



Microsoft
Your potential. Our passion.™



Focused on Security.
Committed to Success.

U.S. National Security Team White Paper

Enabling Secure Collaboration for Professional Services Firms

Produced by the Microsoft U.S. National Security Team

Prepared by Martin Grasdal, CISSP, MCSE

Co-authored by Shirley Wyatt, Strategic Security Advisor, and Elliott Ichimura, Industry Manager

Published: June 2007

Abstract

This white paper describes the challenges that professional services firms experience around document collaboration and security, both within their own organizations and with client organizations. The focus of this paper is to provide information on and guidance for leveraging Microsoft® technologies, both current and next generation, to help professional service firms improve document management and collaboration, and, by so doing, maximize the value of their intellectual capital, develop stronger business relationships with clients, improve productivity, meet regulatory requirements and achieve other significant benefits.

About the U.S. National Security Team (NST)

The US National Security Team is composed of strategic security advisors who work with Microsoft customers, partners, MS internal constituencies and the information security industry to promote the adoption of security processes and technologies. Its goal is assist customers and partners to increase their security awareness and implementation to create more secure businesses, mitigate risk, and make Security cost of ownership more effective. Its activities are informed by three simple tenets: protect the consumer, secure the enterprise, and enable developers to write secure code.

As part of its mandate, in addition to producing white papers such as this one, the NST is responsible for developing and executing security-focused events and Security Round Tables across Microsoft's U.S. geographies. These events include the annual CSO Summit, which provides formal feedback to business groups, security industry updates from leading analysts, peer perspectives on security management from MSIT, and updates on the latest initiatives and industry trends in enterprise security.

The NST also focuses on driving vertical security solutions for a wide range of industries. To this end, the NST has produced a number of white papers that address the specific security needs of particular industries, such as the professional services and financial services industries.

The information contained in this document represents the current view of Microsoft Corporation on the issues discussed as of the date of publication. Because Microsoft must respond to changing market conditions, it should not be interpreted to be a commitment on the part of Microsoft, and Microsoft cannot guarantee the accuracy of any information presented after the date of publication.

This White Paper is for informational purposes only. MICROSOFT MAKES NO WARRANTIES, EXPRESS, IMPLIED OR STATUTORY, AS TO THE INFORMATION IN THIS DOCUMENT.

Complying with all applicable copyright laws is the responsibility of the user. Without limiting the rights under copyright, no part of this document may be reproduced, stored in or introduced into a retrieval system, or transmitted in any form or by any means (electronic, mechanical, photocopying, recording, or otherwise), or for any purpose, without the express written permission of Microsoft Corporation.

Microsoft may have patents, patent applications, trademarks, copyrights, or other intellectual property rights covering subject matter in this document. Except as expressly provided in any written license agreement from Microsoft, the furnishing of this document does not give you any license to these patents, trademarks, copyrights, or other intellectual property.

© 2006 Microsoft Corporation. All rights reserved.

Microsoft, Forefront, Antigen, Excel, SharePoint, Windows, Windows Server System, and the Windows Server System logo are either registered trademarks or trademarks of Microsoft Corporation or Sybari Software, Inc. in the United States and/or other countries. Sybari Software, Inc. is a subsidiary of Microsoft Corporation.

All other trademarks are property of their respective owners.

Microsoft

Contents

Introduction	5
Overview of Secure Collaboration Challenges and Business Drivers	7
Defining a Framework for Best Practices in Secure Collaborative Environments	9
Infrastructure Optimization.....	10
Optimization Collaboration Scenario	12
Background.....	12
Network Infrastructure Security: Defense in Depth.....	15
Patch Management	15
Anti-Virus and Anti-Malware Protection	16
Confidentiality, Integrity and Authentication Controls	17
Service Management and Monitoring	18
Edge Protection.....	18
Sample Engagement	21
Client Work Acceptance Process.....	22
Proposal Creation Process.....	25
Contract Creation and Agreement Process	29
Project Planning and Initiation.....	36
Product Development.....	41
Product Delivery	51
Project Closure.....	56
Conclusion	60
Appendix A: What Are Professional Service Firms?	62
Intra-Organizational Challenges Faced by Professional Service Firms for Secure Collaboration	63
Inter-Organizational Challenges Faced by Professional Service Firms for Secure Collaboration	65
Ethical, Regulatory and Legal Obligations.....	65
Summary of Technological Challenges for Inter-Organizational Collaboration.....	67
Appendix B: Overview of Compliance and Government Regulations	69
Consequences of Non-Compliance	69
Common Characteristics of Regulatory Compliance	70
Summary of Key Compliance Regulations	72

Appendix C: General Overview of the Infrastructure Optimization Model: Basic, Standardized, Rationalized and Dynamic	75
Appendix D: Resources and References	82
Infrastructure Optimization Model	82
Regulatory Compliance with Microsoft Products	83
Regulatory Compliance and IT Control Frameworks.....	84
Product Resources and White Papers.....	85
Developer and Architect Resources	86
Security Resources	88

Introduction

When professional service firms deploy collaboration solutions that allow them to leverage their intellectual capital and know-how more efficiently and securely, their employees can more easily and effectively focus on providing clients with the benefits of knowledge, experience and professional judgment that cannot be easily codified, and thus better realize value for clients and the firm.

