

Best Practices for Service Vendor Management

A MOF Companion Guide

Version 1.0

Published: June 2010

For the latest information, please see [microsoft.com/mof](http://www.microsoft.com/technet/solutionaccelerators/default.mspx)

Copyright © 2010 Microsoft Corporation. This documentation is licensed to you under the Creative Commons Attribution License. To view a copy of this license, visit [http://creativecommons.org/licenses/by/3.0/us/](http://creativecommons.org/licenses/by/3.0/us/%20) or send a letter to Creative Commons, 543 Howard Street, 5th Floor, San Francisco, California, 94105, USA. When using this documentation, provide the following attribution: The Microsoft Operations Framework 4.0 is provided with permission from Microsoft Corporation.

This documentation is provided to you for informational purposes only, and is provided to you entirely "AS IS". Your use of the documentation cannot be understood as substituting for customized service and information that might be developed by Microsoft Corporation for a particular user based upon that user’s particular environment. To the extent permitted by law, MICROSOFT MAKES NO WARRANTY OF ANY KIND, DISCLAIMS ALL EXPRESS, IMPLIED AND STATUTORY WARRANTIES, AND ASSUMES NO LIABILITY TO YOU FOR ANY DAMAGES OF ANY TYPE IN CONNECTION WITH THESE MATERIALS OR ANY INTELLECTUAL PROPERTY IN THEM.

Microsoft may have patents, patent applications, trademarks, or other intellectual property rights covering subject matter within this documentation. Except as provided in a separate agreement from Microsoft, your use of this document does not give you any license to these patents, trademarks or other intellectual property.

Information in this document, including URL and other Internet website references, is subject to change without notice. Unless otherwise noted, the example companies, organizations, products, domain names, email addresses, logos, people, places and events depicted herein are fictitious.

Microsoft and Active Directory are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries.

The names of actual companies and products mentioned herein may be the trademarks of their respective owners.

You have no obligation to give Microsoft any suggestions, comments or other feedback ("Feedback") relating to the documentation. However, if you do provide any Feedback to Microsoft then you provide to Microsoft, without charge, the right to use, share and commercialize your Feedback in any way and for any purpose. You also give to third parties, without charge, any patent rights needed for their products, technologies and services to use or interface with any specific parts of a Microsoft software or service that includes the Feedback. You will not give Feedback that is subject to a license that requires Microsoft to license its software or documentation to third parties because we include your Feedback in them.

Contents

[Introduction 1](#_Toc263174770)

[Intended Audience 1](#_Toc263174771)

[Goals of Service Vendor Management 2](#_Toc263174772)

[Service Agreements 2](#_Toc263174773)

[Types of Service Agreements 2](#_Toc263174774)

[Creating Service Agreements 4](#_Toc263174775)

[Elements of Service Agreements 4](#_Toc263174776)

[Before Writing the Service Agreement 7](#_Toc263174777)

[Living with the Service Agreement 12](#_Toc263174778)

[Beyond the Contracts 14](#_Toc263174779)

[About MOF 4.0 15](#_Toc263174780)

[About MOF Companion Guides 15](#_Toc263174781)

[Feedback 15](#_Toc263174782)

[Appendix: Key Terms 16](#_Toc263174783)

[Acknowledgments 17](#_Toc263174784)

# Introduction

Today, organizations frequently elect to have certain services be provided by service vendors, also referred to as service providers or partners. In such situations, the need for well-defined, coordinated working relationships increases. Setting clear roles, establishing responsibilities, putting change processes in place, and defining measures of success are all necessary best practices if the organization and service vendors are to work together successfully to deliver agreed-upon results.

Building and maintaining the working relationship between the service vendor and the organization is an important aspect of service relationship management, which is defined as the ongoing process that ensures that service providers and the organizations employing them remain in sync. Effective service relationship management also includes the following activities:

* Clarifying expectations and documenting them in service agreements.
* Preparing for a new service.
* Monitoring results.

