Chapter 1

Overview of Operations Management

System Center 2012 Configuration Manager, like the previous versions of the product, plays a very important role in operations management in the information technology (IT) world. As IT professionals, we are not responsible for every task required to accomplish a key business activity in our environments. However, we are an important piece of the IT systems management process. This is one of the many reasons Microsoft created the Microsoft Operations Framework (MOF), which is based on the IT Infrastructure Library (ITIL).

The idea behind MOF and ITIL is to create a complete team structure with the ultimate goal of service excellence. Numerous groups fall under the IT department tag, but we often see many of them acting as separate departments rather than as one cohesive unit. Desktop support, application developers, server support, storage administrators, and so forth are all members of IT, but they are not always as unified as they should be.

System Center 2012 Configuration Manager was built with MOF and ITIL in mind, so we will start the book by describing these two systems and how they are the basis for the System Center family of products. System Center Configuration Manager, or ConfigMgr, is much more than just a mechanism to deploy software. In this chapter, you will learn how we define IT service management, how ITIL is the foundation, and how MOF expands ITIL, but you will also learn about all of the Microsoft System Center products and new features of the ConfigMgr 2012.

Defining Operations Management

There is often some confusion when it comes to the actual definition of operations management. Microsoft’s System Center family of products comprises several products that span a wide range of “management” aspects. The most confusing overlap of this area is between systems management and operations management. This section looks at the differences between the two.

Systems Management

Systems management is typically defined as using software to centrally manage large groups of computer systems. This software contains the tools to control and measure the configuration of both hardware and software in the environment.

Microsoft’s solution in this arena is a product called System Center 2012 Configuration Manager. Configuration Manager provides remote tools, software update management (otherwise known as patch management), software distribution, hardware and software inventory, software metering, settings management, operating system deployment, and much more. With each capability of Configuration Manager you take advantage of, you can reduce the total administrative effort required to maintain the systems within your environment, thus lowering the total cost of ownership (TCO) of the resources that are being fully managed.
Operations Management

Now that you have an understanding of what falls under the category of systems management, we can explore operations management. Operations management is mainly focused on ensuring that business operations are efficient and effective through processes that are aimed at improving the reliability and availability of IT systems and services. You accomplish this by gathering information from your current systems, having the proper people in place to decipher that data, and having proper procedures in place to carry out any tasks that may arise if there is a current or potential problem in your environment.

The System Center solution that addresses this need is System Center Operations Manager. Operations Manager provides you with the information you need (i.e., performance, security, scalability, knowledge, and so on) to help reduce time and effort in managing your IT infrastructure by automating service tasks and giving you a proactive approach to determining possible problems.

Understanding IT Service Management

The IT Infrastructure Library and the Microsoft Operations Framework were introduced as a way to deliver consistent IT service management (ITSM). Some of the key objectives of ITSM are as follows:

◆ To align IT services with current and future needs of the business and its customers
◆ To improve the quality of IT services delivered
◆ To reduce the long-term cost of service provisioning

Think of ITSM as a conduit between the business and the technology that helps run the business. Without a proper conduit in place, one cannot function properly without the other. ITSM is about process, not about software products.

Exploring the IT Infrastructure Library

Before we dig into the inner workings of ITIL Version 2, it is important for the ITIL beginner to understand that ITIL, and its counterpart Microsoft Operations Framework Version 4, are not based on technology. Both ITIL and MOF are based on IT processes. This is an important distinction. Readers interested in IT processes and procedures, as well as how the Microsoft System Center family of products fits into these processes, should find the rest of this chapter very interesting.

If you start researching ITIL, you will find that it is a series of books that describe an approach to IT service management. Originally created in the United Kingdom to address strict operations management standards, ITIL has become the accepted standard in IT service management. The library is owned by the UK government’s Office of Government Commerce (OGC). If you really want to get cozy with ITIL, be prepared to spend a lot of time reading. In its original form, the ITIL volumes were at a count of 60 books. These books were created by industry leaders of the time and described best practices for IT processes.

There is much more to ITIL than just the books, however. ITIL as a whole includes the books, certification, ITIL consultants and services, and ITIL-based training and user groups. ITIL is mainly updated by its own user group, known as the IT Service Management Forum (itSMF). The last piece of the puzzle, ITIL certification, is administered by the Netherlands Examination Institute for IT (EXIN) and the Information Systems Examination Board (ISEB).
ITIL can be divided into two categories: service support and service delivery. The two categories include numerous processes.

**Service Support**  Service support is described as the practice of disciplines that enable IT services to be provided. Without those disciplines, which we’ll outline shortly, any attempt to provide IT services would potentially be unmanaged and possibly chaotic.

**Service Delivery**  Service delivery is described as the management of the IT services themselves, and it involves a number of practices to ensure IT services are provided between the provider and the customer.

Underlying this division is the difference between what is considered a *user* of the system and what is considered a *customer* of the system.

Now you may be thinking, “I run an internal network. Everyone on my network is a user; we don’t have any customers who connect into the network.” In all actuality, every administrator (admin) has both users and customers on their network, and often the same individual can be both a user and a customer. For example, HallieM is a *user* of the network when she interacts with the service desk. HallieM is also a *customer* of the network when she obtains certain services from another department, such as services that she must pay for or services that have Availability Management in place, as would be the case with email and database services.

Table 1.1 shows the breakdown of the differences between service support and service delivery.

<table>
<thead>
<tr>
<th><strong>TABLE 1.1</strong>: ITIL service support and service delivery differences</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>CATEGORY</strong></td>
</tr>
<tr>
<td>Service support</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td>Service delivery</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
</tbody>
</table>
CHAPTER 1 OVERVIEW OF OPERATIONS MANAGEMENT

SERVICE DESK
We will first look at the service desk, because it is unique among the items in Table 1.1. The service desk is a function, unlike the other items listed, which are processes. All incident reporting and service requests are routed through the service desk. It is the function that ties the service providers with the users, keeping users informed of service events and actions that may impact their day-to-day activities. The service desk becomes a single point of contact for customers and users to interact with the IT department. This approach helps expedite the call process by managing it in a timely and satisfactory way.

