

***Mapping ITIL and  
MOF to Regulations  
Using Quest Compliance Suite  
for Windows***

---

Technical Brief

**© Copyright Quest® Software, Inc. 2005. All rights reserved.**

This guide contains proprietary information, which is protected by copyright. The software described in this guide is furnished under a software license or nondisclosure agreement. This software may be used or copied only in accordance with the terms of the applicable agreement. No part of this guide may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying and recording for any purpose other than the purchaser's personal use without the written permission of Quest Software, Inc.

## **WARRANTY**

The information contained in this document is subject to change without notice. Quest Software makes no warranty of any kind with respect to this information. QUEST SOFTWARE SPECIFICALLY DISCLAIMS THE IMPLIED WARRANTY OF THE MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. Quest Software shall not be liable for any direct, indirect, incidental, consequential, or other damage alleged in connection with the furnishing or use of this information.

## **TRADEMARKS**

All trademarks and registered trademarks used in this guide are property of their respective owners.

World Headquarters  
5 Polaris Way  
Aliso Viejo, CA 92656  
[www.quest.com](http://www.quest.com)  
e-mail: [info@quest.com](mailto:info@quest.com)  
U.S. and Canada: 949.754.8000

Please refer to our Web site for regional and international office information.

Updated – September 21, 2005

# CONTENTS

- ABOUT QUEST INFRASTRUCTURE MANAGEMENT..... III**
- ABOUT QUEST SOFTWARE, INC. .... III**
  - CONTACTING QUEST SOFTWARE..... III
  - CONTACTING CUSTOMER SUPPORT ..... IV
- ABSTRACT ..... 5**
- INTRODUCTION TO ITIL AND MOF ..... 6**
- ITIL AND MOF APPLY TO MANY REGULATIONS ..... 7**
- HOW QUEST COMPLIANCE SUITE FOR WINDOWS PRODUCTS ALIGN WITH ITIL AND MOF ..... 14**
- MAPPING QUEST PRODUCTS TO ITIL AND MOF SERVICE MANAGEMENT PROCESSES TO ADDRESS CERTAIN REGULATIONS ..... 16**
- SUMMARY ..... 18**
- APPENDIX A..... 19**
  - ITIL STRUCTURE..... 19
    - 1. *Service Support* ..... 19
    - 2. *Service Delivery* ..... 19
    - 3. *Planning to Implement Service Management* ..... 20
    - 4. *ICT Infrastructure Management*..... 20
    - 5. *Application Management*..... 20
    - 6. *Security Management* ..... 20
    - 7. *Software Asset Management* ..... 21
    - 8. *The Business Perspective*..... 21
  - MOF STRUCTURE ..... 21
    - The MOF Process Model*..... 21
    - Service Management Functions of the Process Model*..... 21
    - The MOF Team Model* ..... 22
    - The Risk Management Discipline*..... 23
  - COMPARING MOF AND ITIL..... 23
    - The ITIL Publication Framework* ..... 24
- APPENDIX B..... 26**
  - ITIL AND MOF SERVICE MANAGEMENT PROCESSES DEFINED AND HOW QUEST SOLUTIONS FIT ..... 26
- NOTES..... 29**



# ABOUT QUEST INFRASTRUCTURE MANAGEMENT

Quest Software, Microsoft's 2004 Global Independent Software Vendor Partner of the Year, provides solutions that simplify, automate, and secure Active Directory, Exchange, and Windows, as well as integrate Linux and Unix into the managed environment. Quest's Infrastructure Management products deliver comprehensive capabilities for secure management, migration, and integration of the heterogeneous enterprise.

## ABOUT QUEST SOFTWARE, INC.

Quest Software, Inc. delivers innovative products that help organizations get more performance and productivity from their applications, databases and infrastructure. Through a deep expertise in IT operations and a continued focus on what works best, Quest helps more than 18,000 customers worldwide meet higher expectations for enterprise IT. Quest Software can be found in offices around the globe and at [www.quest.com](http://www.quest.com).

## Contacting Quest Software

Phone: 949.754.8000 (United States and Canada)

Email: [info@quest.com](mailto:info@quest.com)

Mail: Quest Software, Inc.  
World Headquarters  
5 Polaris Way  
Aliso Viejo, CA 92656  
USA

Web site [www.quest.com](http://www.quest.com)

Please refer to our Web site for regional and international office information.

# Contacting Customer Support

Quest Software's world-class support team is dedicated to ensuring successful product installation and use for all Quest Software solutions.

SupportLink     [www.quest.com/support](http://www.quest.com/support)  
Email at         [support@quest.com](mailto:support@quest.com).