Without careful attention to good service relationship management, the service vendor/organization arrangement can have negative consequences. For example:

* Unclear definition of roles and responsibilities can lead to work being overlooked, duplicated, or completed inefficiently.
* Unclear expectations can lead to misunderstandings and confusion and failure to achieve the expected value of the partnership.
* A lack of agility can mean missed opportunities and delays in resolving issues.

Service agreements, and their management, are the means of carrying out the above functions and preventing the negative consequences. This document defines the basic service agreements (service level agreements, operating level agreements, and underpinning contracts) and discusses their roles in the management of service vendors.

## Intended Audience

This document will be most useful for the service consumer and service provider managers who are directly involved in managing service vendors:

* Service level managers
* Operations managers
* Supplier managers
* Risk and compliance managers

# Goals of Service Vendor Management

Organizations must manage the ongoing delivery and enhancement of their services.
To deliver services effectively, all partners involved in the service must work well together. Service vendor management ensures that ongoing requirements and communications between partners are proactively managed and that all expectations are being met.

As organizations enter into vendor relationships, effective service vendor management becomes even more important, due to the following factors:

* A shift in responsibility. Certain services, such as infrastructure support, may be owned outside the organization; others, like testing and interfaces with other systems, are often still the organization’s responsibility. An organization also continues to have management responsibilities for oversight.
* A shift in ownership of components. Servers and other hardware, as well as decisions about them, are owned outside the organization. The partner needs information about demand in order to continue to provide the appropriate level of service.
* More parties involved. Handoffs and interfaces become critically important.
* Integration with other systems. For example, identity management and access control (enterprise integration) requires keeping systems in sync.

Therefore, the goals of effective service vendor management are to:

* Promote coordination across multiple teams to ensure that a service provides the expected value.
* Provide a positive experience for users by meeting their technology needs and addressing complaints and issues that arise during the normal course of using a technology service.
* Reflect the fact that responding to changes or issues is a shared responsibility that demands good coordination.

# Service Agreements

Strong service vendor relationships require that shared expectations be clearly documented. Prior to embarking on a service vendor relationship, the organization should create a written, binding agreement—called a service agreement—between itself and the service vendor.

## Types of Service Agreements

Here are the types of agreements that cement the understanding between service providers and clients:

* **Service level agreement (SLA).** A written agreement documenting required levels of service. The SLA is agreed upon by the service provider and the consumer, or by the service provider and a partner provider. SLAs should list the metrics and measures that define success for both the service provider and the consumer.
* **Operating level agreement (OLA).** An agreement between one or more internal teams that supports the requirements set forth in the SLAs.
* **Underpinning contract (UC).** A legally binding contract in place of or in addition to an SLA. This type of contract is with a partner service provider responsible for building service deliverables for the SLA.

For simplicity, in this document we will use the general term service agreement to refer to any of these agreements.

Figure 1 depicts an example relationship between various types of customers and SLAs, OLAs, and UCs.



Figure 1. An example relationship between customers and the SLA, OLA, and UC

## Creating Service Agreements

These are the steps needed to determine what service agreements are needed and to put those agreements into place:

1. Define the list of services under consideration.
2. Define service level objectives for each service.
3. Create a service map for each service.
4. Use the service map to identify required SLAs, OLAs, and UCs for the defined service.
5. Draft initial agreements and ensure UCs underpin OLAs, which in turn underpin the SLA defined.
6. Finalize, approve, publish, and distribute agreements.
7. Monitor and report on service levels.

## Elements of Service Agreements

The elements shown in Table 1 are common to all service agreements. This table lists the topics that go into the agreement and key questions that relate to those topics. Document the decisions made about these elements in the formal service agreement.