INCIDENT MANAGEMENT
Incident management is the mechanism by which the service desk records, updates, and tracks the enterprise “fires.” The incident-management process is mainly concerned with restoring normal service operations as soon as possible. This will help minimize any adverse effects on business operations and will ensure high levels of service quality and availability. Service-level agreements (SLAs) will determine what a “normal” service operation is. Information is collected about the incident to allow changes or enhancements in the environment to prevent future incidents. This information can also be used to compare against SLA compliance metrics and service quality information.

PROBLEM MANAGEMENT
The problem-management process is mainly concerned with minimizing the impact of incidents and problems. The goal is to reduce incident resolution times by providing insights for known errors and removing the underlying causes. This strategy improves IT service quality by helping the service desk resolve incidents at the time of logging. If an incident can be resolved at the time of logging, business impact is reduced, business efficiency is improved, and IT efficiency is improved.

The problem-management process should not be considered a reactive-only approach, however. When dealing with incident management, problem control, or error control, it is very reactive. However, the problem-management process can be viewed as proactive when you consider how it is used for problem prevention.

Problem investigation and diagnosis are used when known errors are created. During this investigation and diagnosis period, insightful details of the known errors are captured and communicated until a fix for the problem is found. This approach helps with the staffing of the incident-management process, thus ensuring there aren’t too many IT staff members duplicating work while trying to fix the same issue.

CONFIGURATION MANAGEMENT
The configuration-management process is responsible for keeping an accurate and up-to-date model of the entire IT infrastructure. It uses this information to help support a number of areas by doing the following:

◆ Allowing for assessment of change or problem-management functions
◆ Allowing financial information to be gathered to help determine lease, rental, maintenance, and support costs for IT infrastructure components
◆ Supplying information about component performance and reliability to support capacity and availability management
◆ Improving security by identifying the location and details of assets, making it difficult for unauthorized changes to be carried out undetected
◆ Helping with legal obligations by identifying the location of unauthorized software, determined by enabling authenticity checks on software and making sure current, correct versions of the software are being used

Configuration management uses this information to identify relationships between items that are going to be changed and any other components of the infrastructure that an item is tied to. Such a strategy enables the owners of the other components to be notified and involved in the impact-assessment process.

CHANGE MANAGEMENT
The change-management process is used to ensure that standard methods are used when implementing change and for developing and documenting reusable processes. Implementing a change-management system can reduce the possibility that a change in the environment could cause a failure, thus resulting in an incident.

The IT infrastructure is constantly changing. Patches, service packs, updates, firmware, drivers, and so forth are released on an almost daily basis. Having a safe and repeatable process in place is vital to service management.

RELEASE MANAGEMENT
Changes in the environment often result in the need for new iterations of software, hardware, documentation, and so forth. The release-management process works closely with change management and configuration management to produce a secure and managed rollout of the new item. Consequently, physical changes to the environment are taken into account and the transition to live operation is successful—including both hardware and software releases.

The quality of a new software release is identified through this process, along with tests to determine whether patches and updates are going to affect already approved software. In this way, the process guarantees that only the authorized versions of software releases are being installed.

SERVICE LEVEL MANAGEMENT
The service-level management (SLM) process is responsible for creating service-level agreements and ensuring that operation-level agreements (OLAs) are met at all times. During this process, changes to the environment are assessed to determine the effect on SLAs.

SLAs play an important role in SLM. They help set expectations for IT by determining what the customer’s service-level requirements are, and they help customers by having a measurable understanding of what good service is. Both sides can agree on timelines for deliverables for everything from service upgrades to updates to incident resolution. SLAs also provide a clear understanding of what value customers are receiving from IT and can be used as a basis for charging for IT services. This brings us to the Financial Management process.
**Financial Management**

The Financial Management process is responsible for determining the costs of IT services as well as calculating the return on IT service investments. It is also a key role in recovering costs from customers if you charge for your services. As mentioned earlier, having SLAs in place to manage expectations is very important.

Budgeting can become much more accurate as well because Financial Management is responsible for tracking costs of IT assets and resources. Financial management allows you to break down the money spent on IT services so you can clearly view where IT budget money went. Because budgeting is a more accurate and a much more precise data point, it helps support future business decisions on IT investments.

If you are considering charging for IT services, a fair recovery system is determined by data gathered through the financial-management process. Charging for internal services has its advantages and disadvantages. One advantage to charging for IT services is that it helps customers and users see the value of IT. Customers and users may also behave differently if they are faced with a charge model. Such a model helps the customers decide whether the services they are receiving are cost justified. Using a model could lower the demands on the IT department.

One of the disadvantages of charging for services is that the customer has the ability to take business or services elsewhere, which could have a severe effect on budgeting. Also, charge systems are often expensive, and the cost of such a model could offset the money that is generated by the system.

**Capacity Management**

The capacity-management process involves determining the required service delivery, the current service delivery, and the IT infrastructure and ensuring that all current and future capacity and performance requirements from the business are met. Capacity management also needs to take into account changes in new technology and the improvement in performance that new technology brings to the table. Basically, this process is responsible for identifying the current service delivery as well as the service delivery potential at any given time.

Capacity management is responsible for making sure business requirements for system capacity are met at all times. Again, this does not directly relate to a technical capacity. It is related to the business requirements for the system, not necessarily the performance of the system.

**IT Service Continuity Management**

The IT service continuity management process ensures that an organization can continue to function with predetermined and agreed-on levels of IT services to support the minimum business requirements following an interruption to the business. The idea behind this process is that the organization will always have a base level of required IT services.