This white paper provides information on the business and technical opportunities provided by Microsoft® methodologies and technologies to improve collaboration, information management and security, both within the organization and across organizational boundaries. Improving collaboration and management within a professional services firm will help it realize a number of significant advantages, including the following:

- Increase employee productivity
- Improve employee job satisfaction
- Better realize the value of intellectual capital
- Increase security of data and information
- Improve compliance with laws, rules, contracts, ethical obligations, etc.,
- Enable a mobile workforce
- Mitigate loss and leakage of information
- Improve business relationships

In general, by leveraging the potential that current and future Microsoft® technologies can offer, professional service firms can achieve a competitive advantage that will distinguish them in the marketplace.

The intended audience for this paper includes CIOs, CISOs, IT Directors and others who need to understand and deliver the solutions that will extend and improve management and collaboration capabilities to facilitate improved compliance, improved security, better relationships with clients and partners, and improved employee productivity.

This paper showcases a wide range of products and technologies and, despite its length, takes a high-level approach. However, to assist readers in achieving a better understanding of the possibilities offered by the showcased products and technologies, this paper provides supplementary information throughout in the form of appendices, notes, references and in-line explanations. Because of this ancillary content, IT professionals and other technology specialists also will find relevant information that will help them gain a deeper understanding of the capabilities for providing solutions and extending the benefits of these technologies.

The white paper starts with an overview of the challenges and business issues that professional service firms commonly face. The purpose of this section is to situate the challenges of inter- and intra-organization collaboration within not just a technological and security context, but also within an ethical and professional context, regarding the obligations that professional service firms have toward their clients.

Forming the core of this white paper is a detailed narrative to illustrate a possible set of collaboration, security and optimization solutions that rely on Microsoft technologies. A number of extended usage scenarios comprise the narrative structure. The scenarios show the typical steps of a professional services firm engagement from project initiation to completion. Throughout these usage scenarios, technology is presented as serving particular business needs. A secondary goal of this narrative approach is to assist readers in seeing the benefits of Microsoft technologies as organic and integral elements of the deployment of these technologies.

The usage scenarios also present technology as serving the goals of Microsoft's Infrastructure Optimization Model (IOM). Achieving business, security and compliance requirements on the part of professional service firms and other organizations involves the orchestration of a large number of complex and interrelated elements. Furthermore, these requirements must be achieved in such a way that IT is ultimately more closely aligned with and serves the business needs of the organization so that the benefits are ongoing and reduce costs. The IOM provides framework guidance for organizations that need to tackle this complex undertaking.

The appendices that comprise the remainder of the white paper provide additional information for those who seek more information on some of the topics presented here.

Appendix A provides background information on the nature of professional service firms and a more complete description of challenges they face for inter- and intra-organizational collaboration.

Appendix B provides information on some of the common regulatory and legislative compliance requirements that professional service firms are subject to, depending on their scope of practice and activities.

Appendix C provides a more complete summary of the Infrastructure Optimizations Model.

Finally, **Appendix D** provides a list of resources that may be useful to those who seek a deeper understanding of the topics discussed in this white paper.

Overview of Secure Collaboration Challenges and Business Drivers

Professional service firms face myriad challenges meeting internal business needs and requirements, as well as external requirements arising from the activities they perform for their clients. An increasingly regulated environment and a bewildering array of recent legislation complicate these challenges profoundly and add significant cost to organizations. Professional service firm clients, for example, also experience these increased costs in the form of fees to perform mandated audits. A consequence of this is increasing pressure to control and reduce costs. In a competitive marketplace, professional service firm clients want to see more value for their fees; at the same time, professional service firms must find ways to achieve greater business efficiencies.

Knowledge, expertise and professional judgment are the lifeblood of professional service firms. And, the value of a professional service firm primarily resides in its intellectual capital, in the form of captured and codified knowledge and its personnel.

A key goal of professional service firms is to improve their ability to leverage their intellectual capital. By increasing their store of intellectual capital and by providing easier access to that capital, professional service firms can add value and reduce costs. The realization of these benefits is a natural consequence of improving intra- and inter-organizational communication and collaboration.

However, the need to impose controls to meet business, regulatory, security, ethical and other requirements can become a barrier to efficient communication and collaboration.

Professional service firms must find a balance between openness and transparency of communications to enable efficient collaboration and the need to protect confidential, proprietary and private information. In general, this balance needs to be achieved in such a way that accountability and security through technological controls is maximized at the same time as user acceptance, employee productivity and client satisfaction is increased. The ultimate goal is to provide persistent protection of information without impeding communication, collaboration or the flow of information.