You can use SupportLink to do the following:

- Create, update, or view support requests
- Search the knowledge base
- Access FAQs
- Download patches

# **ABSTRACT**

This technical brief explains the IT Infrastructure Library (ITIL) and Microsoft® Operations Framework (MOF) standards for the management of information technology (IT) best practices. It describes how to utilize these frameworks with certain Quest Software products to address specific government and industry regulations.

## **INTRODUCTION TO ITIL AND MOF**

There are many methodologies and standards for managing IT services. Among the most widely accepted is IT Infrastructure Library (ITIL)<sup>i</sup>, which provides a set of best practices drawn internationally from the public and private sectors. ITIL processes support and are supported by the British Standards Institution's Standard for IT Service Management (BS15000). ITIL was developed and is maintained by the British Office of Government Commerce (OGC).

In keeping with ITIL's spirit to "adopt and adapt," Microsoft has chosen to provide additional, specific guidance, which is applicable to customers using Microsoft technologies within their environments. This approach is called the Microsoft Operations Framework (MOF)<sup>ii</sup> and provides operational guidance that enables organizations to achieve mission-critical system reliability, availability, supportability, and manageability of Microsoft products and technologies. First created in 1999, MOF was designed to complement the well-established Microsoft Solutions Framework (MSF) for solution and application development. With MOF guidance, users can assess their current IT service management maturity, prioritize their processes of greatest concern, and apply proven principles and best practices to optimize their management of the Windows<sup>®</sup> Server platform. Indeed, MOF was built on top of ITIL.

For the purpose of comparison, while ITIL describes IT service management functions, MOF describes these same functions in its Process Model and also expands its guidance with the Team Model and Risk Management Discipline. Together, these combined frameworks provide guidance throughout the IT lifecycle. (A more detailed explanation and comparison of the ITIL and MOF structures is provided in Appendix A.)

The next section of this technical brief identifies certain regulations and emphasizes which IT service management processes, as defined by ITIL and MOF, are applicable to those regulations.

---

## ITIL AND MOF APPLY TO MANY REGULATIONS

Whether supporting the integrity, security, or privacy of data, an IT group can better address its role in an organization's initiative to meet regulations by applying IT management industry standards – such as ITIL and MOF. Figure 1 below shows a sample of regulations, with an emphasis on which ITIL and MOF IT service management processes apply. Following are brief descriptions of these regulations. (For definitions of the IT service management processes, please see the Appendix B.)

- **SOX** – or the Sarbanes-Oxley Act of 2002—was written as a result of high-profile corporate scandals such as the collapse of Enron. The Act introduced legislation intended to rebuild investor confidence in the integrity of corporate disclosures and financial reporting of publicly traded companies by, among other things, ensuring that adequate internal controls over financial reporting are in place.
- **HIPAA** – or the Health Insurance Portability and Accountability Act of 1996—protects health insurance coverage for individuals and their families and enforces standards for privacy, security, and electronic interchange of health information.
- **FISMA** – or the Federal Information Security Management Act of 2002—describes general guidelines for improving the security of federal information systems.
- **Basel II** – aims to improve the consistency of capital regulations internationally, make regulatory capital more risk sensitive, and promote enhanced risk-management practices among large, internationally active banking organizations.
- **GLBA** – or the Gramm-Leach-Bliley Act of 1999—requires all financial institutions to disclose to customers their policies and practices for protecting the privacy of non-public personal information.

**Mapping ITIL and MOF to Regulations Using Quest Compliance Suite for Windows**

**Figure 1: Many regulations can be addressed from an IT perspective by utilizing IT service management processes defined in ITIL and MOF.**

REGULATION  IT SERVICE MANAGEMENT PROCESS	SOX	HIPAA	FISMA	BASEL II	GLBA
<b>Service Desk</b>					
<b>Incident Management</b>	<ul style="list-style-type: none"> <li>• Sec. 404 Assessment of Internal Controls</li> <li>• ISACA’s IT Control Objectives for SOX: Manage Problems and Incidents</li> </ul> <p>“Control Objective – Controls provide reasonable assurance that any problems and/or incidents are properly responded to, recorded, resolved or investigated for proper resolution.”</p>	<ul style="list-style-type: none"> <li>• 164.308(a)(6) Security Incident Procedures</li> </ul>	SP 800-53 <ul style="list-style-type: none"> <li>• Incident Response</li> </ul>	Pillar 1: Minimum Capital Requirements: Operational Risk <ul style="list-style-type: none"> <li>• Incident Management as part of Risk Management</li> </ul>	<ul style="list-style-type: none"> <li>• C.1.f. Monitoring systems and procedures to detect actual and attempted attacks on or intrusions into customer information systems</li> <li>• C.1.g. Response programs that specify actions to be taken when the bank suspects or detects that unauthorized individuals have gained access to customer information systems.</li> </ul>
<b>Problem Management</b>	<p>“Deficiencies in this area could significantly impact financial reporting.”</p>				
<b>Configuration Management</b>	<ul style="list-style-type: none"> <li>• Sec. 404 Assessment of Internal Controls</li> <li>• ISACA’s IT Control Objectives for SOX: Manage Configuration</li> </ul>		SP 800-53 <ul style="list-style-type: none"> <li>• Configuration Management</li> </ul>		<ul style="list-style-type: none"> <li>• C.1.a.a. Access controls on customer information systems, including controls to authenticate and permit access to only authorized individuals and controls to</li> </ul>

