Fulfillment process.

4. **Prioritization:** Prioritization determines the order in which the incident will be handled. The service desk agent, in consultation with the user, determines the priority based on impact and urgency.

   If it is a major incident, the appropriate major incident procedure is followed.

5. **Initial Diagnosis:** The service desk agent makes an initial diagnosis. Diagnostic scripts and known error information are valuable here. If possible, the service desk agent will resolve the incident and close the incident if the resolution is successful.

   If the service desk agent cannot resolve the incident, the user should be given the incident reference number (ticket number), and the service desk should **escalate** the incident so another team can find a resolution.

6. **Investigation and Diagnosis:** As the assigned technical group investigates and diagnoses the incident, a historical record of activities must be maintained in the incident record (ticket).

7. **Resolution and Recovery:** When a resolution has been identified and tested, the recovery action completed, and the service has been fully restored to the user(s), the incident record must be marked as resolved. The resolving party must be sure to record in the incident record the steps taken to resolve the incident. When complete, the incident record is passed back to the service desk for closure.

8. **Closure:** The *service desk (only)* should check that the incident is fully resolved and that the users are satisfied and willing to agree the incident can be closed. Before closure, the service desk should also:

   - Double-check that the incident is in the proper category to ensure accuracy in reporting.
   - Check to see whether they should ask the Problem Manager to open a problem record.

Incident Management Roles

The Incident Manager is the **process owner** of the Incident Management process.

As the **process** owner, this person is responsible for the following tasks (DEMI):

1. **D**ocumenting the Incident Management process.
2. **E**ducating process participants on how to use the Incident Management process correctly and ensuring that process participants are complying with the process.
3. **M**easuring the success of the process against KPIs, CSFs, and other targets he/she has set.
4. Continually **I**mproving the process. (This is done with input and assistance from the Continual Service Improvement Manager.)

First-line support is typically handled by the service desk. Second-line support can either be a second tier of the service desk employing more technically skilled agents, or it can fall outside of the service desk function. Third-line support is typically Technical Management, IT Operations Management, and Application Management, as well as any third-party suppliers who might be assisting in incident resolution.

Note

Because the service desk is the team that champions the Incident Management process, it might make sense to have your service desk supervisor/manager also serve as the Incident Management process owner. However, this is not an official ITIL edict; it is merely a suggestion as a way to consolidate headcount.

Lesson 5: Request Fulfillment

Request Fulfillment refers to the process of dealing with Service Requests from the users.

The **objectives** of the Request Fulfillment process include: [132]

- To provide a channel for users to request and receive standard services for which a predefined approval and qualification process exists
- To provide information to users and customers about the availability of services and the procedure for obtaining them
- To source and deliver the components of requested standard services
- To assist with general information, complaints, or comments

Request Fulfillment Scope

Because of their frequency and the fact that Service Requests are low risk, it is better to handle them through a separate process rather than obstruct the Incident and Change Management processes.

It is up to the organization to define which requests will be handled through the Request Fulfillment process and which ones need to be addressed via the Change Management process, however.

Request Fulfillment Key Terms

Some of the key Request Fulfillment terms are as follows:

- **Service Request**: Term used as a generic description for many varying types of demands that are placed upon the IT Department by the users. Many of these are actually small changes—low risk, frequently occurring, low cost, etc. (e.g., password reset, additional software on a single desktop) or might be just a request for information or documentation.
- **Request Models:** A predefined approach for handling a frequently occurring service request. This is similar to the concept of Incident Models, described in the previous lesson.

Request Fulfillment Roles

Initial handling of Service Requests will be undertaken by the Service Desk and Incident Management staff. Eventual fulfillment of the request will be undertaken by the appropriate Service Operation team(s) or departments and/or by external suppliers, as appropriate. Often, Facilities Management, Procurement, and other business areas aid in the fulfillment of the Service Request.

Lesson 6: Problem Management

Problem Management is the process responsible for managing the lifecycle of all problems by finding the root cause, finding the solution, and submitting a Request for Change (RFC) to have the problem permanently fixed through a change.

A **problem** is defined as the unknown root cause of one or more incidents.[133]

Problem Management Objectives[134]

The primary objectives of Problem Management are to prevent problems and resulting incidents from happening, to eliminate recurring incidents, and to minimize the impact of incidents that cannot be prevented.

In addition, Problem Management

- Finds the root cause of problems.
- Finds the solution to problems.
- Submits RFCs to Change Management to get the problem fixed via a change.
- Prevents problems and resulting incidents from happening (*Proactive Problem Management*).
- Eliminates recurring incidents.
- Minimizes the impact of incidents that cannot be prevented.
- Maintains the Known Error Database and ensures its accuracy.
- Keeps track of the costs associated with problems and reports those to Financial Management.

Problem Management Scope[135]

Problem Management includes the activities required to diagnose the root cause of incidents and to determine the resolution to those problems. It is also responsible for ensuring that the resolution is implemented through the appropriate control processes, especially Change and Release and Deployment Management.

Problem Management will also maintain information about problems and the appropriate workarounds and resolutions, so that the organization is able to reduce the number and impact of incidents over time. In this respect, Problem Management has a strong interface with Knowledge Management.

Problem Management will also maintain information about problems and the appropriate workarounds and resolutions, so that the organization is able to reduce the number and impact of incidents over time. In this respect, Problem Management has a strong interface with Knowledge Management, and tools such as the Known Error Database will be used for both.

Note

Although Incident and Problem Management are separate processes, they are closely related and will typically use the same tools, and should use the same categorization, impact, and priority coding systems. This will help ensure accurate and meaningful reporting, as well as help ensure effective communication while dealing with incidents and related problems.

Value to the Business[136]

Implementing a robust Problem Management process leads to a higher availability of IT services, higher productivity of IT staff, reduced expenditure on workarounds or fixes that do not work, and reduction in cost of effort in resolving recurring incidents.

Problem Management Key Terms

Some of the key Problem Management terms are as follows:

- **Problem:**[137] A problem is defined as the unknown root cause of one or more incidents.
- **Workaround:**[138] Reducing or eliminating the impact of an incident or problem for which a full resolution is not yet available. Rebooting a PC when an application crashes is considered a workaround because the root cause of the word processing crash was not found, but this action enables the user to continue working. **Workarounds for problems are documented as Known Error records in the Known Error Database (KEDB).**
- **Known Error**:[139] Known Errors have a *known* root cause. As diagnosis is complete and particularly where a workaround has been found (even though it may not yet be a permanent resolution) a Known Error record must be raised and placed in the Known Error Database so that if further Incidents or problems arise they can be identified and the Service restored more quickly. There might be scenarios where a permanent solution has been identified as well but not yet applied due to any reason; in that case, an Error should be recorded in the Known Error Database.