Each IT service is examined to determine the minimum level it can function at to meet the business requirements. A plan is then put in place to guarantee that this level of service can be reached at all times under any circumstances.

**Availability Management**

The availability management process deals with the design, implementation, and management of IT services to guarantee that certain business requirements for availability are obtained. This requires information from both incident management and problem management to determine
why an IT service failed and the time it took to resume service. This process can help IT departments meet SLAs that define availability levels. These SLAs cannot be met without a thorough understanding of the availability and reliability of IT components.

Availability management is a high-profile process. Take an accounting server offline during a month-end run and see what kind of attention it gets. Because of this high-profile status, it is beneficial to have a single process owner for all availability issues to ensure that consistent and comprehensive measures are taken for managing and improving availability to IT systems.

Exploring the Microsoft Operations Framework

As stated earlier, the Microsoft Operations Framework is the basis of System Center 2012 Configuration Manager. The MOF was developed by Microsoft and a group of partners to expand on the best practices developed by ITIL. MOF includes a plethora of resources that are available to help you achieve mission-critical system reliability, manageability, supportability, and availability with Microsoft products and technologies. These resources are in the form of white papers, operation guides, assessment tools, best practices, case studies, templates, support tools, courseware, and services. All of these resources are available on the official MOF website at www.microsoft.com/mof.

How MOF Expands ITIL

While ITIL is based on IT operations as a whole, MOF has taken the route of providing a service solution as its core. MOF focuses on the release and life cycle of a service solution, such as an application or infrastructure deployment.

Because ITIL was based on a philosophy of “adopt and adapt,” Microsoft leveraged that strategic fundamental basis for the MOF. Although Microsoft supports ITIL from a process perspective, Microsoft decided to make a few changes and add a few things when it built MOF. One of these changes and additions includes moving to a “prescriptive” Process Model. Microsoft defines the ITIL Process Model as “descriptive.” It has more of a “why” approach, whereas MOF has more of a “prescriptive,” or “how,” approach.

MOF also introduced the concept of service management functions (SMFs). As Table 1.2 illustrates, there are now 21 SMFs that describe the series of management functions performed in an IT environment. All of these SMFs map to an ITIL-based best practice for performing each function. Notice that the SMFs are grouped into quadrants, a concept we explain shortly in the section “The Microsoft Operations Framework Process Model.”

<table>
<thead>
<tr>
<th>QUADRANT</th>
<th>SMF</th>
</tr>
</thead>
<tbody>
<tr>
<td>Optimizing</td>
<td>Service-Level Management</td>
</tr>
<tr>
<td></td>
<td>Financial Management</td>
</tr>
<tr>
<td></td>
<td>IT Service Continuity Management</td>
</tr>
<tr>
<td></td>
<td>Availability Management</td>
</tr>
</tbody>
</table>
MOF also extended many of the existing processes in ITIL and created new processes. These will be discussed later in the chapter.

MOF also introduced the Team Model. This gives the MOF two core models: the Team and Process Models. The Team Model was added to fill a gap in ITIL, which identifies roles for the process owner of each operation process, whereas MOF creates seven distinct role clusters that describe the functional role or team:

**Service** Primary responsibility is to make sure all IT services are at a satisfactory level to customers and users. This is done by creating SLAs and ensuring that they are being met on a regular basis.

<table>
<thead>
<tr>
<th>QUADRANT</th>
<th>SMF</th>
</tr>
</thead>
<tbody>
<tr>
<td>Optimizing</td>
<td>Capacity Management</td>
</tr>
<tr>
<td></td>
<td>Workforce Management</td>
</tr>
<tr>
<td></td>
<td>Infrastructure Engineering</td>
</tr>
<tr>
<td></td>
<td>Security Management</td>
</tr>
<tr>
<td>Changing</td>
<td>Change Management</td>
</tr>
<tr>
<td></td>
<td>Configuration Management</td>
</tr>
<tr>
<td></td>
<td>Release Management</td>
</tr>
<tr>
<td>Operating</td>
<td>System Administration</td>
</tr>
<tr>
<td></td>
<td>Security Administration</td>
</tr>
<tr>
<td></td>
<td>Service Monitoring and Control</td>
</tr>
<tr>
<td></td>
<td>Job Scheduling</td>
</tr>
<tr>
<td></td>
<td>Network Administration</td>
</tr>
<tr>
<td></td>
<td>Directory Services Administration</td>
</tr>
<tr>
<td></td>
<td>Storage Management</td>
</tr>
<tr>
<td>Supporting</td>
<td>Service Desk</td>
</tr>
<tr>
<td></td>
<td>Incident Management</td>
</tr>
<tr>
<td></td>
<td>Problem Management</td>
</tr>
</tbody>
</table>
Infrastructure  Responsible for ensuring that plans are in place to keep networking, telecommunications, hardware, and software running in order to satisfy business requirements.

Support  Maps to the Service Desk, Incident Management, and Problem Management functions in ITIL.

Operations  Responsible for making sure that the day-to-day tasks of running the IT systems are met, according to SLAs.

Partner  This is more of a “virtual” team in the IT department, usually made up of outsource vendors, IT partners, resellers, service providers, consultants, and so forth.

Security  Responsible for data confidentiality, data integrity, and data availability.

Release  Transitions a release between a development or test environment into production. A release could be a new software package, an update, a patch, and so forth. The release role also has the responsibility of maintaining accurate inventory management and asset management.

The risk-management discipline was added to recognize that the management of risk is its own discipline. ITIL only provides discussion about the handling of risk for each IT operations process.

Explicit management review checkpoints are also built into MOF to guarantee that there is involvement by management at each key step in the process. The ITIL books do not include these checkpoints. This is another added value that Microsoft provides with MOF.