Table 1. Elements of Service Agreements

| **Section** | **Goal** | **Key Questions** |
| --- | --- | --- |
| **Purpose** | Intent of the service | * To what service does this service agreement refer?
* What is the organization trying to accomplish with this service?
* What is this document meant to communicate or guarantee?
 |
| **Authorization** | Ownership and responsibility for the service | * Who are the groups or representatives that share ownership of the service?
* How is this updated as personnel changes?
 |
| **Service** | Shared expectations | * What exactly does the service do?
* What is its user community?
 |
| **Business organization and scale** | Users of the service | * What are the characteristics of the user community (including, but not limited to: number of users, physical location, computer platform, operating system, and number and type of desktops)?
* How is this expected to change?
* What is the process for communicating changes?
 |
| **Reviews** | Regularly scheduled meetings | * How and when will service targets be reviewed? (For more information, see Management Reviews: <http://go.microsoft.com/fwlink/?LinkId=186460>.)
 |

| **Section** | **Goal** | **Key Questions** |
| --- | --- | --- |
| **Time conventions** | Common definitions | * What hour/minute format will be used?
* What time zone is reflected?
* What are the conventions for business hours and business days (Monday through Friday, or 24/7)?
 |
| **Service availability** | Availability requirements and usage patterns | * When is the service normally available?
 |
| **Job scheduling** | Outage constraints | * What are the nature and duration of any scheduled outages?
 |
| **Changes to the service** | Modification process | * What is the process for enhancing or changing the service?
* How will proposed changes be handled? What are the triggers, decision makers, process? (For more information, see the Change and Configuration SMF: <http://technet.microsoft.com/en-us/library/cc543211.aspx>.)
 |
| **Monitoring and reporting** | Evaluating the service | * What form does monitoring and reporting of the service take?
* What is the frequency/timeline of any reports? (For more information, see Management Reviews: <http://go.microsoft.com/fwlink/?LinkId=186460>.)
 |
| **Metric definitions** | Evaluating the service | * How are metrics measured (in terms of percentage of service availability, request response time, or incident resolution time)? (For more information, see the Service Monitoring and Control SMF: <http://technet.microsoft.com/en-us/library/cc543300.aspx>.)
 |
| **Service lifecycle** | Beginning and ending the service partnership | * How will the service be set up for the customer, their data migrated over, and their systems switched?
* What is the exit plan at the end of the contract? How will the customer’s data be returned or destroyed and in what time frame?
 |
| **Ongoing system integration** | Data transfer between systems (For example, Active Directory® Domain Services or identity management) | * How will that be initiated? Maintained? Problems solved?
* What systems need to be integrated?
* How will the integration be tested and accepted?
 |

| **Section** | **Goal** | **Key Questions** |
| --- | --- | --- |
| **Key contacts** | Ongoing communication | * What happens when personnel on either side changes?
* Who is responsible for key services in both parties?
* Who will they contact?
* What is the expected response time?
 |
| **Confidentiality** | Data protection | * What are the requirements for confidentiality?
* What data needs special protection?
* How will data be stored and then deleted when necessary?
 |
| **Data integrity** | Data protection | * What backups will be done? What proof of restore capability will there be?
* Does any of the data need special handling?
 |
| **Follow up** | Incident management | * When a problem occurs, who will they contact? Names, numbers, email addresses, other ways to contact.
 |
| **End-user support** | Incident management | * Who will end users call with problems and questions?
* How can they be contacted?
* What are the hours of support?
* What is the expected response time?
 |
| **Provisioning and de-provisioning** | Handling user changes | * How will normal provisioning and de-provisioning of new and departing users or systems be handled?
 |
| **Compliance** | Meeting policy requirements | * What are the management objectives and policies that must be met by the service?
* Who is responsible for design, test, and documentation of controls?
* What certifications are required from the provider? How will these be verified?
 |

## Before Writing the Service Agreement

Decision makers need to identify and complete any necessary agreements and contractual considerations prior to implementing the new service. This includes detailed considerations of policies, management and reporting processes, work flows and reliability, and the pre-adoption work involved as a service, before moving into production, along with operation and support issues.

The pre-implementation tasks in Table 2 can help business decision makers:

* Consider the risk implications of expanding the software delivery portfolio beyond its firewall.
* Assess how it affects existing assets.
* Identify steps to mitigate risks associated with making the transition to a new software delivery model.