- **Known Error Database (KEDB)**:[140] The purpose of a Known Error Database is to allow storage of previous knowledge of Incidents and Problems—and how they were overcome—to allow quicker diagnosis and resolution if they recur. The Known Error record should hold exact details of the fault and the symptoms that occurred, together with precise details of any workaround or resolution action that can be taken to restore the Service and/or resolve the problem. The Known Error Database is owned by Problem Management; however, it is used by many teams, most notably the Service Desk.

  The service desk uses the KEDB during the Incident Management process to see if any incidents with the same or similar symptoms already exist. If they do exist, there might be a workaround documented in the KEDB that can be used to restore the service much faster.

  Service desk agents use the CMS to cross-reference data within their incident tracking system and the KEDB to help determine the impact of the incident and to see if there is additional information about the incident available.

Note

Only the Problem Manager is allowed to populate the KEDB. Anyone can read from it, and anyone can suggest additions to it; however, to keep the integrity of the data high, only the Problem Manager can write to the KEDB. As the saying goes, "Too many cooks spoil the soup."

- **Problem Model**: Many Problems will be unique and will require handling in an individual way; however, it is conceivable that some Incidents might re-occur because of dormant or underlying Problems (for example, where the cost of a permanent resolution will be high, so leadership decides to simply live with the problem.). A Problem Model is a way of predefining the steps that should be taken to a particular type of recurring problem in an agreed way. This is similar to the concept of Incident Models.

Problem Management Process Flow[141]

Figure 5-3 illustrates a flowchart of the Problem Management process, the steps for which are described in the list that follows.

1. **Problem Detection**: Problems can be detected through various means. The Service Desk might notice that multiple users have called about the same issue, an event monitoring tool might send a notification which warrants attention, or a network technician might notice a Problem while performing routine tasks.
2. **Problem Logging**: Regardless of the detection method, all the relevant details of the problem must be recorded so that a full historic record exists. This must be date and time stamped to allow suitable control and escalation. A cross-reference must be made to the incident(s) which initiated the Problem Record—and all relevant details must be copied from the Incident Record(s) to the Problem Record.

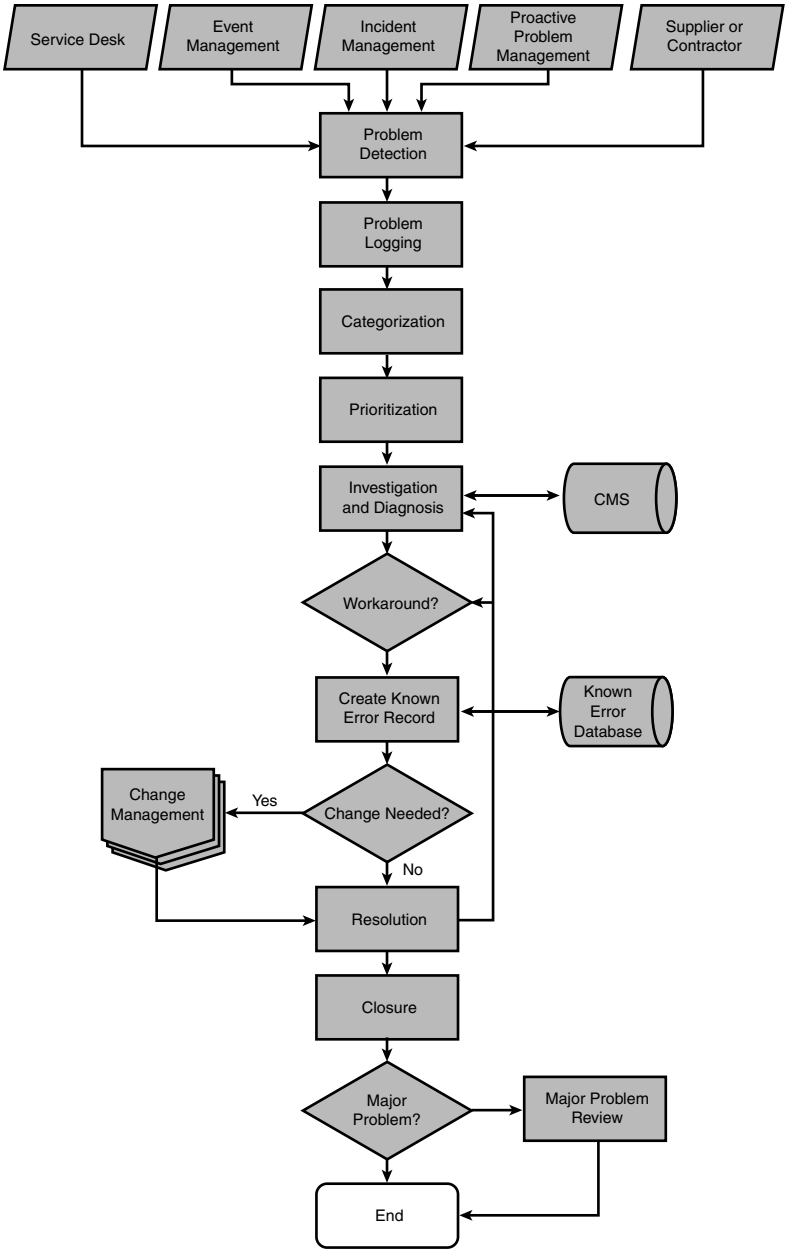

Figure 5-3 Problem Management Process

3. **Problem Categorization**: Problems must be categorized in the same way as incidents (and it is advisable to use the same coding system) so that the true nature of the problem can be easily traced in the future and meaningful management information can be obtained.

4. **Problem Prioritization**: Problems must be prioritized in the same way and for the same reasons as incidents **(Urgency + Impact)**; however, the frequency and impact of related incidents must also be taken into account.
5. **Problem Investigation and Diagnosis**: An investigation should be conducted to try to diagnose the root cause of the problem.
6. **Workaround**: In some cases it might be possible to find a workaround to the incidents caused by the problem—a temporary way of overcoming the difficulties. In cases where a workaround is found, it is therefore important that the problem record remains open, and details of the workaround are always documented within the Problem Record.
7. **Raising a Known Error Record**: As soon as the diagnosis is complete, and particularly where a workaround has been found (even though it may not yet be a permanent resolution), a Known Error Record must be raised and placed in the Known Error Database, so that if further incidents or problems arise, they can be identified and the service restored more quickly. However, in some cases it might be advantageous to raise a Known Error Record even earlier in the overall process—just for information purposes, for example—even though the diagnosis might not be complete or a workaround found, so **it is inadvisable to set a concrete procedural point exactly when a Known Error Record must be raised. It should be done as soon as it becomes useful to do so!**
8. **Problem resolution**: Ideally, as soon as a solution has been found, it should be applied to resolve the problem; however, in reality safeguards might be needed to ensure that this does not cause further difficulties. If any change in functionality is required this will require an RFC to be raised and approved before the resolution can be applied.
9. **Problem Closure**: When any change has been completed (and successfully reviewed), and the resolution has been applied, the Problem Record should be formally closed—as should any related Incident Records that are still open. A check should be performed at this time to ensure that the record contains a full historical description of all events—and if not, the record should be updated. The status of any related Known Error Record should be updated to shown that the resolution has been applied.
10. **Major Problems/Major Problem Review:** Similar to major incidents, only your organization can determine what counts as a major problem and how exactly they should be handled. All major problems should be followed up with a major problem review. Be sure to examine the following:
    - Those things that were done correctly
    - Those things that were done wrong
    - What could be done better in the future
    - How to prevent recurrence
    - Whether there has been any third-party responsibility and whether follow-up actions are needed