Some of the specific business needs and challenges include:

- Facilitating effective intra- and inter-organizational collaboration in a wide variety of forms, whether online, offline, synchronous, asynchronous, centralized or decentralized
- Codifying, storing, organizing and indexing information from across the enterprise, including disparate and heterogeneous systems
- Ensuring information retention policies are met to ensure appropriate and compliant disposition
- Providing the means for employees to find, use and revise relevant information easily and, by so doing, improve employee productivity and job satisfaction by reducing the amount of manual clerical activity around document management
- Imposing controls and policies on information access within the organization, and improving security of the information to ensure compliance with regulation.
- Ensuring that ethical obligations (such as the fiduciary duty professional service firms owe their clients) are enforced as much as possible with technological controls.

- Providing appropriate workflows to ensure compliance with business rules to mitigate loss of data and ensure information integrity
- Providing robust and accurate auditing and logging of information access
- Meeting regulatory compliance requirements, such as the Sarbanes Oxley Act (SOX).
- Enabling mobile workers to work collaboratively regardless of their network context, online or offline.
- Mitigating loss or leakage of intellectual capital
- Improving user acceptance of collaboration, security and other solutions to ensure greater compliance with internal controls and business rules¹

¹ For a more complete description of the needs and challenges that professional service firms face, please see Appendix A of this document.

Defining a Framework for Best Practices in Secure Collaborative Environments

Microsoft continues to improve its solution scenarios for secure collaboration in the professional services through recent and future product releases, guidance and industry partnerships. These solutions leverage Windows® Vista™, Microsoft Office SharePoint® Server 2007, Exchange Server 2007, Office System 2007, Microsoft Systems Center 2007 and Forefront™ security solutions, among other products.

To take full advantage of the benefits of intra- and inter- organizational collaboration, professional services firms can benefit by moving their infrastructure to these new products. By doing so, professional services firms may be able to reduce the costs associated with collaboration while at the same time achieving better compliance with legislation and industry-specific regulation.

Professional services firms will need to go through design, testing and budget procurement cycles and will need to develop transition plans (including training, documentation, etc.) for new product deployments. In the meantime, these firms can leverage their current infrastructure to better enhance collaboration and compliance, and to provide a smoother pathway to Microsoft product offerings, when they are in a position to upgrade their infrastructure.

Every professional services firm will be unique in the mix of products and solutions that it has deployed in an effort to meet its business, regulatory and ethical requirements. To greater or lesser degrees, these solutions are likely to be based on Microsoft products. For example, most organizations are standardized on a Windows® platform and applications: Windows 2000 Professional and Windows XP for the desktop OS, Windows 2000 Server and Windows Server® 2003 for the server OS, and Office XP or Office 2003 for desktop productivity applications.

However, there is greater divergence among professional services firms in their mix of products for messaging, collaboration, regulatory compliance and business process solutions.

Many organizations may use applications and platforms other than SharePoint or Exchange Server for document management and collaboration and messaging. In many cases, organizations may have developed custom applications or purchased third-party applications to provide Web portals for document and knowledge management. To meet SOX, tax planning and other regulatory and ethical requirements, organizations will use a wide variety of applications, many of which came from ISVs or are built in-house.

This complexity makes it difficult for professional services firms to meet their own and their clients' needs. There is, for example, the need to integrate diverse platforms and applications and to align the functionality of those applications and platforms with business processes or regulatory compliance needs.

It's also difficult to describe an environment that is currently "typical" for all professional services firms, in terms of product-specific solutions. Despite this fact, however, all professional services firms tend to share common goals and functionality in their implementation of solutions to meet needs for secure information collaboration. These common goals and functionality can be expressed as a framework model that describes the ultimate goals in terms of levels of maturity that also comprise standards for best practices.

Infrastructure Optimization

The challenge for professional service firms to achieve a state where their business processes are aligned with the IT infrastructure is a complex challenge. To assist customers in meeting this challenge, Microsoft provides guidance in the form of the Infrastructure Optimization Model (IOM), which forms a core part of Dynamic Systems Initiative.²

Microsoft's Infrastructure Optimization Model is related to the Information Technology Infrastructure Library (ITIL). It is based on models proposed by the Gartner Group and MIT, and a distillation of Microsoft's experience in managing its own infrastructure and assisting its enterprise customers, as codified in the Microsoft Operations Framework (MOF).

The IOM describes four levels of increasing infrastructure and business process maturity: basic, standardized, rational and dynamic. In very general terms, the IOM defines the characteristics of each level (basic, standardized, rational and dynamic) as a function of the degree of automation, security, usability and utility inherent within the IT infrastructure and the degree to which that IT infrastructure is aligned with and serves the needs of the business. As each level of maturity is achieved, organizations realize significant benefits, such as lower and more controlled costs associated with their IT infrastructure.³

Professional service firms can leverage the IOM to provide guidance and functional descriptions of the business goals for secure information and collaboration.