The following tasks and best practices are set up as a table to facilitate a clear division of responsibility.

Table 2. Pre-Implementation Tasks

| Responsible Party | Actions |
| --- | --- |
| GovernanceDecision Maker | * Assign executive sponsor or leadership team with primary responsibility for incorporating service delivery into the organization’s governance structure.
* Set strategic direction and objectives for managing service delivery and the relationship between parties.
* Align business case, value metrics, and measurements to expected value to be realized.
* Develop governance operating model to supply decision-making rights, management reviews, escalated service issues or conflict resolution, service performance, and change management to the service requirements.
* Determine key roles, responsibilities, and accountabilities between the two organizations.
* Assign individuals to roles within the governance structure.

**Note**   For more information, see the [Governance, Risk, and Compliance SMF](http://technet.microsoft.com/en-us/library/cc531019.aspx). |
| Service Provider Account Manager | * Develop business control processes to maintain service vendor performance oversight per criteria defined for governance.
* Require the service vendor to provide reporting that compares actual service delivery against the applicable SLA or performance metrics.
* Establish regular meeting schedules to review service level performance and changes to service delivery needs.
* Review and monitor service delivery according to contractual terms and conditions.
* Assess whether the expected business value sought is being realized.
* Monitor stakeholder adoption levels, escalated issue resolutions, and new stakeholder business requirements to ensure that the relationship meets expectations.
* Establish a feedback loop with service vendor to ensure that timely communication of employee issues, system errors, or process problem trends occurs for strategic resolution.
* Review internal change requests and analysis documentation and act as a liaison with service vendor to secure changes and approvals to the agreement scope.
* Consider making service vendor management a dedicated account management function rather than a function of another job. Non-dedicated personnel performing vendor management can lead to poor oversight of the vendor’s performance.
* Consider assigning multiple layers of account management as part of the governance model.
* Develop a plan to rotate account managers periodically to ensure that arm’s-length relationships are maintained.
 |
| Service Provider Operations | * Manage the day-to-day service operations with clearly defined, mature control processes.
* Maintain a multi-pronged, multi-tiered security approach to ensure customer information/data assets are protected at all times.
* Monitor all service level and other performance metrics defined by the SLA.
* Provide around-the-clock, in-house technical expertise to support and resolve any internal operational issues or problems affecting service delivery.
* Notify customer organization of unresolved or escalated issues or problems affecting service vendor’s delivery of service.
* Monitor all critical components of the applications, databases, and infrastructure-related components to ensure that availability, performance, and capacity expectations for the service are being maintained.
* Provide full lifecycle management services including administrative, technical, and engineering resources required to install, maintain, troubleshoot, and operate the offered software systems and services.
* Report operational performance showing actual service delivery against the applicable SLA or performance metrics.
* Review and implement approved changes requested to the agreement scope.
* Facilitate integration with customer’s identity management and access control systems, data exchange interfaces, and compliance reporting.
* Participate in Policy and Control management reviews (<http://technet.microsoft.com/en-us/library/cc506048.aspx>) to make sure that compliance objectives are met and that the people in identified roles regularly meet and fulfill their mutual obligations.
 |