REGULATION  IT SERVICE MANAGEMENT PROCESS	SOX	HIPAA	FISMA	BASEL II	GLBA
	<p>“Control Objective – Controls provide reasonable assurance that all IT components – as they relate to security, processing and availability – are well protected, would prevent any unauthorized changes, and assist in the verification and recording of the current configuration.”</p>				<p>prevent employees from providing customer information to unauthorized individuals who may seek to obtain this information through fraudulent means.</p>
<p><b>Change Management</b></p>	<ul style="list-style-type: none"> <li>• Sec. 302 (a)(6) Significant Changes in Internal Controls</li> <li>• ISACA’s IT Control Objectives for SOX: Manage Changes</li> </ul> <p>“Control Objective – Controls provide reasonable assurance that system changes of financial reporting significance are authorized and appropriately tested before being moved to production.”</p>		<p>SP 800-53</p> <ul style="list-style-type: none"> <li>• CM-4 Change Control</li> <li>• CM-6 Change Access Control</li> <li>• CM-7 Monitoring Change Activity</li> </ul>		<ul style="list-style-type: none"> <li>• C.1.d. Procedures designed to ensure that customer information system modifications are consistent with the bank’s information security program.</li> </ul>

**Mapping ITIL and MOF to Regulations Using Quest Compliance Suite for Windows**

REGULATION  IT SERVICE MANAGEMENT PROCESS	SOX	HIPAA	FISMA	BASEL II	GLBA
<b>Release Management</b>					
<b>Service Level Management</b>	<ul style="list-style-type: none"> <li>• Sec. 404 Assessment of Internal Controls</li> <li>• ISACA's IT Control Objectives for SOX: Define and Manage Service Levels</li> </ul> <p>"Control Objective – Controls provide reasonable assurance that service levels are defined and managed in a manner that satisfies financial reporting system requirements and provides a common understanding of performance levels with which the quality of services will be measured."</p>				

REGULATION  IT SERVICE MANAGEMENT PROCESS	SOX	HIPAA	FISMA	BASEL II	GLBA
<b>IT Service Continuity Management</b>	<ul style="list-style-type: none"> <li>• Sec. 404 Assessment of Internal Controls</li> <li>• ISACA's IT Control Objectives for SOX: Manage Operations</li> </ul> <p>"Control Objective – Controls provide reasonable assurance that authorized programs are executed as planned and deviations from scheduled processing are identified and investigated, including controls over job scheduling, processing, <b>error monitoring</b> and system <b>availability</b>."</p>				
<b>Availability Management</b>					
<b>Service Monitoring and Control</b>					
<b>Operations Management</b>					
<b>Capacity Management</b>	<ul style="list-style-type: none"> <li>• Sec. 404 Assessment of Internal Controls</li> <li>• ISACA's IT Control Objectives for SOX: Manage Performance and Capacity</li> </ul>				
<b>Systems Management</b>					