The Infrastructure Optimization Model can be viewed from three main perspectives: application platforms, business productivity and core infrastructure optimization. Each perspective has its own set of specific requirements. The following graphic provides a high-level overview of core infrastructure optimization.⁴

² For more information on the Dynamic Systems Initiative, see the [DSI Overview](http://www.microsoft.com/business/dsi/default.aspx) white paper at <http://www.microsoft.com/business/dsi/default.aspx>.

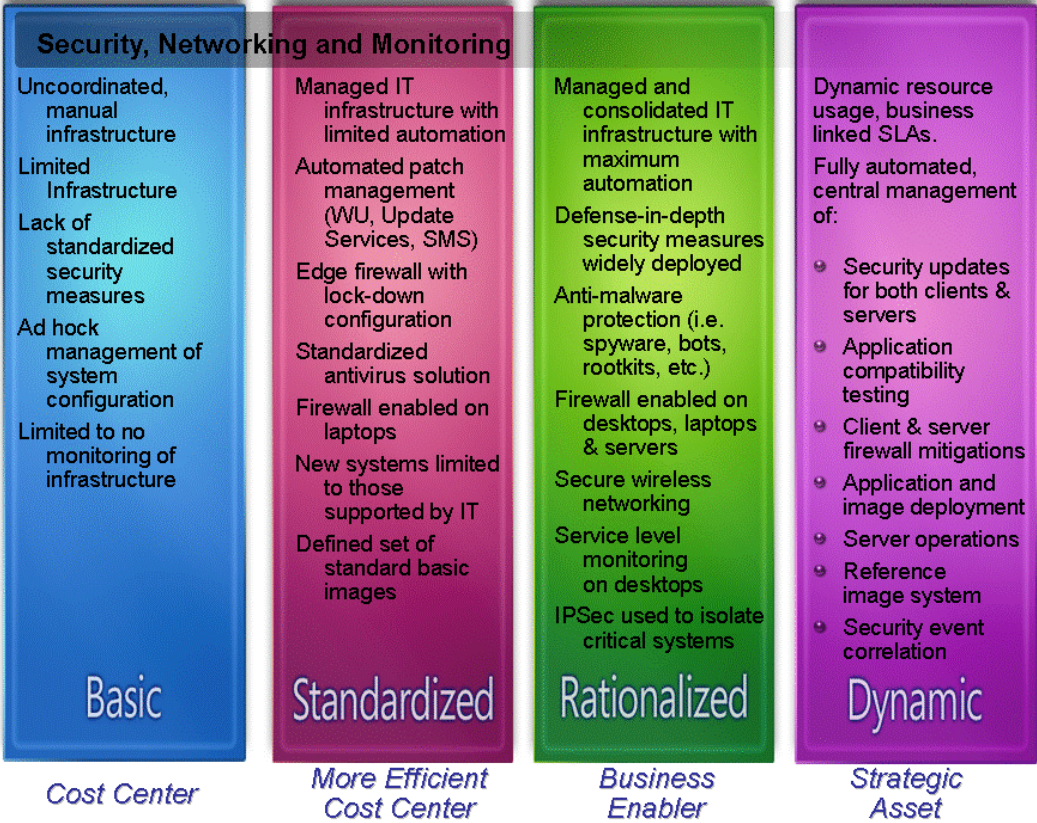
³ For example, according to Gartner, a managed PC of a 2,500-seat organization typically costs approximately \$4,600–\$5,000 per year, with 13 percent of the cost being labor. A Microsoft-commissioned study shows that by moving from a Basic to Rationalized infrastructure, organizations can reduce IT costs by up to \$513 per PC. For more information on these metrics and the cost benefits of infrastructure optimization, please see the white paper, *Infrastructure Optimization: Driving Down the Costs of the Business Desktop* at <http://www.microsoft.com/technet/infrastructure/bestpractices.aspx>.

⁴ For more information on the Infrastructure Optimization Model, please see Appendix C and Appendix D of this white paper.

General Overview of Core Infrastructure Optimization



Increasing levels of automation, service delivery, communications, and security



Optimization Collaboration Scenario

To provide a more immediate sense of how infrastructure optimization affects the collaborative and compliance ecosystems of professional services firms, the following section presents a number of scenarios that illustrate typical challenges and benefits that organizations experience, based on optimization levels and their collaboration and business requirements.

Note: *Although many solutions described below are available out-of-the box, some of the following scenarios require custom solutions that can be built in-house or acquired from Microsoft Partners.*

Background

Contoso Consulting Services is a multi-disciplinary professional services firm that provides accounting, audit and management consulting. The firm provides its services to a wide range of industries, including petrochemical, manufacturing, telecom, power generation, IT services and governments. The majority of its work force is located in the continental U.S.; however, it also has offices in Canada and Europe.