Reactive and Proactive Problem Management[142]

Problem Management has both reactive and proactive subprocesses, though Problem Management is primarily a reactive process.

In **reaction** to incidents that appear similar and suggest a common root cause, Problem Management creates a problem record and investigates. Development of a workaround is critical to alleviate and address the incidents until the root cause is found and a solution is discovered.

Proactive Problem Management is initiated in Service Operation but generally driven as part of Continual Service Improvement. The objective of Proactive Problem Management is to identify problems that might otherwise be missed by analyzing incident records and utilizing data collected by other processes to identify suspicious trends. After a trend has been identified, a problem record is opened and moved through the Problem Management process.

Relationships with Other Processes[143]

Problems can be identified and corrected in many ways. One of the main benefits of Problem Management is the "many-to-one" relationship between incidents and problems. This enables an IT Service Provider to resolve many incidents in an efficient manner by correcting the underlying root-cause.

It is important to note that not all problems are diagnosed, often because the root cause is simply never found. In addition, there might be known errors that remain unresolved, possibly because the cost to permanently fix the known error are too high, or it is just deemed easier to "live with it."

Figure 5-4 illustrates several ways that Problem Management interfaces with other processes. In the first scenario, Incident Management spawns a problem. When the root cause of that problem is found, a Known Error record is opened. Problems are solved when a RFC is submitted to Change Management who manages and coordinates the activities as Release and Deployment Management implements the change.

Figure 5-4 Relationships Between Problem Management and Other Processes

The second scenario shows that not all known errors get fixed via a change; sometimes changes are too expensive, or too difficult to implement; other times, the priority just doesn't warrant the effort. In this case, no permanent solution will be implemented.

In the final scenario, Problem Management wasn't able to identify the root cause, so the problem remains a problem.

Problem Management Roles[144]

There should be a designated person (or, in larger organizations, a team) responsible for Problem Management. Smaller organizations might not be able to justify a full-time resource for this role, and it can be combined with other roles in such cases, but it is essential that it not just left to technical resources to perform. There needs to be a single point of coordination and an owner of the Problem Management process.

This role will coordinate all problem management activities and will have specific responsibility for:

- Liaison with all problem resolution groups to ensure swift resolution of problems within SLA targets
- Ownership and protection of the Known Error Database
- Gatekeeper for the inclusion of all known errors and management of search algorithms
- Formal closure of all problem records
- Liaison with suppliers, contractors etc., to ensure that third parties fulfill their contractual obligations, especially with regards to resolving problems and providing problem-related information and data
- Arranging, running, documenting and all follow-up activities relating to major problem reviews

In addition, the Problem Manager is the **process owner** of the Problem Management process.

As the process owner, this person is responsible for the following tasks (DEMI):

1. **D**ocumenting the Problem Management process.
2. **E**ducating process participants on how to use the Problem Management process correctly and ensuring that process participants are complying with the process.
3. **M**easuring the success of the process against KPIs, CSFs, and other targets set.
4. Continually **I**mproving the process. (This is done with input and assistance from the Continual Service Improvement Manager.)

Lesson 7: Access Management[145]

Access Management is the process of granting authorized users the right to use a service, while preventing access to non-authorized users. It is therefore the execution of policies and actions defined in Information Security Management and Availability Management.[146]

Always remember that Access Management is the process followed when the access control portion of the Information Security policy is being executed.

Access Management Key Terms[147]

Access Management is the process that enables users to use the services that are documented in the Service Catalogue. It is comprised of the following concepts:

- **Access**: Refers to the level and extent of a service's functionality or data that a user is entitled to use.
- **Identity**: Refers to the information about them that distinguishes them as an individual and which verifies their status within the organization. By definition, the identity of a user is unique to that user.
- **Rights**: (sometimes also called "privileges") Refer to the actual settings whereby a user is provided access to a service or group of services. Typical rights, or levels of access, include read, write, execute, change, delete.
- **Service Groups**: Most users do not use only one service, and users performing a similar set of activities will use a similar set of services. Instead of providing access to each service for each user separately, it is more efficient to be able to grant each user—or group of users—access to the whole set of services that they are entitled to use at the same time.
- **Directory Services**: Refers to a specific type of tool that is used to manage access and rights.

Access Management Roles[148]

Because Access Management is an execution of Information Security Management and Availability Management, these two areas will be responsible for defining the appropriate roles.

It is unusual for an organization to appoint an Access Manager, although it is important that there is a single Access Management process and a single set of policies related to managing rights and access. This process and the related policies are likely to be defined and maintained by Information Security Management and executed by the various Service Operation functions. Their activities can be summarized as follows:

- **The service desk** is typically used as a means to request access to a service, normally using a service request. The service desk validates the request and passes the request to the appropriate team to provide access.
- **Technical and Application Management** ensures that mechanisms are created to simplify and control Access Management on each service that is designed. They will also specify ways in which abuse of rights can be detected and stopped and are involved in dealing with incidents and problems related to Access Management.

Lesson 8: Sample Questions Based on Chapter 5

Answers can be found at the end of this chapter.

1. Which of the following should NOT be done when closing an incident?
    a. Check that the user is satisfied with the resolution.
    b. If a workaround is found, document it in the Known Error Database.
    c. Check for incident trends to see if the Problem Manager should raise a problem record.
    d. Double-check the incident categorization and correct it if it is incorrect; this ensures accurate incident metrics.
2. Which process or function is responsible for monitoring components and generating alerts when a threshold has been exceeded?
    a. Change Management
    b. Service Level Management
    c. Technical Management
    d. Event Management
3. Which ITIL process is responsible for taking calls from end users and restoring their service as quickly as possible?
    a. Incident Management
    b. Service Desk
    c. Request Fulfillment
    d. Problem Management
4. Which ITIL function is responsible for taking calls from end users and restoring their service as quickly as possible?
    a. Incident Management
    b. Service Desk
    c. Request Fulfillment
    d. Problem Management
5. For which of the following is the Technical Management function responsible?
    1. Day-to-day maintenance and administration of the technical infrastructure.
    2. Documenting and maintaining the technical skills required to manage and support the IT infrastructure.