**Mapping ITIL and MOF to Regulations Using Quest Compliance Suite for Windows**

REGULATION  IT SERVICE MANAGEMENT PROCESS	SOX	HIPAA	FISMA	BASEL II	GLBA
<b>Application Management</b>					
<b>Security Management</b>	<ul style="list-style-type: none"> <li>• Sec. 404 Assessment of Internal Controls</li> <li>• Sec. 302 (a)(5)(A)&amp;(B) Deficiencies in Internal Controls</li> <li>• Sec. 302 (a)(6) Significant Changes in Internal Controls</li> <li>• ISACA’s IT Control Objectives for SOX: Ensure Systems Security</li> </ul> <p>“Control Objective – Controls provide reasonable assurance that financial reporting systems and subsystems are appropriately secured to prevent unauthorized use, disclosure, modification, damage or loss of data.”</p>	<ul style="list-style-type: none"> <li>• 164.308(a)(1) Security Management Process</li> <li>• 164.308(a)(4) Information Access Management</li> <li>• 164.308(a)(2) Assigned Security Responsibility</li> <li>• 164.308(a)(3) Workforce Security</li> <li>• 164.308(a)(5) Security Awareness and Training</li> </ul>	<p>SP 800-53</p> <ul style="list-style-type: none"> <li>• Security Planning</li> <li>• Security Control Review</li> <li>• Security Awareness and Training</li> <li>• Personnel Security</li> <li>• Identification and Authentication</li> </ul>	<p>Pillar 1: Minimum Capital Requirements: Operational Risk</p>	<p>Interagency Guidelines Establishing Standards for Safeguarding Customer Information:</p> <ul style="list-style-type: none"> <li>• Must implement an Information Security Program</li> </ul>

REGULATION  IT SERVICE MANAGEMENT PROCESS	SOX	HIPAA	FISMA	BASEL II	GLBA
<b>Software Asset Management</b>			SP 800-53 <ul style="list-style-type: none"> <li>Hardware and Software Maintenance</li> </ul>		
<b>Contingency Planning</b>	<ul style="list-style-type: none"> <li>Sec. 404 Assessment of Internal Controls</li> <li>ISACA's IT Control Objectives for SOX: Manage Data</li> </ul> "Management has implemented a strategy for cyclical backup of data and programs."	<ul style="list-style-type: none"> <li>164.308(a)(7) Contingency Planning</li> </ul>	SP 800-53 <ul style="list-style-type: none"> <li>Contingency Planning and Operations</li> </ul>	Pillar 1: Minimum Capital Requirements: Operational Risk	<ul style="list-style-type: none"> <li>C.1.h. Measures to protect against destruction, loss, or damage of customer information due to potential environmental hazards, such as fire and water damage or technological failures.</li> </ul>
<b>Storage Management</b>	<ul style="list-style-type: none"> <li>Sec. 802 Long-term retention of records relevant to audits and reviews</li> </ul>			Must store historical data for long periods of time	

# HOW QUEST COMPLIANCE SUITE FOR WINDOWS PRODUCTS ALIGN WITH ITIL AND MOF

Certain Quest Software products help support specific IT service management processes in ITIL and MOF to address certain regulations. Figure 2 shows a combination of ITIL and MOF processes (leaving out the Microsoft-specific paragraphs from the MOF Process Model) and identifies which Quest Compliance Suite for Windows products support which IT service management processes. Quest products currently included in Compliance Suite for Windows are Quest Reporter, Quest InTrust for Windows and Quest InTrust for Active Directory.

**Reporter** allows administrators to collect, store, and report on network security and file permissions-related data. This enables configuration change auditing, a security assessment of the Windows infrastructure, and Active Directory pre- and post-migration analysis, thereby baselining the environment.

**InTrust for Windows** helps administrators collect, efficiently store, and report on event data, and also alert on business-critical events, to meet the needs of external regulations and internal policies.

**InTrust for Active Directory** provides comprehensive auditing of all changes to Active Directory and Group Policy—without the overhead of native auditing. InTrust for Active Directory also proactively prevents changes to the most critical objects and takes corrective action for undesired changes.

**ActiveRoles Server** automates user provisioning, reprovisioning, and deprovisioning in Active Directory, Exchange, and Windows. With role-based security, HR and ERP system integration, automated group management, Active Directory structure reporting, ActiveRoles Server provides a practical approach to complete user lifecycle management for the Windows enterprise.

**Figure 2: ITIL and MOF intersection matrix and alignment with Quest Compliance Suite for Windows products**

ITIL	MOF	QUEST COMPLIANCE SUITE FOR WINDOWS PRODUCTS
Service Desk	Service Desk	ActiveRoles Server
Incident Management	Incident Management	InTrust for Windows InTrust for Active Directory
Problem Management	Problem Management	InTrust for Windows InTrust for Active Directory
Configuration Management	Configuration Management	Reporter ActiveRoles Server