A few years ago, Contoso identified a number of problem areas that restricted its ability to conduct its business efficiently and in a cost-effective and secure manner. From the perspective of the Infrastructure Optimization Model, the company operated primarily at the basic level, but was well on its way to the standardized level. Specifically, the following problem areas were identified:

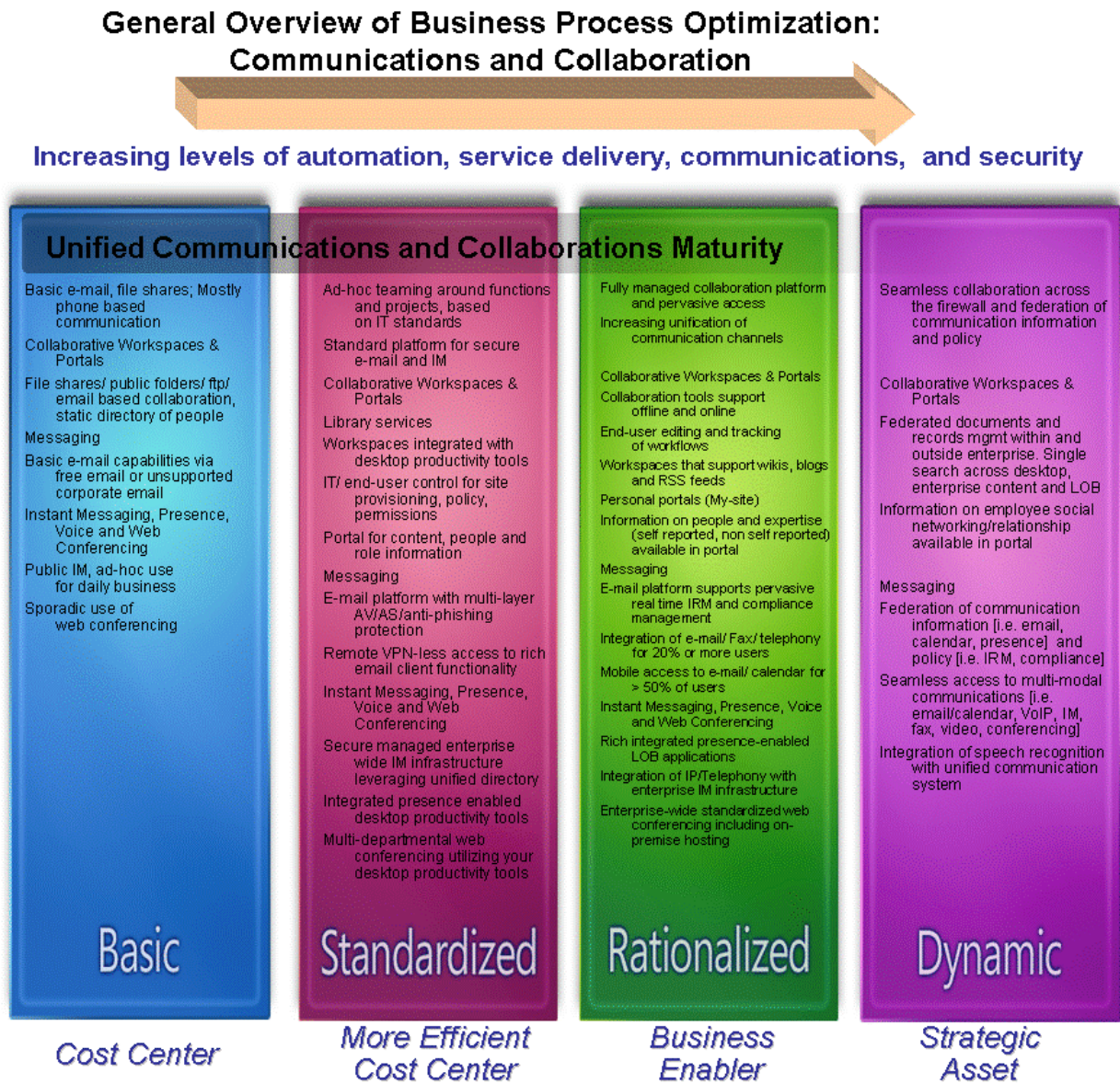
- Employees spent up to 25% of their time searching for information that was spread across the infrastructure.
- Employees were needlessly recreating documents and information that they couldn't find as a result of inefficient search capabilities, or they were using out-of-date documents as source boilerplates, creating additional risk.
- Employees sometimes had inappropriate access to confidential information.
- Collaboration was inefficient and involved too many face-to-face and telephone meetings.
- Document version control was lacking and multiple versions of documents created confusion and increased risk.
- Lack of consistent information classification resulted in users' confusion over corporate policies and compliance requirements regarding the disposition of data.
- There was no single sign-on for applications used by employees.
- There was little in the way of automated workflow processes to ensure review, update or approval
- IT costs were not controlled because of a lack of mechanisms to perform comprehensive inventories of hardware, software and licenses, and by the lack of automation for a number of processes, such as server and desktop patching and desktop imaging.
- Patch management was inefficient.
- IT constantly reacted to exposed threats and vulnerabilities.
- The lack of a pervasive adoption of security and business process best practices led to increased risk throughout the organization.