THE MICROSOFT OPERATIONS FRAMEWORK PROCESS MODEL

The MOF Process Model breaks down a complex environment into an easy-to-manage and easy-to-understand set of functions, thanks to the numerous SMFs that Microsoft added when they created the MOF. SMFs are just a portion of the overall release cycle that MOF employs.

Microsoft defines a release as any change, or set of changes, that is incorporated into a managed environment. A release includes not only changes in applications or operating system updates but also changes in operations processes or in the physical environment. These releases have a defined life cycle. The life cycle is defined by quadrants, operations management reviews (OMRs), and SMFs. The four quadrants are essentially categories, defined by the different SMFs that each quadrant contains. SMFs are groups of best practices; each category explains the activities of an operations environment. These quadrants reflect those found in Table 1.2.

The Changing Quadrant

The Changing quadrant is a group of SMFs that define the proper introduction of approved changes into a well-managed IT environment. This can include changes in applications, hardware, and systems, as well as changes in policies and procedures. The Changing quadrant maps to the ITIL discipline of service support. The three SMFs that reside in the Changing quadrant are Change Management, Configuration Management, and Release Management:

Change Management  The Change Management SMF is intended to place a rigorous process for introducing change into a well-managed IT environment with minimal impact to the operations of that environment. In the most efficient and well-managed enterprises, there are Change Advisory Boards as well as special subcommittees such as the Change Advisory Boards—Emergency committee.
**Configuration Management**  Configuration Management is all about being able to identify and maintain revisions and track every version of processes, procedures, documentation, hardware, software, or any other component within the enterprise. Once this catalog manifest has been achieved, these attributes can become potential configuration items (CIs), which then build into an overall model with the environment.

**Release Management**  Release Management is the culmination of Change and Configuration Management to inject or deploy change into the environment. This can be a single change or multiple changes that have been developed, tested, and packaged for a deployment. The goal of Release Management is to record and track changes into an environment with success, accountability, and the least impact possible to the environment.

**The Operating Quadrant**

The Operating quadrant is a group of SMFs that are used to monitor, control, manage, and administer service solutions to achieve and maintain service levels. All of the SMFs in the Operating quadrant are items that Microsoft has specifically added to expand ITIL:

- **System Administration**  The day-to-day administration of services and systems in an IT infrastructure could include user and group account administration; administration of file, print, database, and applications servers; low-level monitoring; and troubleshooting of the systems in the IT infrastructure.

- **Security Administration**  The administration of security in an IT infrastructure includes monitoring the environment in both a reactive and proactive way, thus ensuring that the environment is safe from attack. This is accomplished in many ways, including identification and authorization control, access control, and auditing.

- **Service Monitoring and Control**  The near real-time monitoring and alerting of the health of an IT environment ensures that SLAs are in place and that business requirements for IT services are being met.

- **Job Scheduling**  This SMF covers the administration and scheduling of jobs and processes so that an efficient sequence is utilized. This could include scheduling batch jobs to maximize system throughput and utilization and to meet SLAs.

- **Network Administration**  Administration of the network ensures that the network operates at an efficient level at all times. This includes the administration of people, processes and procedures, vendors, and service providers, as well as the administration of the network hardware.

- **Directory Services Administration**  This SMF provides for the administration of resources in Active Directory, such as users, applications, servers, printers, and so forth. The goal of this SMF is not only to make sure that directory access is always available but also to ensure that information from the directory is available via a simple and centralized process.

- **Storage Management**  This SMF covers administration and control of data, both electronic and physical, for the purposes of restoration and historical archiving. This includes both onsite and offsite storage. Storage Management was put into place to help guarantee the physical security of backups and archives.

**The Supporting Quadrant**

The Supporting quadrant is a group of SMFs that identify, assign, diagnose, track, and resolve incidents and problems in a timely manner within SLAs. The Supporting quadrant maps to the
ITIL discipline of service support. The three SMFs that reside in the Supporting quadrant are Service Desk, Incident Management, and Problem Management:

Service Desk  Almost identical to the service desk within ITIL, the service desk should be the primary point of contact for an organization to receive customers’ problems, concerns, questions, complaints, or requests. This function can also bridge or broker other technical resources that work independently across multiple geographic locations.

Incident Management  Incident management is the process by which, when an issue or occurrence is detected, the correct support resource can address and resolve the incident as quickly as possible. This process allows an organization to better understand the impact an incident has on the overall SLA, as well as to map recurring issues and potential financial impact.

Problem Management  In conjunction with incident management, problem management leverages the data results from the incident-management process to trend repeating incidences, prioritize, and analyze root causes. Without this important process, IT can be perceived as a “budgetary black hole” as well as impacting customers’ productivity by repeating incidences.

The Optimizing Quadrant

The Optimizing quadrant is a group of SMFs that help maintain business and IT alignment by attempting to decrease IT costs while maintaining or improving service levels. The Optimizing quadrant introduces three new SMFs to help expand the base ITIL disciplines:

Workforce Management  This function was added specifically to address staffing issues in the IT infrastructure team. It helps with the process of attracting, developing, and retaining a properly trained and prepared IT staff. It also ensures that the work environment is safe and efficient.

Security Management  This function was created to help an IT infrastructure define and communicate the business’s security plans and policies, based on the guidelines and regulations that apply to that business.

Infrastructure Engineering  Infrastructure engineering is the conduit and link between the people, process, and technology of an IT department. The reusable and consistent standards, policies, and procedures in the Infrastructure Engineering SMF could be linked to any other SMF to help coordinate engineering policies and standards.

Service Level Management  The process of service-level management is where the rubber meets the road. This process defines which services are offered and supported and at what cost to the business. Most organizations we have spoken and worked with have unwritten expectations or assumptions (“we expect the application to be available 100 percent of the time,” “my email is running slowly,” and so on), but few have well-defined, written SLAs. As organizations start defining and agreeing on service levels, along with seeing the cost of doing business, drastic behavior modifications or acceptance will generally result.