ITIL	MOF	QUEST COMPLIANCE SUITE FOR WINDOWS PRODUCTS
Change Management	Change Management	InTrust for Active Directory InTrust for Windows
Release Management	Release Management	
Service Level Management	Service Level Management	
Financial Management for IT Services	Financial Management	
IT Service Continuity Management	IT Service Continuity Management	
Availability Management	Availability Management	
Contingency Planning		
Capacity Management	Capacity Management	
Network Service Management		
Operations Management	Job Scheduling	
Management of Local Processors		
Computer Installation and Acceptance		
Systems Management	System Administration	
Application Management		
Security Management	Security Management Security Administration	InTrust for Windows InTrust for Active Directory Reporter ActiveRoles Server
Software Asset Management		Reporter
	Workforce Management	
	Infrastructure Engineering	
	Directory Services Administration	
	Service Monitoring and Control (Health monitoring)	
	Storage Management	InTrust for Windows InTrust for Active Directory
	Risk Management	

# MAPPING QUEST PRODUCTS TO ITIL AND MOF SERVICE MANAGEMENT PROCESSES TO ADDRESS CERTAIN REGULATIONS

Figure 3 shows that Quest Compliance Suite for Windows products map to ITIL and MOF IT services management processes in specific areas. Using these products to address these service management processes can help an IT organization better understand the gaps in achieving compliance with external regulations.

**Figure 3: ITIL and MOF service management processes fulfilled by Quest solutions, and their application to certain regulations.**

REGULATION \ IT SERVICE MANAGEMENT PROCESS	SOX	HIPAA	FISMA	BASEL II	GLBA
<b>Reporter</b>	<ul style="list-style-type: none"> <li>• Configuration Management</li> <li>• Security Management</li> </ul>	<ul style="list-style-type: none"> <li>• Security Management</li> </ul>	<ul style="list-style-type: none"> <li>• Configuration Management</li> <li>• Security Management</li> <li>• Software Asset Management</li> </ul>		<ul style="list-style-type: none"> <li>• Configuration Management</li> <li>• Security Management</li> </ul>
<b>InTrust for Active Directory</b>	<ul style="list-style-type: none"> <li>• Incident Management</li> <li>• Problem Management</li> <li>• Security Management</li> <li>• Storage Management</li> <li>• Change Management</li> </ul>	<ul style="list-style-type: none"> <li>• Incident Management</li> <li>• Problem Management</li> <li>• Security Management</li> </ul>	<ul style="list-style-type: none"> <li>• Incident Management</li> <li>• Problem Management</li> <li>• Security Management</li> <li>• Change Management</li> </ul>	<ul style="list-style-type: none"> <li>• Incident Management</li> <li>• Problem Management</li> <li>• Security Management</li> </ul>	<ul style="list-style-type: none"> <li>• Incident Management</li> <li>• Problem Management</li> <li>• Security Management</li> <li>• Change Management</li> </ul>

REGULATION  IT SERVICE MANAGEMENT PROCESS	SOX	HIPAA	FISMA	BASEL II	GLBA
<b>InTrust for Windows</b>	<ul style="list-style-type: none"> <li>• Incident Management</li> <li>• Problem Management</li> <li>• Security Management</li> <li>• Storage Management</li> <li>• Change Management</li> </ul>	<ul style="list-style-type: none"> <li>• Incident Management</li> <li>• Problem Management</li> <li>• Security Management</li> </ul>	<ul style="list-style-type: none"> <li>• Incident Management</li> <li>• Problem Management</li> <li>• Security Management</li> <li>• Change Management</li> </ul>	<ul style="list-style-type: none"> <li>• Incident Management</li> <li>• Problem Management</li> <li>• Security Management</li> </ul>	<ul style="list-style-type: none"> <li>• Incident Management</li> <li>• Problem Management</li> <li>• Security Management</li> <li>• Change Management</li> </ul>
<b>ActiveRoles Server</b>	<ul style="list-style-type: none"> <li>• Security Management</li> <li>• Configuration Management</li> </ul>	<ul style="list-style-type: none"> <li>• Security Management</li> </ul>	<ul style="list-style-type: none"> <li>• Security Management</li> <li>• Configuration Management</li> </ul>	<ul style="list-style-type: none"> <li>• Security Management</li> </ul>	<ul style="list-style-type: none"> <li>• Security Management</li> <li>• Configuration Management</li> </ul>

## **SUMMARY**

Nearly every company is faced with achieving compliance with external regulations. Understanding the impact that the IT organization has in helping the company achieve compliance is important. IT organizations must align themselves with best practices, like ITIL and MOF, in order to establish the proper framework to address compliance-related IT audits. Fortunately, Quest Software can help map the processes in such best practices to address certain regulations. For more information on how we can help, please visit us on the Web at <http://wm.quest.com/compliance>.