| Responsible Party | Actions |
| --- | --- |
| Decision Maker Focused on Service Level Agreements | * Establish SLAs with the service vendor that define the scope of the service guarantees, including metrics used to measure availability, performance, security, and support.
* Ensure the SLAs provide sufficient levels of mitigation (for example, data loss protection, backup and recovery services, and disaster recovery capabilities) in even the worst-case scenarios.
* Ensure the SLAs guarantee a high level of service to your business and define the actions the provider will take—or the compensation it will provide—in the event that it fails to meet these guarantees.
* Ensure that the penalties for nonperformance, poor performance, or contract noncompliance are sufficiently significant to motivate the vendor to meet business requirements.
* Consider building a bonus structure into the contract to reward the service vendor for consistently performing better than what the SLAs require.
* Define a consistent and documented process for managing SLA exceptions resulting in service interruptions.
* Promote a commitment to quality and the continuous improvement process by conducting adequate due diligence when SLAs are missed: Determine the root cause and perform timely remediation.
 |
| Business Intelligence/Data Reporting Services | * Determine what reporting services the service provider offers and whether they are compatible with your business-intelligence requirements. Because service delivery may involve giving up direct control to some level of corporate data, accurate and useful reporting services may be needed across internal and service vendor-hosted systems to verify that data is in synch and that interfaces are operating as expected.
* Develop a process to identify service vendor data errors and to research and resolve possible data integrity issues.
 |
| Regulatory Compliance Officer | * Develop a process to systematically communicate policy changes, regulatory compliance procedures, and new initiatives to the service vendor and define responsibility for this function in the governance model.
* If the service vendor has a SAS 70 accreditation, determine if it applies to a Type I or Type II audit.
* Review the service vendor’s SAS 70 report thoroughly to determine if the processes and controls being tested apply to the data center, infrastructure, or application services provided by the service vendor’s offerings under consideration. Be aware that many providers will claim SAS 70 Type II, but it only applies to the hosting infrastructure and not the hosted applications.
* Examine the report thoroughly to determine whether the provider can comply with your own policies.
 |

| Responsible Party | Actions |
| --- | --- |
| Billing and Invoicing Personnel | * Review the service vendor’s pricing model for costs or charges related to any initial setup, installation, or implementation fees, monthly recurring subscription or usage fees, and one-time charges (such as customizations or data migrations).
* Establish controls and respective ownership around invoice review, reconciliation, authorization, and payments.
* Establish a link between invoicing and service vendor performance, SLA adherence, satisfaction survey results, and contract requirements.
* Develop a process whereby the organization’s vendor account management team reviews the invoices for accuracy, validates that SLAs and performance requirements were met, and payments were authorized accordingly.
 |
| Confidentiality and Privacy Manager | * Regularly assess the service vendor’s privacy and confidentiality compliance defined by your internal policies, and assign responsibility for this function in the governance model.
* Determine if the service provider privacy policies and practices are in compliance with requirements set forth by the U.S. Department of Commerce Safe Harbor Act (also known as the European Union Data Protection Directive). Certifying to the ”adequacy” standard for privacy protection will assure European Union (EU) organizations that your company provides adequate privacy protection for transferring personal data.
* Develop a process to manage privacy and confidentiality complaints related to the service provider outsourcing arrangement. This should include defining an escalation path and a process to resolve complaints with the service vendor.
* Verify that the service vendor’s employees and subcontractors with access to your organization’s data are required to sign a non-disclosure agreement and undergo background checks as a condition of employment.
* Require the service vendor to administer privacy and confidentiality training to all employees and subcontractors handling your organization’s personal data.
* Limit vendor and subcontractor access to sensitive, employee-personal data, such as government-provisioned identification credentials (for example, social security or driver’s license numbers), financial transaction authorization data (for example, credit card information), financial or medical profiles, and other highly sensitive information where unauthorized disclosure would cause considerable material loss.
 |
| Employee Liaison | * Define the timing, frequency, and population of employees that will be surveyed, and develop a process to systematically collect and summarize survey results.
* Develop a process to confirm that the survey results are reviewed by the appropriate management teams and to address and resolve concerns identified in the surveys in a timely manner.
 |
| Data-Security Specialist | * Assess your information security policy and data-security needs to ensure that the service provider has sufficient security measures and data protections in place to meet your corporate standards.
* Evaluate the service provider’s security measures for its data center, networks, servers, and SaaS application security. Additional considerations for protecting data include firewalls, digital certificates, security scans, vulnerability assessments, and industry-recognized security certifications.
* Review the service vendor’s backup and data recovery capabilities: frequency and type of backups, off-site storage, retention periods, and archiving services.
* Review the service vendor’s disaster recovery and business continuity plans and the testing of those plans.
* Develop an employee satisfaction survey about the success of the service offering. Include questions about the success of the transition process and identify issues and opportunities for improvement.
 |
| Manager in Charge of Implementation | * Review service provider’s implementation methodology and procedures it uses, including any provisions for data-migration and identity integrations required for single sign-on.
* Develop a plan for migrating to the new service provider. Include a complete list of activities each party is responsible for during the migration process.
* Identify risk factors, risk mitigation strategies, necessary security tasks, data preparation tasks, communication plans, and other measures necessary to minimize disruption to the organization during implementation.
* Transfer knowledge through training and other measures to facilitate using the service applications.
 |
| Contracts Manager | * Develop exit plan for migrating data out of the application in the event the contract is terminated prematurely or expires naturally. Ensure the contract language specifically addresses:
* Terms and conditions in effect upon termination or expiration of the agreement.
* Termination assistance services, fees, charges, or other compensation.
* Control and ownership of data throughout the life of the contract.
* Source code disposition, including code escrow for any derivative works created during the contract term.
* Specifications, documentation, information, and other assistance necessary to enable the organization to receive services from another provider.
 |