Capacity Management  The art and process of capacity management understands what an organization has and how it’s performing, knowing its current and future capabilities and optimizing for existing and future needs. The art is bringing together business, services, and appropriate optimized resources, which achieve the agreed SLAs of the customer.

Availability Management  As noted previously, it’s an expectation within the service-level management process for an application to be available 100 percent of the time. So it becomes
apparent that availability management has become one of the most important aspects with an IT service organization. Availability, or the occurrence of an incident, has a tremendous impact on customer perception of the IT services being provided.

**Financial Management**  In order for an organization to meet its requirements within the service-level management process, there are business demands for fiscal responsibility from a cost and budgetary perspective. In other words, for every request (action) there is a financial impact (reaction). At the end of the day, there needs to be a cost/benefit analysis.

**Service Continuity Management**  Another reason you should work toward achieving a well-defined SLA is preparing for the worst to happen: losing a hard drive, having an incorrect network configuration, having a WAN link trunk cut, or having a network administrator accept another job, for example. A customer or consumer of IT services doesn’t really care about the “hows” or “whys” of making things happen; they just want their things to happen.

In order to keep things happening, an organization must adopt a service continuity management process. This ensures keeping the business running or documenting risks that the business is willing to accept when managing an incident. This is a fine balance of resilient systems, failover or recovery options, and risk management.

**Operations Management Reviews**

Because the Microsoft Operations Framework is depicted as a circle, it is a continually evolving set of processes. Along with the distinct processes, continual customer feedback is always a part of the processes in order to further refine them. Along with the four distinct SMF quadrants are the operations management reviews, which are process review assessments that include the appropriate stakeholders.

OMRs are either event based or time based. The Change Initiation and Release Readiness reviews are event based and occur at the initiation and final installation of a review into the target environment.

**Change Initiation Review**  The Change Initiation Review is triggered when approval has been requested for a proposed change to the environment. This begins the process of actually implementing the release. Investments in money, time, equipment, and staff will now begin to work on the process and get it ready for release.

**Release Readiness Review**  The Release Readiness Review determines when a release is confirmed as ready for production. The proposed release is checked to ensure standards, policies, and quality; metrics are in place to support the release.

The Operations Review and Service Level Agreement Review occur at regular intervals to assess the internal operations as well as performance against customer service levels.

**Operations Review**  The Operations Review is a regularly scheduled review to assess and improve IT operations based on business needs and SLAs. Operations reviews use information from operations guides, company policies and procedures, and operating-level agreements to measure and evaluate the performance of the operations staff.

**Service Level Agreement Review**  The Service Level Agreement Review is a regularly scheduled review to assess and improve the alignment of business needs with IT service delivery defined in SLAs. During this review, the operations staff and service-level management take current information and measure that against published SLAs to determine whether the service has met its service-level requirements.
Within these four quadrants is a collection of 21 SMFs. Each quadrant consists of a group of SMFs that divide the quadrant into logical procedures and tasks. Each SMF is assigned to a home quadrant, but SMFs are by nature cross-functional and cross-quadrant.

**ITIL Version 3 and MOF Version 4**

In April 2008, Microsoft released MOF Version 4, which is based on ITIL Version 3. Although there is somewhat of a realignment of service management functions and the like, the fundamentals remain true. MOF v4 consists of four phases that include 16 SMFs. The four phases and goals are as follows:

**Plan**  Plan and optimize an IT service strategy to support business goals and objectives.

**Deliver**  Ensure IT services are developed effectively, deployed successfully, and ready for operations.

**Operate**  Ensure IT services are operated, maintained, and supported in a way that meets business needs and expectations.

**Manage**  This is the foundation of the IT service life cycle. This phase provides operating principles and best practices to ensure that the investment in IT delivers expected business value at an acceptable level of risk. This phase focuses on IT governance, risk, compliance, roles and responsibilities, change management, and configuration. Processes in this stage occur during all phases of the life cycle.

Within each phase, service management functions define the people, process, and activities required to align IT services. These functions are shown in Figure 1.1.

**Figure 1.1**
Microsoft Operations Framework 4.0
CHAPTER 1  OVERVIEW OF OPERATIONS MANAGEMENT

**Reliability Workbook for ConfigMgr**

This workbook can be found on the MOF Technology Library:


This workbook presents hands-on tasks that you can fine-tune to meet the goals of your organization. The workbook provides knowledge, specific tasks, and schedules needed to keep ConfigMgr running smoothly in your environment. Two documents are contained within the workbook:

- The first of these documents is an Excel spreadsheet that has Monitoring Activities, Maintenance Activities, Health Risks, and Standard Changes that can help you understand the task you need to modify or implement to support the MOF quadrant for this technology.

- The second is a Word document that is a guide to help you understand this quadrant and how to fine-tune the ConfigMgr servers’ daily tasks to achieve a desired compliance state.

---

**Real World Scenario**

**Workbook on Real IT World**

You are the Contoso Pharmaceuticals ConfigMgr administrator and your manager asks you to provide the most common ITIL and MOF associated with ConfigMgr. You find the Reliability Workbook for ConfigMgr and start reading it. After a few moments you find out this workbook will help you identify the tasks and procedures you need to deliver and implement as standard operating procedures for ConfigMgr in your environment. You provide the task lists that are used to monitor and maintain the reliability of your IT environment.

---

**Overview of System Center Configuration Manager**

So far you have read about the IT Infrastructure Library and Microsoft Operations Framework and now have a better understanding of the IT process and its quadrants. Now let’s look at System Center 2012 Configuration Manager, explore the new features of the product, and examine how the product has developed into an enterprise management tool that provides a total solution for Windows client and server management. ConfigMgr includes the ability to acquire hardware and software inventory in order to identify the assets for the enterprise; provides a wide variety of features that include delivery of new software packages, virtual applications, software updates, and operating systems; and also ensures the systems are protected with the latest antivirus definitions. All of these features are available through a single centralized console. ConfigMgr provides IT administrators with the capability to stay in control of the environment and help configure, manage, and secure the clients and applications.