Over the past few years, Contoso has made a concerted and intensive effort to streamline its operations to enable more effective collaboration, more efficient business processes, better regulatory compliance and better security.

To this end, Contoso implemented a number of integrated solutions, including the following:

- Standardized desktop operating systems to Windows XP, Service Pack 2, and is currently evaluating Windows Vista with a pilot group of users
- Standardized productive applications to Office 2003 Enterprise Professional Edition, and is in the process of upgrading to Office System 2007.
- Standardized server operating systems on Windows Server 2003 and Windows Server 2003 R2
- Deployed Rights Management Services for persistent document protection
- Consolidated and rationalized Active Directory® domains
- Deployed Active Directory Group Policies to enforce security and other settings on the desktop and servers
- Initially implemented Software Update Services (SUS), and later transferred patch management functions to Systems Management Server.
- Standardized the messaging infrastructure on Exchange Server 2003 and recently upgraded to Exchange Server 2007
- Deployed Systems Management Server for software deployment, patch management and inventory collection.
- Implemented SoftGrid® to deploy virtualized applications
- Deployed Forefront integrated security solutions to protect against viruses and malware
- Deployed Microsoft Identity and Integration Server (MIIS) for single sign-on and account provisioning across the enterprise, and is considering upgrading to Identity Lifecycle Manager 2007, which also includes certificate management functionality
- Deployed SharePoint Portal Server 2003 and recently upgraded to Microsoft Office SharePoint Services 2007 to provide Web portals and document workspaces
- Deployed InfoPath® 2007
- Deployed Information Bridge Framework and other solutions to enable integration between line of business (LOB) applications and Microsoft Office System
- Deployed a Public Key Infrastructure (PKI), based on Certificates Services in Windows Server 2003
- Enabled Encrypted File System (EFS) for laptop users
- Enabled BitLocker™ full volume encryption for Windows Vista users
- Began a process to adopt security and business process best practices, as described by common framework models

By implementing these solutions, Contoso categorizes its optimization level somewhere between the Standardized and Rationalized level. To help situate Contoso within a specific IOM level, the following graphic shows the communications and collaboration sub-category of the business process optimization.



Given the number of solutions, amount of automation and improved process Contoso has implemented, the fact that it characterizes its optimization level somewhat below the Standardized level might appear as if it underestimated its optimization level. However, before Contoso can characterize itself as having fully achieved a Rationalized or Dynamic optimization level, it must meet some necessary, but currently

missing, requirements. For example, Contoso has yet to fully deploy IPSec to provide isolation of servers to meet full security and compliance requirements. Providing this kind of secure isolation is a necessary requirement for Contoso to characterize itself as having achieved a Rationalized level of optimization.⁵

Network Infrastructure Security: Defense in Depth

To achieve increased optimization according the IOM framework, Contoso needed to create numerous projects to manage the changes. Many of these projects ran parallel to one another, while others ran sequentially. One of the first priorities that Contoso identified for immediate action was network infrastructure security. In particular, Contoso needed to ensure that it adopted defense-in-depth strategies whenever feasible to protect its infrastructure.

The following provides a high-level summary of some changes that Contoso implemented to improve network security.

Patch Management

Contoso's IT department encountered many challenges managing software updates and patches. Patching was, for the most, a manual process with few mechanisms for reporting the update status of computers. This led in turn to an unacceptable level of vulnerability and increased risk to server and desktop computers.

Contoso initially deployed Software Update Services (SUS) to manage updates and patches in its infrastructure. By doing so, Contoso was able to automate the deployment of patches and updates, and achieve more efficient management of its update infrastructure.

At the same time as it deployed SUS, it began a project to implement Systems Management Server (SMS). With the release of Windows Software Update Services (WSUS), which superseded SUS, Contoso began a process of evaluation to determine whether to upgrade its update infrastructure to WSUS or to transfer this functionality to SMS.