# APPENDIX A

## ITIL Structure

ITIL is broken up into eight publications with respective topics:

### 1. Service Support

Service Support focuses on ensuring that the customer has access to appropriate services to support business functions. Issues covered include:

- Service Desk
- Incident Management
- Problem Management
- Configuration Management
- Change Management
- Release Management

It expands the necessary interactions between these and other core IT service management disciplines, and updates best practice to reflect recent changes in technology and business practices.

### 2. Service Delivery

Service providers need to offer business users adequate support. Service Delivery covers all aspects that must be taken into consideration. Issues covered include:

- Service Level Management
- Financial Management for IT Services
- IT Service Continuity Management
- Availability Management
- Contingency Planning
- Capacity Management

The purpose of Service Delivery is to show the links and the principal relationships between all the Service Management and other Infrastructure Management processes.

### **3. Planning to Implement Service Management**

This book answers the question, “Where do I start with ITIL?” It explains the steps necessary to identify how an organization might expect to benefit from ITIL and how to set about reaping those benefits. It also helps organizations identify their strengths and weaknesses, enabling them to develop the former and overcome the latter.

### **4. ICT Infrastructure Management**

ICT Infrastructure Management is concerned with the processes, organization, and tools needed to provide a stable IT and communications infrastructure, and is the foundation for ITIL service management processes. Issues covered include:

- Network Service Management
- Operations Management
- Management of Local Processors
- Computer Installation and Acceptance
- Systems Management

### **5. Application Management**

This book embraces the Software Development Lifecycle. Applications Management also provides more detail on Business Change, with emphasis on clear requirement definition and implementation of solutions.

### **6. Security Management**

This is a recently published ITIL guide that explains the process of security management with IT service management. The guide focuses on the process of implementing security requirements identified in the IT Service Level Agreement, rather than considering business issues of security policy. The book was developed taking into consideration the plans for consolidating and inter-linking the ITIL Service Support and Service Delivery core guides.

## 7. Software Asset Management

Software is one of the most critical elements of information and communications technologies, and most organizations have huge investments in software, whether internally developed or externally procured. However, organizations often do not invest commensurate effort into managing these software assets. This guide has been developed to assist with the understanding of what Software Asset Management (SAM) is and to explain what is required to perform it effectively and efficiently, as identified in industry best practices.

## 8. The Business Perspective

This book is concerned with helping business managers to understand IT service provision. Issues covered include business relationship management, partnerships and outsourcing, and continuous improvement and exploitation of Information, Communication and Technology (ICT) for business advantage.

## MOF Structure

Like ITIL, MOF describes the same IT service management functions (SMFs) in its Process Model, and provides expanded guidance with the Team Model and Risk Management Discipline.

### The MOF Process Model

The *MOF Process Model* provides a functional blueprint and description of the processes that operations teams perform to manage and maintain IT services. It assumes that the operations group's main responsibility is managing change in the IT environment. The most effective way to deal with change throughout the lifespan of a service is to group related changes together into a package called a release, so that the changes can be planned and managed as a unit. The *MOF Process Model* describes a lifecycle that can be applied to any release, and the processes and activities that make up each part of that lifecycle.

### Service Management Functions of the Process Model

The Process Model consists of the service management functions. Each of the SMFs within a particular quadrant shares a common mission of service, or goal. Many of the SMFs are based on the OGC's IT Infrastructure Library. The notable exceptions are Workforce Management (in the Optimizing Quadrant) and all SMFs in the Operating Quadrant. Because ITIL is platform-independent, it does not cover these items. SMFs are best practices and typically require customization to address unique or specific requirements of a particular operations environment.

## Mapping ITIL and MOF to Regulations Using Quest Compliance Suite for Windows

The SMFs and the quadrants they belong to are shown in the following diagram.



## The MOF Team Model

The *Team Model for Operations* paper provides best practices based on the Microsoft Operations Framework approach, combined with the experience of Microsoft IT groups, customers, and partners. It provides guidance on how to structure IT operations teams to achieve greater efficiency and synergy. This document describes:

- Guiding principles that help operate and maintain distributed computing environments on the Microsoft platform.
- Best practice role clusters for structuring operations teams.
- The key activities and competencies of each role cluster.
- How to scale the teams for different sizes and types of organizations.
- The roles that can be combined effectively.
- How the MOF Team Model relates to the Microsoft Solutions Framework (MSF) Team Model.

The *Team Model for Operations* paper serves as a guide to team roles and functions in all other MOF-based content, including the SMF guides and service offerings created for partners and customers to use when managing and running solutions on the Microsoft platform.