3. Diagnosis of, and recovery from, technical failures.
4. Defining and negotiating the underpinning contracts for the technical teams and suppliers.

a. All of the above
b. 1, 2, and 4
c. 1, 2, and 3
d. 4 only

6. Which process has the activity of assigning users the appropriate access rights to a service?

a. Access Management
b. Information Security Management
c. Availability Management
d. Service Desk

7. Facilities Management is

a. The ITIL process that manages data centers and cabling requests
b. The ITIL process that provides assistance to IT Operations personnel on issues regarding third-party providers
c. The ITIL function that manages the physical IT environment (for example, the data center)
d. The ITIL function responsible for negotiating contracts with external suppliers regarding back-up facilities

8. Which of these is a valid service desk structure?

a. Help Desk
b. Regional service desk
c. Virtual service desk
d. Federated service desk

9. Functions are best described as

a. Teams lacking an operational run book
b. The combination of processes and roles
c. Self-contained units of organizations
d. A single task or activity that is part of a process

10. The most accurate definition of an event is

    a. The replacement or correction of a failed Configuration Item (CI).

    b. An occurrence where a performance threshold has been exceeded and an agreed service level has been impacted.

    c. An occurrence that is significant for the management of the IT infrastructure or delivery of services.

    d. The process responsible for identifying, assessing, and controlling risks.

11. Who is allowed to populate the Known Error Database?

    a. The Service Desk

    b. Technical Management and Application Management

    c. The Service Level Manager

    d. The Problem Manager

12. Which of the following statements are included in Availability Management?

    1. Verifying the identity of users requesting access to services.

    2. Setting the rights or privileges of systems to allow access to authorized users.

    3. Defining security policies for system access.

    4. Monitoring the availability of systems to which users should have access.

    a. 4 only

    b. 3 only

    c. 2 and 3 only

    d. 1 and 2 only

13. True or False? The Configuration Management Database (CMDB) maintains relationships between service components and any related incidents, problems, known errors, changes, and release documentation.

Answers to Sample Questions Based on Chapter 5

1. **B is correct.**

    a. Incorrect. This step should always be done when closing an incident.

    b. **Correct. This step should not be done when closing an incident. Only the Problem Manager can populate the KEDB, but only the service desk can close an incident.**

c. Incorrect. This step should always be done when closing an incident.

d. Incorrect. This step should always be done when closing an incident.

2. **D is correct.**

   a. Incorrect. Change Management would manage the change if any were ultimately associated with the alert, but it is not responsible for monitoring operational events.

   b. Incorrect. Service Level Management does not monitor components or generate alerts.

   c. Incorrect. Technical Management is a function that might define operational events, but Event Management (or IT Operations Control) would be the proper process/function respectively for monitoring operational events.

   d. **Correct. Event Management is the process responsible for monitoring components and generating alerts when a threshold has been exceeded.**

3. **A is correct.**

   a. **Correct. Incident Management is the *process* responsible for this objective.**

   b. Incorrect. The service desk is a *function*, even though it has similar goals and objectives as Incident Management.

   c. Incorrect. Request Fulfillment deals with service requests, which do not represent a failed service.

   d. Incorrect. Problem Management does not restore service as quickly as possible; it is a slow and methodical process.

4. **B is correct.**

   a. Incorrect. Incident Management is the *process* responsible for this objective; this question is looking for the function that performs this process.

   b. **Correct. The service desk is the *function* responsible for fulfilling this objective.**

   c. Incorrect. Request Fulfillment deals with service requests, which do not represent a failed service.

   d. Incorrect. Problem Management does not restore service as quickly as possible; it is a slow and methodical process.

5. **C is correct.**

   a. Incorrect. This option asserts that all the statements are true; however, point number four is the duty of the Service Level Manager.

   b. Incorrect. This option asserts that all the statements except number three are true. Point number three is a true statement; point number four is the duty of the Service Level Manager.

   c. **Correct. Statements one, two, and three are all duties of the Technical Management Function.**

   d. Incorrect. Service Level Management is responsible for defining UCs. SLM may get input from Technical Management, but this activity belongs to SLM.

6. **A is correct.**
    a. **Correct. Access Management is the process that assigns users the appropriate access to a service.**
    b. Incorrect. Information Security creates the Information Security Policy that Access Management uses when determining which groups should be allowed access, but Access Management assigns the access directly.
    c. Incorrect. Availability Management monitors the services and applications to which Access Management will provide access, but Availability Management does not grant that access.
    d. Incorrect. The service desk is a function, not a process.
7. **C is correct.**
    a. Incorrect. Facilities Management is a function, not a process.
    b. Incorrect. Facilities Management is a function, not a process.
    c. **Correct. Facilities Management is a function, which is part of the IT Operations Management function. It is responsible for managing the physical IT infrastructure, such as managing data centers, HVAC systems, backup power generators, cabling, and so on.**
    d. Incorrect. Facilities Management is a function, not a process. Also, Supplier Management and Service Level Management are the processes that would negotiate these types of contracts.
8. **C is correct.**
    a. Incorrect. This is not a valid service desk structure.
    b. Incorrect. This is not a valid service desk structure.
    c. **Correct. This is a valid type of service desk structure, along with Local Service Desk, Centralized Service Desk, and Follow the Sun.**
    d. Incorrect. This is not a valid service desk structure.
9. **C is correct.**
    a. Incorrect. Although functions are often teams who have their own body of knowledge, the ITIL books say nothing about "operational run books."
    b. Incorrect. A function is a self-contained unit of an organization; there are four functions in ITIL. Functions are not the combination of processes and roles.
    c. **Correct. Functions are self-contained units of organizations.**
    d. Incorrect. This option describes the term "activity," which is a step within a process.