In the end, Contoso decided to transfer this functionality to SMS. While SMS requires a little more work up front to deploy patches and updates than SUS or WSUS, it has a number of enterprise features that make it a superior choice for large networks. For example, SMS provides richer reporting mechanisms, better compliance checking and more flexible scheduling.⁶

When evaluating whether to transfer update functionality to SMS, Contoso performed a risk analysis and identified the patch status of laptops as one vulnerability. Mobile users who weren't able to connect to the corporate network for long periods of time weren't receiving updates from the management infrastructure. With SUS, Contoso configured an Active Directory Group Policy that forced computers to

⁵ Windows Server 2003 SP2 allows the use of an IPSec "Simple Policy," potentially reducing the complexity of IPSec implementations. However, implementing IPSec to meet security and compliance requirements can still be a complex undertaking. For more information on the topic of server and domain isolation by using IPSec, see [Server and Domain Isolation Using IPsec and Group Policy](http://www.microsoft.com/technet/security/guidance/architectureanddesign/ipsec/default.mspx) at <http://www.microsoft.com/technet/security/guidance/architectureanddesign/ipsec/default.mspx>

⁶ For a comparison of SMS versus other patch update mechanisms, see [Comparing MBSA, MU, WSUS, and SMS 2003](http://www.microsoft.com/windowsserversystem/updateservices/evaluation/compare.mspx) at <http://www.microsoft.com/windowsserversystem/updateservices/evaluation/compare.mspx>.

get updates from the SUS servers. Users could not receive updates from Windows Update, unless they performed a manual scan by visiting the Windows Update site.

Contoso wrestled with this issue for some time. However, based on its risk analysis, it decided that laptops used by remote workers should automatically receive patches and updates from both Microsoft Update by using Automatic Update, and from the internal update infrastructure through SMS, depending on availability. SMS provides better roaming user support than WSUS and more easily allows for this kind of flexibility.

Anti-Virus and Anti-Malware Protection

Initially, Contoso relied on a single vendor to provide anti-virus protection on its servers, desktops and Exchange Server. However, during the risk analysis it performed as part of the process to optimize its infrastructure, Contoso identified several vulnerabilities associated with the single-vendor solution, which for example, did not lend itself easily to a defense-in-depth strategy for protection against malware and viruses for the messaging infrastructure.

While its anti-virus vendor usually provided timely signature updates, Contoso had on a few occasions experienced significant downtime during particularly pernicious virus outbreaks, because the anti-virus vendor had not released a signature update in time to prevent the outbreak on the network. Additionally, every time Contoso deployed a new signature to its Exchange Servers, they needed to shut down Exchange services, resulting in interrupted mail flow. Also, the vendor could not provide an antivirus solution for SharePoint or Office Communications Servers.

To implement a defense-in-depth strategy for virus and malware protection, Contoso would have needed to implement solutions from multiple vendors, but this would have increased the workload on the IT department, and introduced additional and unacceptable costs.

For these reasons and others, Contoso decided to purchase and implement the Forefront Security Suite, which includes Forefront for Exchange Server, Forefront for Office SharePoint Server, Forefront for Communications Server, and Forefront Client Protection, and Exchange Hosted Filtering, which is a part of Exchange Hosted Services.⁷

The Forefront Security Suite provides defense-in-depth protection automatically for application servers, such as Exchange Server and SharePoint. Through Exchange Hosted Filtering, multiple anti-virus engines provided by different vendors can scan both inbound and outbound email. Different vendors have different response times, based on a number of factors, such as the time of outbreak, to virus outbreaks.⁸

⁷ At the time of this writing, Forefront for Office Communications Server is still in beta and will be available later in 2007 for general release. For information on Forefront Security Suite availability and licensing, see [Microsoft Enterprise Client Access License Suite](http://www.microsoft.com/calcsuites/enterprise_product.msp) at http://www.microsoft.com/calcsuites/enterprise_product.msp.

⁸ This does not mean that a particular vendor is better or worse than another. Given a particular outbreak, one vendor might respond faster than another. For a subsequent outbreak, their positions might just as easily be reversed. For a sample of different response times for a particular outbreak, you can view a spreadsheet made available by [AV-Test.org](http://www.av-test.org) at <http://www.av-test.org/download/ms05-039.zip>.

By using multiple antivirus vendor engines, the chances that one or more of the engines will catch emerging and new viruses are increased. Exchange Hosted Filtering also catches spam with a high degree of accuracy before it reaches the network. An added advantage of catching viruses and spam before they reach the network is that bandwidth is freed up for legitimate business traffic.⁹

Like Exchange Hosted Filtering, the application server-based Forefront solutions, such as Forefront for Exchange Server, also use multiple antivirus engines from different vendors. For example, it is possible to configure up to nine antivirus engines to protect against viruses. However, depending on the Exchange Server role and the desired level of protection and performance, only a subset of the available engines generally are used at any one time to scan for viruses.

This means that Forefront security for Exchange, SharePoint and Communications server can provide consistent levels of protection during anti-virus engine updates. When one engine needs to be updated, Forefront will swap an available engine in (based on an algorithm that looks at its success history and other factors) to perform virus scanning. Furthermore, mail keeps flowing during virus engine updates, unlike other solutions.¹⁰

Confidentiality, Integrity and Authentication Controls

Because of the proprietary and confidential nature of much of Contoso's communications and data, Contoso implemented its own Public Key Infrastructure to issue X.509 digital certificates to internal employees and other end entities, such as routers and computers. With X.509 certificates, a Certificate Authority asserts the identity of the subject of the certificate (the end user, computer, device, etc). The CA further asserts that subject of the certificate is in possession of the private key that is mathematically linked to the public key included with the certificate.¹¹

The implementation of its Public Key Infrastructure was a major undertaking that required significant planning. Based on the intended usage for some of the issued certificates, Contoso needed to establish a high degree a trust for its issued certificates and, by extension, for the Certificate Authorities. Some of the high-value certificates that Contoso wished to deploy included certificates for signing custom code, certificates to authorize purchase orders for significant amounts, and to verify identity and assert non-repudiation.