**Configuration Manager Features**

Before you can begin planning to deploy Configuration Manager on your network, you need at least a basic understanding of the features that Configuration Manager provides. For veteran
SMS 2003 and Configuration Manager 2007 administrators, these features will not be very different from what you are already familiar with. However, you will find several new features added to Configuration Manager 2012, several features that were feature packs or add-ins in SMS 2003, and others that have been improved from Configuration Manager 2007. Configuration Manager 2012 no longer takes advantage of the Microsoft Management Console (MMC) technology for the administrator console; instead, each administrator console has its own stand-alone application, as shown in Figure 1.2.

The major features include the following:

**Inventory**  Configuration Manager offers you the ability to inventory the hardware and software of its client computers. Hardware inventory can gather information from your systems such as processor information, the computer manufacturer, and the amount of installed memory. Software inventory can gather lists of file types and their versions installed on your computers, with EXE files being the default. Combine this with extensive information in the Asset Intelligence (AI) knowledge base, and you can use Configuration Manager to really get a handle on what kind of hardware and software are being used in your environment.

Inventory is the backbone of Configuration Manager; you can run Configuration Manager without enabling inventory, but you really wouldn’t be able to do much, since so many other features, such as software updates, require inventory. Inventory is just about the same as it was in SMS 2003 and Configuration Manager 2007. Inventory is a very important piece of the MOF quadrant. Operations management is easy to maintain with a proper inventory of the IT environment; without one it’s very hard to maintain detailed information of the infrastructure and the current assets. We will go into more detail about this feature in Chapter 11, “Inventory and Software Metering.”
**Queries**  Queries allow you to gather information from the Configuration Manager database through the WBEM query language. This allows you to answer questions quickly or make mini-reports that might not be used often enough to be imported into the reporting interface. You can export these reports from the Configuration Manager console into different file formats and then email them for others to use in programs such as Microsoft Excel. Queries are primarily used to make groups of Configuration Manager resources, called collections, that are used by other Configuration Manager features. These queries are a good way to identify resources based on T-SQL. Parameters entered in the queries GUI inside Configuration Manager can simplify the reuse of code within a collection. As you can see, queries are a very important piece of the Capacity Management function in the Optimizing quadrant in ITIL and MOF.

**Collections**  Collections can be the answers or results to a question that involves specifying various resources, such as, “Which resources are running Windows XP Professional Service Pack 2 with more than 2 GB of RAM, with more than 1 GB of free disk space, and with a certain BIOS version?” Collections allow you to organize Configuration Manager resources into logical groups, based on a query. A collection can target Configuration Manager tasks to the resources that you specify. You can make collections based on queries, allowing them to be updated dynamically based on a configurable schedule or by directly assigning resources. Collections can consist of computers, users, user groups, or any discovered resources in the Configuration Manager database. Collections, as a fundamental feature, have not changed much since SMS 2003 or Configuration Manager 2007, but they are now the necessary building blocks used to enable other features such as maintenance windows and collection variables. Collections are a good way to analyze and organize resources; they can also depend on the Capacity Management SMF and the Optimizing quadrant in ITIL and MOF.

**Application Management**  This feature allows Configuration Manager to distribute just about anything to its client computers. This is probably the most-used feature of all the previous versions of Configuration Manager, and it’s probably the most dangerous if not used carefully. It is likely that just about all SMS admins have accidentally deployed a piece of software that they shouldn’t have (if you haven’t, then keep up the great work!). This isn’t a fault of this feature but something that can happen if you don’t test, test, and then test again. Anything you plan on deploying to client computers must be carefully managed, and you must pay close attention to the details of what you are doing.

---

**Real World Scenario**

**Using AdminStudio Configuration Manager Edition**

It is important to note that Configuration Manager is just the method of distribution; it doesn’t have any built-in capability to package software before it is distributed. You will have to use another piece of software to do that yourself. Microsoft has licensed AdminStudio Configuration Manager Edition to give administrators a reliable and repeatable tool to assist in creating Windows Installer packages. This, of course, is where the testing comes in. This feature has had numerous improvements since SMS 2003, such as the deployment of not only physical applications but also virtual applications, as well as improvements since Configuration Manager 2007, but overall it works basically the same as it did before. Application management is part of systems management on ITIL and the Changing quadrant of the MOF.
**Software Updates** This feature of Configuration Manager has to be one of our favorites. Using this feature, you can manage the daunting task of deploying updates to Microsoft applications and operating systems after the perfect storm that is Patch Tuesday blows through once a month (or whenever updates are released for other applications in your environment). Not only does this apply to Microsoft security patches and updates, but having this flexible and extensible environment has allowed partners (such as HP, Dell, IBM, Citrix, and others) to create custom catalogs to update server and desktop BIOS, firmware, and drivers as well as to create internal catalogs. This enables customers to create their own line-of-business application update catalogs and update them through the same streamlined process as Microsoft uses for patch management.

Deploying updates requires a Windows Server Update Services (WSUS) server. Configuration Manager leverages WSUS with its own functionality and provides a higher level of granularity than is available with WSUS alone. Software updates are an important phase in the Incident Management and Operations Management functions of ITIL and MOF. We will cover software updates in more detail in Chapter 8, “Software Updates.”