10. **C is correct.**
    a. Incorrect. This may be defined as a change.
    b. Incorrect. This is an alert.
    c. **Correct. An event is simply something that is significant for the management of the IT infrastructure or delivery of services; it is significant enough that the event should be logged at the very least.**
    d. Incorrect. Although the statement is true (that is what a Risk Management process should do), it is not related to Event Management nor is it the definition of an event.
11. **D is correct.**
    a. Incorrect. Only the Problem Manager can populate the KEDB in order to keep its integrity.
    b. Incorrect. Only the Problem Manager can populate the KEDB in order to keep its integrity.
    c. Incorrect. Only the Problem Manager can populate the KEDB in order to keep its integrity.
    d. **Correct. Although anyone can look at the KEDB and suggest additions, modifications, or deletions, only the Problem Manager is allowed to populate the KEDB. This is done to keep the integrity of KEDB high.**
12. **A is correct.**
    a. **Correct. This is the only activity associated with Availability Management.**
    b. Incorrect. This is an activity of Information Security Management.
    c. Incorrect. Although Information Security Management, Access Management, and Availability Management are related, these activities do not overlap.
    d. Incorrect. These are activities of Access Management.
13. **False.** It is the Configuration Management System (CMS) that maintains these relationships.

Endnotes/Syllabus Requirements

109. This section satisfies Syllabus Requirement ITILFND02-02-8.

110. This section satisfies Syllabus Requirement ITILFND03-03-33.

111. This section satisfies Syllabus Requirements ITILFND06-06-1 and ITILFND06-06-2.

112. This section satisfies Syllabus Requirement ITILFND06-06-2.

113. This section satisfies Syllabus Requirement ITILFND06-06-2.

114. This section satisfies Syllabus Requirement ITILFND06-06-2.

115. This section satisfies Syllabus Requirement ITILFND06-06-2.

116. This section satisfies Syllabus Requirement ITILFND06-06-2.

117. This section satisfies Syllabus Requirement ITILFND06-06-1.

118. This section satisfies Syllabus Requirement ITILFND06-06-1.

119. This section satisfies Syllabus Requirement ITILFND06-06-1.

120. This section satisfies Syllabus Requirement ITILFND06-06-1.

121. This section satisfies Syllabus Requirement ITILFND06-06-1.

122. This section satisfies Syllabus Requirement ITILFND06-06-1.

123. This section satisfies Syllabus Requirements ITILFND03-03-24 and ITILFND05-05-81.

124. This section satisfies Syllabus Requirement ITILFND05-05-81.

125. This section satisfies Syllabus Requirement ITILFND03-03-25.

126. This section satisfies Syllabus Requirements ITILFND05-05-81 and ITILFND03-03-24.

127. This section satisfies Syllabus Requirements ITILFND05-05-71 and ITILFND03-03-26.

128. This section satisfies Syllabus Requirements ITILFND05-05-71 and ITILFND03-03-28.

129. This section satisfies Syllabus Requirements ITILFND05-05-71 and ITILFND03-03-27.

130. This section satisfies Syllabus Requirement ITILFND05-05-71.

131. This section satisfies Syllabus Requirement ITILFND05-05-71.

132. This section satisfies Syllabus Requirement ITILFND05-05-82.

133. This section satisfies Syllabus Requirements ITILFND03-03-29 and ITILFND05-05-72.

134. This section satisfies Syllabus Requirement ITILFND05-05-72.

135. This section satisfies Syllabus Requirement ITILFND05-05-72.

136. This section satisfies Syllabus Requirement ITILFND05-05-72.

137. This section satisfies Syllabus Requirement ITILFND03-03-29.

138. This section satisfies Syllabus Requirement ITILFND03-03-30.

139. This section satisfies Syllabus Requirement ITILFND03-03-31.

140. This section satisfies Syllabus Requirement ITILFND03-03-32.

141. This section satisfies Syllabus Requirement ITILFND05-05-72.

142. This section satisfies Syllabus Requirement ITILFND05-05-72.

143. This section satisfies Syllabus Requirement ITILFND05-05-72.

144. This section satisfies Syllabus Requirement ITILFND05-05-72.

145. This section satisfies Syllabus Requirement ITILFND05-05-83.

146. This section satisfies Syllabus Requirement ITILFND05-05-83.

147. This section satisfies Syllabus Requirement ITILFND05-05-83.

148. This section satisfies Syllabus Requirement ITILFND05-05-83.

Chapter 6

Continual Service Improvement

Lesson 1: Continual Service Improvement Overview

Continual Service Improvement (CSI) provides guidance on how to identify ways to improve process **p**rogress, **e**ffectiveness, **e**fficiency, and **c**ost-effectiveness (PEEC). It also provides guidance on improving services and the technology that supports those services.

In addition, CSI also helps us understand what to measure and why it is being measured.

CSI is the momentum that keeps the service lifecycle ball rolling. It forces us to go back to the drawing board when something needs to change. For example:

Pretend you are having a house built. In the Service Strategy phase, you are thinking big-picture thoughts, such as what kind of house you want, how many bedrooms you will need, if you would like a ranch or a home with different levels, and what town you'd like to live in. In the Service Design phase, you work with an architect who designs the house according to your specifications. Together, you work through where the bedrooms, kitchen, and bathrooms will go, and you will be sure not to ask for anything that you cannot afford. Any adjustments to the floorplan should be made here in the design phase, because adjustments are exponentially harder to make after the foundation is poured. Take your time in the Service Design phase to get the design exactly right. The architect's job is to create a blueprint; this blueprint is analogous to the Service Design Package, which is passed on to the home builder (Service Transition). The builder constructs the house according to the exact specifications in the blueprint. After the house has been built and the final walkthrough is complete, you can move your stuff in; this starts the Service Operation phase. Changes to the house are driven by the Continual Service Improvement phase, which forces you to go back to Service Strategy to think about what exactly you want to change about the house. The change will be designed in the Service Design phase, and then the change will be implemented through Service Transition. You enjoy the fruits of the change in the Service Operation phase… until you decide to change something else. The lifecycle ball continually rolls because as every homeowner (and customer) knows: There will always be something that needs to be tweaked.

CSI Objectives

The objectives of CSI are as follows:[149]

- Review, analyze, and make recommendations on improvement opportunities in each lifecycle phase:

  Service Strategy, Service Design, Service Transition, and Service Operation.

- Review and analyze Service Level Achievement results.
- Identify and implement individual activities to improve IT service quality and improve the efficiency and effectiveness of enabling IT Service Management (ITSM) processes.
- Improve cost effectiveness of delivering IT services without sacrificing customer satisfaction.
- Ensure applicable quality management methods are used to support continual improvement activities.

The primary purpose of CSI is to continually align and re-align IT services to the changing business needs by identifying and implementing improvements to IT services that support business processes.