## Living with the Service Agreement

Review the results of day-to-day operations using the Service Alignment or Operational Health management reviews to catch issues early. Compare the day-to-day results to the agreed service levels. Look at areas for possible improvements and follow up on any changes as needed, which may sometimes require renegotiating the agreement. Review the following on a monthly basis:

* Performance that is outside of established tolerance levels and possible causes for this.
* Operational maturity compared to desired state.
* Compliance violations.
* Whether service level metrics targets have been consistently met.
* Any confusion arising from handling issues or daily operations.

An agreement is only helpful when it is current. On a regular basis—annually, at a minimum—review the agreement to ensure it still reflects the organization’s requirements. As you use the service agreement, make sure to get answers to the following questions:

* Has the demand changed?
* Has the technology changed in a way that offers new opportunities or changes assumptions from the original agreement?
* Are there changes by either the organization or the provider that will involve a change to the agreement? For instance, are there any new services offered either by the provider or requested by the organization?
* Do the service level metrics targets continue to meet the business needs?

Take into account any anticipated future changes. For example:

* Ongoing or emerging issues, reflected in action items and previous management review minutes and from other industry and organizational sources.
* Changes in risk assessments or tolerance boundaries.
* Upcoming changes that may affect operations.

Table 3 describes each of the management reviews used to evaluate key metrics and show trends over time and compared to targets. You can find more information on the MOF management reviews at <http://go.microsoft.com/fwlink/?LinkId=186460>.

Table 3. Management Reviews

| **Management Review** | **Description** | **Use in Partner Relationships** |
| --- | --- | --- |
| **Operational Health** | This management review provides a structure for reviewing and analyzing results and taking action to improve performance. It might result in requests for changes or improvements in existing services, as well as changes to SLAs and OLAs. | Compare actual performance to expected metrics. Track and review trends to evaluate for possible changes to the service (for example, increased demand or changing patterns of use or upcoming changes to related services that will have an impact). |

| **Management Review** | **Description** | **Use in Partner Relationships** |
| --- | --- | --- |
| **Service Alignment** | This management review focuses on understanding the state of supply and demand for services and directing investments to make sure that the business value of the services is realized. It is responsible for officially proposing new services, making changes to existing services (such as service improvements) that are larger than standard changes, and decommissioning features and services. | Anticipate and plan for changes to supply and demand for services. Review customer satisfaction with the service. |
| **Portfolio** | This management review focuses on proposed service changes and the current mix of projects and services being built and in production. The ultimate outcome of the Portfolio Management Review is the initial project charter, with which a project team can begin the process of creating the project plan that will ultimately result in building and delivering new or updated services. | Evaluate and approve proposed investments in new or updated services. |
| **Project Plan Approved** | This management review focuses on finalizing the scope of a delivery project. It signals a complete review of key project plans and the readiness of the project team to move on to the development of the solution. | Proceed with changes to the services. |
| **Release Readiness** | This management review focuses on the readiness of a new or improved service to be deployed; it results in a go/no-go decision about whether to deploy the release. | Prepare for a new service. |
| **Policy and Control** | This management review evaluates the effectiveness of the policies and compliance controls in place across the service management lifecycle. The Policy and Control Management Review should identify requests for changes that will improve the management and enforcement of policies as well as improve the management of risk. | Evaluate compliance with policy and processes that support or inhibit compliance. Adjust services in response to changes in policy. Implement new controls or improve existing controls where needed. |