**Software Metering** Software metering, also covered in Chapter 8, allows you to collect information on software usage to assist in managing software purchases and licensing. Using software metering, you can do the following:

- Report on the software that is being used in your environment and on which users are running the software
- Report on the number of concurrent users of a software application
- Report on software license requirements
- Find unnecessary software installs
- Find software that is installed but isn’t being used

The new twist to software metering is that the metering rules are autopopulated, or created, but disabled by default, based on the software inventory. This allows you to rapidly meter applications and gain insights into usage. SMS 2003 had metering, but it was cumbersome to figure out the appropriate rule setup. This now is a thing of the past. Software metering is part of the Supporting quadrant in ITIL and MOF. Based on the utilization of software, you can measure when applications are properly used in the environment for better inventory of the current assets.

**Operating System Deployment (OSD)** This feature was originally released as a feature pack for SMS 2003. It was workable but was a minimalist approach that was sometimes difficult to implement and troubleshoot. Configuration Manager not only has this feature fully integrated into the product, but it has become a feature-rich, process-driven way to deploy servers and workstations. It leverages other new technology specifically designed by Microsoft to deploy operating systems to computers with multiple options.

Originally this feature supported the deployment of desktops only, but it now supports deploying servers. With the addition of the task sequencer and driver catalog, you can deploy to bare-metal computers or to ones that already have an operating system installed, as well as deploy software to these computers after they have been configured. This allows you to
minimize the number of images for different hardware, and it gives you more granular configuration options. OSD is also part of the Changing quadrant of the ITIL and MOF and an important piece of systems management. We will discuss this robust feature in more detail in Chapter 9, “Operating System Deployment.”

Remote Control This feature allows computer support staff to remotely troubleshoot problems with users’ computers just like they were sitting in front of the computer. This feature is still integrated with Remote Assistance and Remote Desktop, and it works pretty much the same as it did in the previous version.

The ability to support the desktops via remote control is a beneficial part of the Service Continuity Management function for ITIL and MOF.

Settings Management This feature is designed to address configuration drift within the enterprise. Enterprise administrators (for workstations and servers) as well as security teams need a tool that enables them to set configuration baselines (based on SOX, HIPPA, GLBA, or other compliancy regulations), deploy machines to an environment meeting these baselines (for example, with the local guest account disabled, Windows Integrated Security for SQL Server enabled, and so on), and then detect when these changes occur. Microsoft delivers configuration packs that jump-start an organization in the compliancy areas mentioned and allow you to set up a baseline of standards for your workstations and servers and audit your environment against that baseline.

You can configure your own baselines from scratch, or you can use best practices from Microsoft and their partners in the form of Configuration Manager Configuration Packs, which can be modified if needed. The ability to configure, monitor, and remediate the systems based on specific needs is key to System Management on ITIL and MOF. This feature will be covered in Chapter 13, “Compliance Settings.”

Mobile Device Management This feature allows you to manage mobile devices such as Windows Mobile Pocket PC and smartphones. Inventory, file collection, software distribution, and device configuration are all options with this feature. This was an add-on feature in SMS 2003 and is now fully integrated into Configuration Manager. New environments are bringing mobile devices to each environment. There is a need to support mobile devices to ensure that IT is running on the same track as the consumer. This is part of the Supporting, Changing, Operating, and Optimizing quadrants on ITIL and MOF. This feature will be discussed in Chapter 14, “Mobile Device Management.”

Network Access Protection This is a new feature in Configuration Manager. It leverages technology built into Windows Vista and Windows Server 2008 that allows you to protect your network from potential threats by not allowing computers to access your network that do not meet certain system health requirements such as having updated antivirus definitions or security patches installed. With this feature you can also enforce certain network protocols. The ability to secure the environment is one of the tasks on the Supporting and Operating quadrants on ITIL and MOF. Chapter 15, “Troubleshooting,” covers this feature.

Wake on LAN This feature, added to software distribution, was available in SMS 2003 only by purchasing third-party software. It allows you to leverage technology built into computer hardware to wake up computers that have been turned off so they can run assigned deployments. Chapter 7, “Application Deployment,” shows how to enable it. This option brings more power to the tasks of the Operating and Supporting quadrants for the ITIL and MOF.
**Reporting**  This feature is great for reviewing the status of the environment, for showing return on investment, and for matching licensing with what is actually installed. It grants visibility into the enterprise with the integration of Asset Intelligence (covered in Chapter 10, “Asset Intelligence”). This allows you to gain an understanding into licensing (Microsoft and third-party licenses), asset age, Client Access License (CAL) utilization, product families/categories, and much more insightful data. With this feature you can create web-based reports, via Configuration Manager or through SQL Reporting Services, that can show all the data that has been collected by the various other Configuration Manager features, such as software update deployment success or a list of computers of a certain manufacturer.

You can also group together commonly viewed reports into “dashboards” for easy viewing with just one click. Numerous reports are already created out of the box, and you can create your own custom reports with a little knowledge of SQL queries. On ConfigMgr 2012 the only report option we have is based on Reporting Services. This is the most beneficial piece of systems management for ITIL and MOF: being able to report back everything that is going on with the IT resources makes the job of auditing and reporting a simple one. Reporting is discussed in several chapters and is covered fully in Chapter 12, “Reporting.”

**Out-of-Band Management**

A business challenge that has been a struggle for years is the ability for software to communicate directly with hardware. Let’s say, for example, that you’re supporting a worldwide organization and have a centralized help desk. You have a desktop that is thousands of miles away, and the user has contacted you because of an operating system “blue screen.” A typical support remediation from years past would be to create a ticket so that a local technician would be able to physically visit the location.

Intel introduced manageability directly into its chip set with the Intel Active Management Technology (AMT) initiative; the direct result was the Intel vPro desktop processor. Intel and Microsoft worked on a strategic management initiative so that software could communicate directly with hardware. Now, when a user contacts the help desk with that same scenario, a help desk administrator can actively engage and potentially resolve an issue without needing to escalate a ticket to another team.