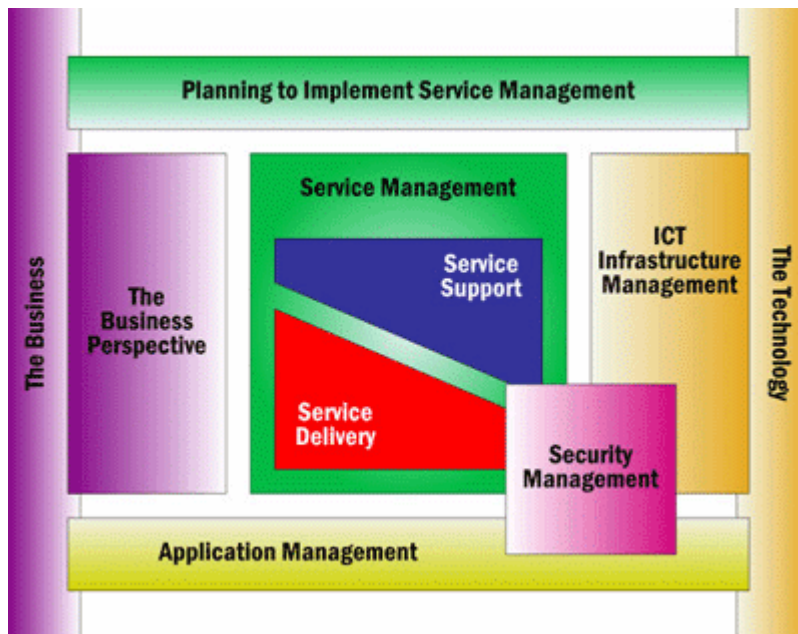
## The Risk Management Discipline

The *Risk Management Discipline* paper explains that risk management has become more important and more difficult. It describes the risk management discipline for operations as a process for managing risks with a proactive approach that embeds risk management practices into every IT operations role, process, and review. This paper concludes with examples of how risk management can be applied to real-world operations.

## Comparing MOF and ITIL

MOF aligns and builds on the IT service management practices that have been documented within ITIL maintained by the OGC. The OGC is a U.K. government executive agency chartered with development of best-practice advice and guidance on the use of information technology in service management and operations. Microsoft has been actively involved with the ITIL community since 1999, both using the ITIL content and contributing to new and updated documentation, including co-authoring several books.

ITIL currently includes more than 40 books. Of these, 10 are of particular significance to a corporate IT organization. The following figure illustrates these ten titles and their relationships.



## **The ITIL Publication Framework**

Each of these ITIL publications is devoted to a function of IT service management and contains cross-references to its companion publications.

One goal of MOF is to extend and enhance the practices and guidance offered through ITIL in order to provide more detailed prescriptive guidance in specific areas of IT management.

MOF is similar to ITIL in several ways:

- MOF (in conjunction with MSF) spans the entire IT lifecycle.
- MOF is based on best practices for IT management, drawing on the expertise of an international group of practitioners, including Microsoft World Wide Services, Microsoft Partners, Microsoft customers, and the internal (and extensive) Microsoft IT operations group.
- The MOF body of knowledge is applicable across the business community—from small business to enterprise. MOF is not just for those operating on the Microsoft platform within homogenous environments.
- Like ITIL, MOF has expanded to include more than just a documentation set. MOF is a core component of the MSIM solution accelerators, ensuring that solutions are operable in your IT environment, post-deployment. Furthermore, a variety of resources have been developed to support MOF principles and guidance, including self-assessments, IT management tools that incorporate MOF terminology and features, training programs and certification, and consulting services. These are offered by numerous third-party vendors and consultants.

MOF expands upon and extends ITIL through the following:

- Addition of the MOF Team and Process models and Risk Management discipline (summarized subsequently within this document).
- Simplification of IT processes into a diagrammatic model, with all components and their relationships visible at a glance.
- Focus on the service-delivery level of IT management, rather than on IT operations in their entirety. For example, ITIL identifies individual service functions such as Service Level Management and Capacity Management; these are described within the ITIL Service Delivery publication. In contrast, MOF individually recognizes more than 20 service delivery functions and devotes an entire publication to each of them, providing descriptions, examples, and best practice guidance.
- Combination of ITIL collaborative industry standards with specific guidelines for using Microsoft products and technologies.
- Scalability of MOF guidance and principles from implementation within a single service to implementation across a high-order structure such as a data center or entire operations environment. MOF also extends the ITIL code of practice to support distributed IT environments and industry trends such as application hosting and Web-based transactional and e-commerce systems.

## APPENDIX B

# ITIL and MOF Service Management Processes Defined and how Quest Solutions Fit

**Service Desk** serves to provide a single point of contact for customers and to facilitate the restoration of normal operational service with minimal business impact on the customer within agreed service levels and business priorities.