# Beyond the Contracts

The most successful service vendor relationships use best practices that go beyond formal agreements. The following best practices build trust and support good communication:

* Stay in sync by:
* Developing common expectations.
* Identifying clear handoffs.
* Defining common language—confirm that you both mean the same thing when using key terms. Remember that you are coming from different perspectives and may be making different assumptions.
* Stay in contact by:
* Assigning designated contacts on both sides.
* Scheduling regular communication via strategic, tactical, and operational meetings.
* Manage risk by:
* Being proactive in evaluating and managing risk.
* Designing interlocking controls to manage risk and increase confidence.
* Sharing information about how controls are operating for better monitoring and improved risk management.
* Building resilience for handling the unexpected.
* Deal with everyday issues early before you have to enforce through the contract by:
* Identifying triggers and warning signs, responsibilities, and escalation paths.
* Partnering problem solving with the service vendor.

# About MOF 4.0

Microsoft Operations Framework (MOF) 4.0 is concise guidance that helps organizations improve service quality while reducing costs, managing risks, and strengthening compliance. MOF defines the core processes, activities, and accountabilities required to plan, deliver, operate, and manage services throughout their lifecycle. The MOF guidance encompasses all of the activities and processes involved in managing a service: its conception, development, operation, maintenance, and—ultimately—its retirement.

MOF organizes activities and processes into service management functions (SMFs), which provide detailed processes and outcomes related to a series of disciplines. Each SMF is anchored within a lifecycle phase and contains a unique set of goals and outcomes that support the objectives of that phase. For more information about SMFs, visit [www.microsoft.com/mof](http://www.microsoft.com/mof).

## About MOF Companion Guides

MOF companion guides are intended to help business and technical decision makers and service providers perform activities effectively and cost-efficiently. Each guide focuses on a specific activity and applies MOF 4.0 principles.

## Feedback

Please send comments and feedback to MOF@microsoft.com. To keep current with the latest releases and beta review programs, please subscribe to our news feed on the [MOF home page](http://technet.microsoft.com/en-us/solutionaccelerators/dd320379.aspx).

# Appendix: Key Terms

Table A-1 defines terms that are used in this document.

|  |  |
| --- | --- |
| **Term** | **Definition** |
| consumer | Users of a service. |
| operating level agreement (OLA) | An internal agreement between one or more teams within an organization that supports the requirements set forth in the service level agreements (SLAs). |
| service level agreement (SLA) | A written agreement documenting required levels of service. The SLA is agreed upon by the service provider and the business, or by the service provider and a partner provider. SLAs should list the metrics and measures that define success for both service providers and the larger organization. |
| service level management  | The process of defining and managing performance through monitoring, reporting, and reviewing the required, agreed-upon level of service. |
| service provider/service vendor | Provider of a service. |
| service relationship management | The ongoing process that ensures that service providers and the organization remain in sync.  |
| underpinning contract (UC) | A legally binding contract in place of or in addition to an SLA. This type of contract is with a partner service provider responsible for building service deliverables for the SLA. |

# Acknowledgments

The Microsoft Operations Framework team acknowledges and thanks the people who participated in the development of this guide.

Contributors

Khalid AlHakim, Microsoft

Joe Coulombe, *Microsoft*

Jerry Dyer, Microsoft

Mike Kaczmarek, Microsoft

Don Lemmex, Microsoft

Betsy Norton-Middaugh, Microsoft

Gerard Roth, Microsoft

Writers and Editors

Jude Chosnyk, *GrandMasters*

Ruth Preston, Pultorak & Associates

Pat Rytkonen, Volt Technical Services