CSI Activities[150]

To implement CSI successfully, it is important to understand the different activities that can be applied to CSI. The following activities support a continual process improvement plan:

- Reviewing management information and trends to ensure that services are meeting agreed service levels
- Reviewing management information and trends to ensure that the output of the enabling ITSM processes are achieving the desired results
- Periodically conducting maturity assessments against the process activities and roles associated with the process activities to demonstrate areas of improvement or, conversely, areas of concern
- Periodically conducting internal audits verifying employee and process compliance
- Reviewing existing deliverables for relevance
- Making ad-hoc recommendations for approval
- Conducting periodic customer satisfaction surveys
- Conducting external and internal service reviews to identify CSI opportunities

These CSI activities do not happen automatically and without guidance; they must be owned and driven from within the IT organization. They must also be planned and scheduled on an ongoing basis.

It is essential to develop an ongoing continual improvement strategy for each of the processes as well as the services.

Because any improvement initiative will more than likely necessitate changes, specific improvements will need to follow the defined ITIL Change Management process.

CSI Key Terms

Some of the key CSI terms are as follows:

- **Key Performance Indicator (KPI):**[151] A metric that is used to help manage a Process, IT Service, or Activity. Many metrics can 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. [...] KPIs can be either qualitative or quantitative.

  KPIs are defined by each process owner for the process(es) for which they are responsible. The process owner is also responsible for measuring against these KPIs and using those reports to continually improve their processes.[152]

- **Critical Success Factor (CSF)**: 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.

- **Baseline:** This is the first measurement of a particular service, process, or aspect of the IT infrastructure. Baselines are used both as a starting point and for later comparison.[153]

Lesson 2: CSI Approaches: Deming Cycle, CSI Model, and the Seven-Step Improvement Process

In Continual Service Improvement, several **approaches** and **processes** are identified to support the improvement of services and processes:

- *The Deming Cycle* (commonly known as Plan-Do-Check-Act, after the four steps in the cycle) is a basis for slow, steady quality management and improvement.
- *The Continual Service Improvement Model* is a high-level approach for improving IT Service Management.
- *The Seven-Step Improvement Process* is an approach that assists in carefully measuring all aspects of a service and taking corrective action. It loosely mimics the DIKW Model.

The Deming Cycle[154]

The Deming Cycle can lead organizations to steady, ongoing improvement.

Dr. W. Edwards Deming is best known for his management philosophy leading to higher-quality, increased productivity, and a more competitive position. He recommended that business processes be placed in a continuous feedback loop so that managers could identify and change the parts of the process that need improvements. Deming created a diagram to illustrate this continuous process, commonly known as the PDCA cycle (for Plan, Do, Check, Act), as illustrated in Figure 6.1.

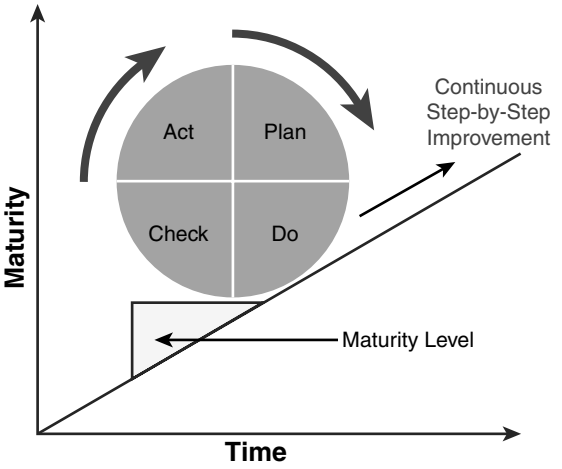

Figure 6-1 PDCA Cycle

- **Plan:** Design or revise business process components to improve results.
- **Do:** Implement the plan and measure its performance.
- **Check:** Assess the measurements (for example, a gap analysis) and report the results to decision makers.
- **Act:** Decide on changes needed to improve the process.

Remember

The four steps of the Deming Cycle are in reverse alphabetical order: P, D, C, A.

The Continual Service Improvement Model (The CSI Model)[155]

Figure 6-2 illustrates a constant cycle for improvement called the Continual Service Improvement Model, the six basic steps for which are as follows:

1. **What is the vision?** Embrace the vision by understanding the high-level business objectives. The vision should align with the objectives.
2. **Where are we now?** Assess the current situation to obtain an accurate, unbiased snapshot of where the organization is right now. This will serve as a baseline.[156]
3. **Where do we want to be?** Understand and agree on the priorities for improvement based on a deeper development of the principles defined in the vision. The full vision may be years away but this step provides specific goals and a manageable timeframe.

4. **How do we get there?** Detail the CSI plan to achieve a higher quality service provision by implementing ITSM processes.
5. **Did we get there?** Verify the measurements and metrics are in place to ensure that milestones were achieved, process compliance is high, and business objectives and priorities were met by the level of service.
6. **How do we keep the momentum going?** Finally, the process should ensure that the momentum for quality improvement is maintained by ensuring that changes become embedded in the organization.

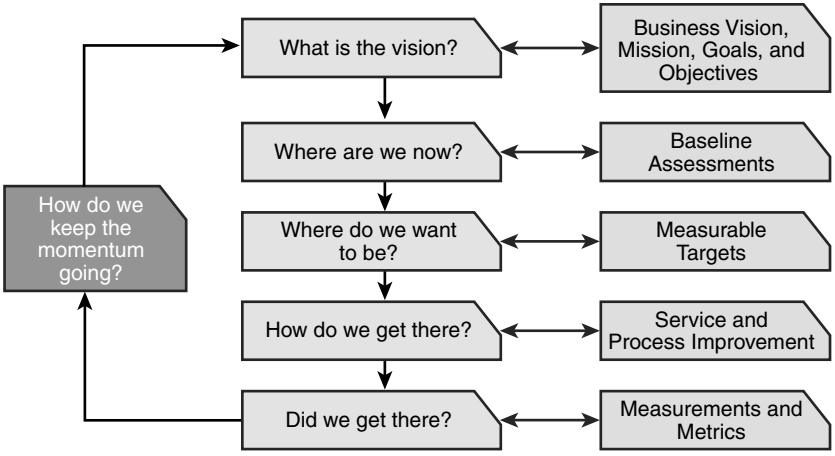

Figure 6-2 CSI Model

The Seven-Step Improvement Process[157]

The concept of measurement is fundamental to CSI. CSI uses the Seven-Step Improvement Process depicted in Figure 6-3 and described in the list that follows:

1. **Define what you should measure:** Service Strategy and Service Design should have identified this information at the onset of the service lifecycle.
2. **Define what you can measure:** Often, this will be different from what you would ideally like to measure from Step 1. Take your time determining this step.
3. **Gather the data:** Data must first be gathered (typically through Service Operation) before we can process the data. Take steps to ensure the integrity of the data.
4. **Process the data:** Here the data is processed in alignment with the Critical Success Factors and the Key Performance Indicators specified. You determine how often you need to process the data, in what system it will be stored, and how you can ensure the accuracy of the data.