Configuration Manager leverages four key areas to communicate directly to hardware. These areas may be leveraged holistically within an organization’s standard operating procedures for in-band and out-of-band management to provide a streamlined resolution process. In-band management is used when the Configuration Manager client agent is functioning, and out-of-band management occurs when software communicates with hardware because no other means may apply. These are the four areas:

**Discovery**  Discovery is an area of out-of-band management that provides an administrator with the ability to achieve discovery on demand. This can be performed on a single machine or groups of machines via a Configuration Manager collection. It also allows you to schedule a discovery so that if the software does not respond, the hardware still can provide the insight into an asset.

**Power Control**  Power control provides the flexibility to allow both scheduled and on-demand power-on capabilities. From a scheduling perspective, this can potentially improve efficiency and data consistency when used in conjunction with other Configuration Manager features such as software distribution, software update management, or operating
system deployment. From an on-demand perspective, this enables administrators to wake up, restart, or shut down a remote machine. One area of efficiency that enterprises are increasingly demanding is power management. Thus, the ability to control hardware and software from a single pane of glass becomes an attractive feature.

Provisioning Provisioning workstations, either as new assets that enter the enterprise or as a means to an end in the remediation process, has become a necessary part of an administrator’s role. As the operating system becomes less independent of hardware (that is, the operating system hardware abstraction layer [HAL]), the provisioning process may become more streamlined. With an integrated solution such as AMT and Configuration Manager, a secure, zero-touch setup and provisioning of workstations can be achieved.

Remote Console Remote console for out-of-band management enables administrators to perform advanced abilities such as serial over LAN, IDE redirection, BIOS password bypass, and manual power control. This allows an administrator to remotely mount a bootable, troubleshooting image (ISO image); boot into the BIOS to change the boot order; or turn the targeted machine on or off at will.

To that end, when the user contacts the help desk with a nonfunctioning operating system, the help desk administrator can proactively take the appropriate actions. For example, the standard operating procedure might look starkly different from just creating a ticket and dispatching a desktop support technician. It may be that the help desk administrator reboots into the BIOS, leveraging the serial-over-LAN capabilities, and changes the boot order in the BIOS so that the network card is the first in the boot order. From there, a diagnostic tool is mounted with IDE redirection, which gives the administrator the insight that the operating system has some corrupt DLLs. Thus, the administrator can then provision a role-based operating system image to this user to re-image the workstation. A process or help desk ticket that might have been very expensive or time-consuming now becomes a streamlined process that results in the user having less downtime and a higher degree of satisfaction with their help desk interaction.

Asset Intelligence

Asset Intelligence, which was included within Configuration Manager 2007, now comes with its own node within the Administrator console. This isn’t the only new aspect of Asset Intelligence; AI also became part of the Software + Services initiative within Microsoft. The services component of AI is not a fee-based feature but is just another extension of the holistic approach; it includes the following functionality:

◆ New catalog and license management UI in the Configuration Manager Administrator console
◆ The ability to customize the local catalog, in other words, create new categories and families
◆ On-demand or scheduled catalog update synchronization through the Configuration Manager console
◆ The ability to tap software assets unknown to the catalog and pass them up to the online service for a-sync identification
◆ The ability to import licensing data from Microsoft and compare it to installed inventory
Asset Inventory is one of the reporting structures used to analyze and ensure every asset on the system is being used properly and report this to management. This ability is part of systems management and configuration management for ITIL and MOF; we’ll discuss this further in Chapter 10.

**APPLICATION VIRTUALIZATION MANAGEMENT**

With the newest release of App-V, Configuration Manager 2012 leverages its existing infrastructure and extends the reach to deliver virtual applications:

- It integrates Microsoft App-V 4.6 with ConfigMgr 2012.
- Application Virtualization Management (AVM) allows you to use Configuration Manager to manage and deploy virtual applications, when possible, to make managing virtual applications for the Configuration Manager admin the same experience as when managing standard or “physical” software.
- AVM has version checking, user-based targeting, and streaming functionality.

**OPERATING SYSTEM DEPLOYMENT ENHANCEMENTS**

Although Configuration Manager 2007 was good at deploying operating systems, a couple of improvements were needed in order to compete in the marketplace. The following enhancements now round out the offerings of Configuration Manager in the enterprise:

- With ConfigMgr 2012, an unknown machine can now receive a task sequence to install an operating system.
- There is support for multicasting operating system images to a PXE environment—for well-connected LANs leveraging Windows Server 2008 R2 technologies, on the same distribution point.

**SQL REPORTING SERVICES INTEGRATION**

SQL Reporting Services (SRS) is an evolution of reporting just as previous technologies have been. The Microsoft management team has standardized on SRS for reporting within the System Center family of products. The SRS integration within Configuration Manager 2012 enhancements includes the following:

- The new server role Reporting Services point
- The ability to manage, browse, and run SRS Configuration Manager reports from the Configuration Manager console

**CENTRALIZED POWER MANAGEMENT**

Saving energy and preserving the environment are important goals for IT professionals and organizations. The ability to control the power-saving settings on workstations is a great achievement for many organizations. Also important are the abilities to monitor the power consumption, create different power plans based on organization need and different operational
departments, and check compliance and remediate those workstations that are in noncompliance. It’s easy to manage these situations on the SQL Reporting Services.

**SYSTEM CENTER ENDPOINT PROTECTION**

This feature brings the ability to scan and secure system resources from viruses or malware. System Center Endpoint Protection enables businesses to align security and management to improve endpoint protection while greatly reducing operational cost.

Endpoint Protection is built on three pillars: simplify, integrate, and protect.

- **Simplify**  Creates a single administrator experience for managing and secure endpoints
- **Integrate**  Lowers ownership cost by using a single infrastructure for both endpoint management and security
- **Protect**  Provides highly accurate detection of known and unknown threats
  Actively protects against network-level attacks by managing Windows Firewall configurations