**Incident Management** is a critical process that provides organizations with the ability to first detect incidents and then target the correct support resources in order to resolve the incidents as quickly as possible.

InTrust for Active Directory and Windows both provide real-time alerts in the case of violations against policies or procedures. These alerts can be sent to specific persons within the organization with a detailed explanation of what happened and what actions must be taken. The alerts are also equipped with scripts which can disable or stop the intruder or application in their tracks.

**Problem Management.** By implementing Problem Management processes at the same time as Incident Management processes, organizations can identify and resolve the root causes of any significant or recurring incidents, thus reducing the likelihood of recurrence.

InTrust for Active Directory and Windows both provide network scalable data collections and long term data storage. This allows the organization to run a complete collection of data across the entire network at the time of the incident, when gathering the data is most critical. The data is stored in such a way that it can be easily consolidated to one location. This allows administrators to retrace the actions leading up to the incident and look for trends or specific actions. This helps administrators to be more proactive in preventing this from happening in the future.

**Configuration Management** is a critical process responsible for identifying, controlling, and tracking all versions of hardware, software, documentation, processes, procedures, and all other inanimate components of the IT organization.

Quest Reporter enables administrators to collect all Windows server based information such as hardware, software and registry information.

**Change Management** describes a consistent set of processes to initiate infrastructure changes, assess and document their potential impacts, approve their implementation, and schedule and review their deployment.

**Release Management** creates a bridge between development or acquisition of new services and the IT organization responsible for operating them. Release Management coordinates efforts to deploy services and applications into a managed environment.

**Service Level Management** is the primary management of IT services, ensuring that agreed services are delivered when and where they are supposed to be delivered.

**Financial Management for IT Services** is the discipline of calculating the cost of providing IT services, so an organization can understand these costs, and ensuring that the IT infrastructure is obtained at the most effective price (which does not necessarily mean cheapest).

**IT Service Continuity Management** provides best practices and guidance to support business continuity through the implementation of effective IT service recovery procedures.

**Availability Management** is concerned with design, implementation, measurement and management of IT services, to ensure that the stated business requirements for availability are consistently met.

**Service Monitoring and Control** provides best practices for monitoring and resolving incidents and alerts in the production environment.

**Capacity Management** works to optimize capacity and improve system performance through planning, sizing and controlling network resources as efficiently as possible.

**Operations Management** has a strong technology focus with an emphasis on monitoring and control. Operations management is of an observing, serving and operational nature, ensuring the stability of the Information and Communication Technologies infrastructure.

**Systems Management** is concerned with providing an in-depth pool of technical advice. Systems management also provides guidance and resources for the support and maintenance of all aspects of the ICT Infrastructure.

**Application Management** addresses the complex subject of managing applications from the initial business need, through the Application Management lifecycle, up to and including retirement.

**Security Management** is the process of managing a defined level of security on information and IT services. Included in the scope of security management is managing the reaction to security incidents.

The Quest Compliance Suite enables organizations to automate the collection of data which allows administrators to track and verify that security models and levels are being adhered to. In the case of business critical incidents InTrust for Active Directory and Windows provides real-time alerts for quicker response.

## **Mapping ITIL and MOF to Regulations Using Quest Compliance Suite for Windows**

---

**Software Asset Management** relates to the infrastructure and processes required for the effective management, control, and protection of software assets within an organization, throughout all lifecycle stages.

Quest Reporter enables administrators to collect and report on all software which is installed on a Windows platform server.

**Contingency Planning** is the process of ensuring that IT Services can continue if a serious incident occurs. Clearly, this is a fundamental part of service management.

**Storage Management** is the set of practices dedicated to safe, secure storage of data, effective backup-and-restore policies, and efficient use of storage resources, to optimize the business's investment in physical storage components.

InTrust for Active Directory and Windows both provide safe and secure storage capabilities. The collected data is compressed and encrypted before being sent across the line. This data stays in its compressed state at rest and can be stored on basic disk space. The data is compressed at a 40:1 ratio thus greatly decreasing the amount of space needed for long term storage and allowing organizations to see an immediate ROI. Normal backup procedures can be used for data backup and recovery. The stored data is kept in its native format which means it's admissible in a court of law increasing its value.

## NOTES

- i. [www.ogc.gov.uk/index.asp?id=2261](http://www.ogc.gov.uk/index.asp?id=2261)
- ii. [www.microsoft.com/technet/itsolutions/cits/mo/mof/default.mspix](http://www.microsoft.com/technet/itsolutions/cits/mo/mof/default.mspix)