5. **Analyze the data:** Here the *data becomes information* as you discover trends, identify service gaps, and consider taking corrective action.
6. **Present the information:** Here you can answer "Did we meet our goal? What fell short?"
7. **Implement Corrective Action:** You finally have the *knowledge* to guide the direction of your business and to make informed decisions.

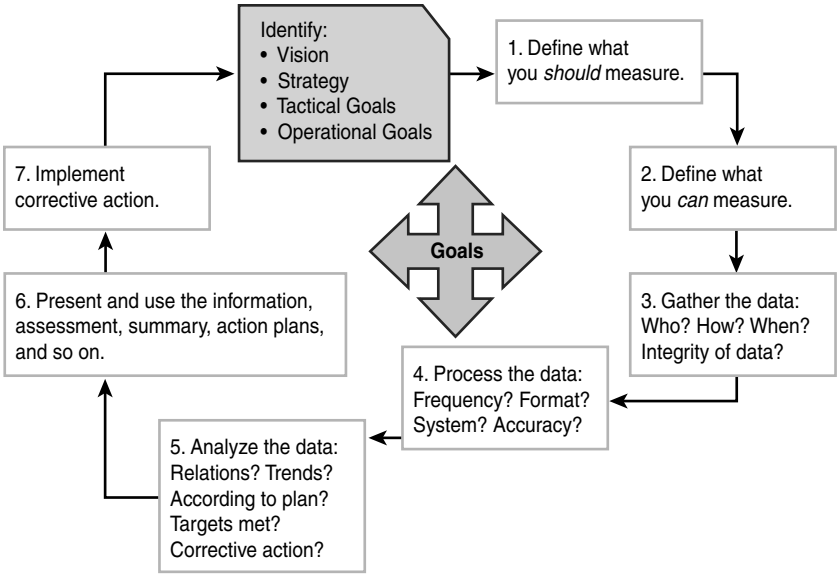

Figure 6-3 The Seven-Step Improvement Process

Lesson 3: CSI Metrics and Measurement

How Do I Measure?

As you design a service's measurement methods and metrics during the Service Design phase of the lifecycle, Key Performance Indicators (KPIs) and Critical Success Factors (CSFs) are defined and agreed upon. KPIs should support and be tied to CSFs.[158]

You should measure constantly, and analyze performance reports consistently for your own use. As already outlined in the Service Level Management lesson in Chapter 3, "Service Design," you should compile and present these reports to the customer as often as stated in the SLA.

What Do I Measure?[159]

It is important to remember that there are three types of metrics that an organization will need to collect to support CSI activities as well as other process activities.

The types of metrics are as follows:

- **Technology metrics**: These metrics are often associated with component and application based metrics such as performance, availability, etc.
- **Process metrics**: These metrics are captured in the form of CSFs, KPIs and activity metrics for the Service Management processes. These metrics can help determine the overall health of a process. Four key questions that KPIs can help answer are around quality, performance, value and compliance of following the process. CSI would use these metrics as input in identifying improvement opportunities for each process.
- **Service metrics**: These metrics are the results of the end-to-end service. Component metrics are used to compute the Service metrics.

Why Do I Measure?[160]

There are four reasons to measure:

- **To validate**: Monitoring and measuring to validate previous decisions
- **To direct**: Monitoring and measuring to set direction for activities in order to meet set targets. It is the most prevalent reason for monitoring and measuring
- **To justify**: Monitoring and measuring to justify, with factual evidence or proof, that a course of action is required
- **To intervene**: Monitoring and measuring to identify a point of intervention including subsequent changes and corrective actions

The four basic reasons to monitor and measure gives you permission then to ultimately ask three important questions:

- "Why are we monitoring and measuring?"
- "When do we stop?"
- "Is anyone using the data?"

To answer these questions, it is important to identify which of the above reasons is driving the measurement effort. Too often, we continue to measure long after the need has passed. Every time you produce a report you should ask, "Do we still need this? Is anyone actually using this data?"

Lesson 4: CSI Interfaces and Roles

CSI Interfaces[161]

You already know that each lifecycle phase provides an output to the next phase of the lifecycle. This same concept applies to CSI. To be effective, CSI requires open and honest feedback from IT

staff. Debriefings or activity reviews work well for capturing information about lessons learned such as, "Did we meet the timelines?" and, "Did we provide quality?" Figure 6-4 illustrates how communication and feedback flows between lifecycle phases. The thick downward arrows show the logical flow starting with Service Strategy flowing into Service Design, which moves into Service Transition, which leads into Service Operation. You can also see that CSI touches every lifecycle phase by the thick upward-pointing arrows. The thin arrows on the right side of the diagram show that any lifecycle phase can provide lessons and feedback to any other phase of the lifecycle if it's helpful to do so. CSI helps lubricate those communication channels.

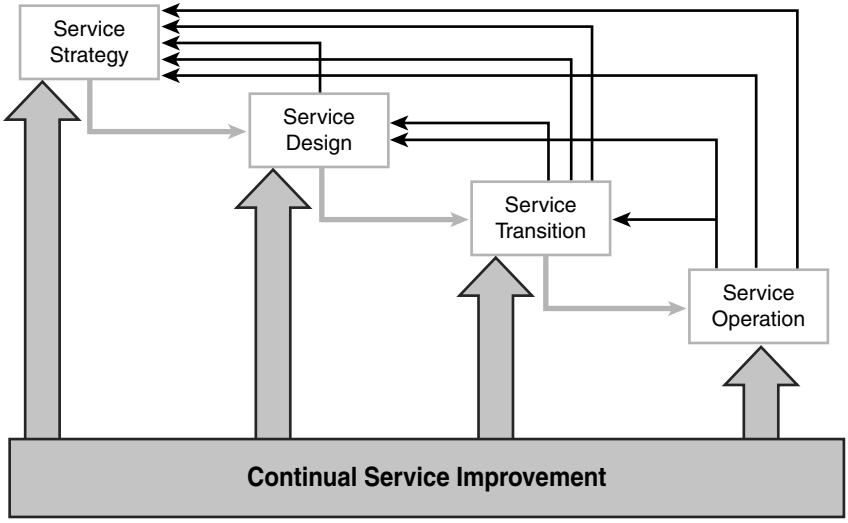

Figure 6-4 CSI and the Service Lifecycle

CSI Interface with SLM[162]

Both Service Level Management and CSI have monitoring and reporting as a primary activity. In fact, CSI assists SLM in the compilation and creation of customer reports. However, the Service Level Manager is the only role who physically presents these reports to the customer, as SLM is the sole customer interface.

Although both CSI and SLM are concerned with improving service quality, there is one key difference—CSI is constantly occurring, even when metrics show that IT is performing well. But improvement initiatives championed by SLM (called Service Improvement Plans, or SIPs) are only implemented when services are not meeting our targets in the Service Level Agreements. SIPs are temporary; CSI is always happening.

CSI Roles[163]

Process owners are *accountable* for the process they own. They are responsible for documenting the process, educating staff members on proper use of the process and ensuring the process is being followed correctly, measuring the process results against KPIs, and *continually improving the process* in terms of its progress, effectiveness, efficiency, and cost (PEEC).

Service owners are *accountable* for a specific service. Their role ensures a service is managed with a business focus, and therefore this role is often filled by an IT Executive. The service owner, in conjunction with the Continual Service Improvement Manager, is responsible for the continual improvement of that service.

Remember

Owners are responsible for continually improving whatever they own. **Process** owners are responsible for continually improving the **processes** they own; **service** owners are responsible for continually improving the **services** they own.

The principle of ownership is fundamental to any improvement strategy. CSI is a best practice and one of the keys to successful implementation is to ensure that a specific manager, **a CSI manager**, is responsible for ensuring the best practice is adopted and sustained throughout the organization. The CSI manager becomes the CSI owner and chief advocate. The CSI owner is accountable for the success of Continual Service Improvement in the organization. This ownership responsibility extends beyond ensuring the CSI practices are embedded in the organization but also to ensuring there are adequate resources (including people and technology) to support and enable CSI. Also included are ongoing CSI activities such as monitoring, analyzing, evaluating trends and reporting as well as project-based service improvement activities—activities that are fundamental to the ITIL framework. Without clear and unambiguous accountability there will be no improvement.

The CSI Manager role is:

- Accountable for the success of all improvement activities
- Communicates the CSI vision across the IT organization
- Defines and reports on CSI Critical Success Factors, Key Performance Indicators and CSI activity metrics
- Coordinates CSI throughout the service lifecycle
- Builds effective relationships with the business and IT managers
- Ensures monitoring is in place to gather data
- Works with *process owners* and *service owners* to identify improvements and improve quality

Lesson 5: Sample Questions Based on Chapter 6

Answers can be found at the end of this chapter.

1. Consider the following statements:

    1. What cannot be measured cannot be managed.
    2. CSI provides guidance on how to improve process efficiency, effectiveness, progress, and cost.
    3. CSI provides guidance on how to improve end-to-end services.
    4. CSI provides guidance on the improvement of how technology is managed.

    Which of the preceding statements is correct?

    a. 1 and 2 only
    b. 2 only
    c. 1, 2, and 3 only
    d. All of the above

2. Which of the following is not a step in the Continual Service Improvement (CSI) model?

    a. Did we get there?
    b. What is the vision?
    c. Do we have the proper personnel?
    d. Where are we now?

3. What are the four basic reasons to monitor and measure?

    a. To Validate, Direct, Justify, and Intervene
    b. People, Products, Processes, and Partners
    c. Define, Analyze, Approve, and Charter
    d. Plan, Do, Check, and Act

4. What do Technology Metrics measure?

    a. The progress, efficiency, effectiveness, and cost of a process
    b. The uptime of systems and their constituent components
    c. The end-to-end service
    d. Resources and capabilities

5. Put the steps of the Deming Cycle in order.
    a. Plan, Check, Do, Act
    b. Plan, Act, Do, Check
    c. Plan, Do, Check, Act
    d. Act, Check, Do, Plan
6. In the Continual Service Improvement (CSI) Model, which activities are performed during the "How do we get there?" stage?
    a. Embrace the vision by understanding the high-level business objectives
    b. Verify the measurements and metrics are in place to ensure that milestones were achieved
    c. Implement service and process improvements
    d. Take a snapshot to capture your baseline

Answers to Sample Questions Based on Chapter 6

1. **D is correct.**
    a. Incorrect. All the options are true statements, including 3 and 4.
    b. Incorrect. All the options are true statements, including 1, 3, and 4.
    c. Incorrect. All the options are true statements, including number 4.
    d. **Correct. All the options are true statements.**
2. **C is correct.**
    a. Incorrect. This is step five of the CSI model.
    b. Incorrect. This is step one of the CSI model.
    c. **Correct. This is not a step of the CSI model.**
    d. Incorrect. This is step two of the CSI model.

3. **A is correct.**
    a. **Correct. You measure to validate your vision and strategy, to direct your future activities, to justify your actions with facts and numbers, and to identify points where intervention is needed so you can fix trouble spots.**
    b. Incorrect. These are the four Ps to be considered to ensure a balanced Service Design.
    c. Incorrect. These are the four steps of Service Portfolio Management.
    d. Incorrect. These are the four steps to the Deming Cycle.
4. **B is correct.**
    a. Incorrect. These are process metrics.
    b. **Correct. This describes technology metrics.**
    c. Incorrect. This describes service metrics.
    d. Incorrect. This is the distracter answer.
5. **C is correct.**
    a. Incorrect. This option has the middle two steps backwards. The steps are Plan, Do, Check, Act.
    b. Incorrect. This option has the final three steps mixed up. The steps are Plan, Do, Check, Act.
    c. **Correct. An easy way to remember the steps to the Deming Cycle is that they are in reverse alphabetical order.**
    d. Incorrect. This has the steps in reverse order. The steps are Plan, Do, Check, Act.
6. **C is correct.**
    a. Incorrect. This step describes the "What is the vision?" stage.
    b. Incorrect. This step describes the "Did we get there?" stage.
    c. **Correct. This step describes the "How do we get there?" stage.**
    d. Incorrect. This describes the "Where are we now?" stage.

Endnotes/Syllabus Requirements

149. This section satisfies Syllabus Requirement ITILFND02-02-10.

150. This section satisfies Syllabus Requirement ITILFND02-02-10.

151. This section satisfies Syllabus Requirement ITILFND04-04-10.

152. This section satisfies Syllabus Requirement ITILFND04-04-10.

153. This section satisfies Syllabus Requirement ITILFND04-04-10.

154. This section satisfies Syllabus Requirements ITILFND02-02-10 and ITILFND04-04-08.

155. This section satisfies Syllabus Requirement ITILFND04-04-09.

156. This section satisfies Syllabus Requirement ITILFND04-04-10.

157. This section satisfies Syllabus Requirement ITILFND02-02-10.

158. This section satisfies Syllabus Requirement ITILFND04-04-10.

159. This section satisfies Syllabus Requirement ITILFND04-04-10.

160. This section satisfies Syllabus Requirement ITILFND04-04-10.

161. This section satisfies Syllabus Requirement ITILFND02-02-10.

162. This section satisfies Syllabus Requirement ITILFND02-02-10.

163. This section satisfies Syllabus Requirement ITILFND02-02-10.

.

.