To achieve the appropriate level of trust, Contoso implemented a hierarchy of Certificate Authorities and purchased specialized hardware in the form of Hardware Security Modules (HSMs) to protect the private key material of the Certificate Authorities that issue certificates. Additionally, to ensure the security of the private key material issued to end users, Contoso issued smart cards to all of its employees. To log onto the internal network, employees must provide a smart card and enter a PIN.

Contoso uses certificates not only for network logon, but also to encrypt email, to digitally sign email and documents, and for Encrypted File System (EFS), to encrypt communication between routers and

⁹ For more information on [Microsoft Exchange Hosted Filtering](http://www.microsoft.com/exchange/services/filtering.aspx), see <http://www.microsoft.com/exchange/services/filtering.aspx>.

¹⁰ To learn more about Forefront security solutions, see <http://www.microsoft.com/forefront/default.aspx>.

¹¹ Public key cryptography employs one-way encryption and decryption. If a message is encrypted with the public key, only the private key can decrypt it and vice versa. The private key is always stored in a secure location, separate from the public key and certificate.

other purposes. A significant advantage of deploying Windows Server 2003 Certificate Services is that Contoso can archive private key material for certificates that are used for encryption purposes. This means that if a user loses the private key used for encryption, access to confidential data can be restored by recovering the private key from the archive.¹²

Currently, the management of certificates and smart cards is a little more cumbersome than Contoso would like. For this reason, it is considering upgrading to Microsoft Identity Lifecycle Manager (ILM) 2007, to ease the management burden by providing better reporting, self-service provisioning, and policy- and workflow-driven solutions for certificate management.¹³

Service Management and Monitoring

Contoso faced a number of challenges in managing and monitoring its network infrastructure to ensure a high level of availability and to plan for growth. To address these challenges, Contoso initially deployed Microsoft Operations Management Server 2005 (MOM). This helped Contoso improve its service uptime by closely monitoring services on its network to prevent outages related to server capacity, server failures and outages. Additionally, MOM 2005 can collect events from event logs and forward them to the MOM database on the MOM management server.

However, while MOM possessed the capability to forward events from event logs, it wasn't a suitable solution for security monitoring and attack detection because it was not designed for this purpose. Furthermore, Contoso faced great challenges meeting audit compliance requirements. For example, with 175 possible security-related events that can appear in event logs, IT administrators found it extremely difficult to map and categorize the security-related events to specific compliance rules that required role separation for audit log process.

To assist in meeting audit log compliance requirements, Contoso recently upgraded its MOM 2005 infrastructure to Systems Center Operations Manager 2007. Operations Manager 2007 includes a new Audit Collection Service, which provides near real-time collection of audit logs and provides role separation capabilities for audit log access.¹⁴

Edge Protection

To provide controlled and secure inbound and outbound access between the corporate network and the Internet, Contoso first implemented Internet Security and Acceleration Server 2004 (ISA), and subsequently upgraded to ISA 2006.

¹² Security of the archived private key material is assured through the requirement for role separation. A minimum of two individuals, each occupying separate roles, are required to recover archived private key material. It should also be noted that key archival and recovery is possible only with keys that are used for encryption: it isn't possible or desirable to archive keys used for signing.

¹³ Microsoft Identity Lifecycle Manager (ILM) 2007 includes the ability to manage digital certificates, found in Microsoft Certificate Lifecycle Management. For more information on [Microsoft Certificate Lifecycle Management](#) and ILM, see <http://www.microsoft.com/windowsserver/ilm2007/default.aspx>.

¹⁴ For more information on Systems Center Operations Manager, see <http://www.microsoft.com/systemcenter/opsmgr/default.aspx>.

ISA Server 2006 provides Contoso with an advanced application-layer firewall that provides deep inspection of inbound and outbound traffic, an integrated proxy and caching server to accelerate Web browsing, and a robust VPN solution for remote access.

During the initial implementation of ISA Server 2004, Conesco leveraged the VPN quarantine feature to provide end-point checking of VPN clients before they were allowed access to the corporate network. Even though this feature provided advanced security, VPN access wasn't always available to remote users who connected their laptops to a network that did not allow VPN traffic.

Another issue that concerned Conesco was related to SharePoint and Outlook® Web Access from unmanaged computers. It was possible for remnants of confidential data to remain on the unmanaged computer after access to the SharePoint or OWA sites.

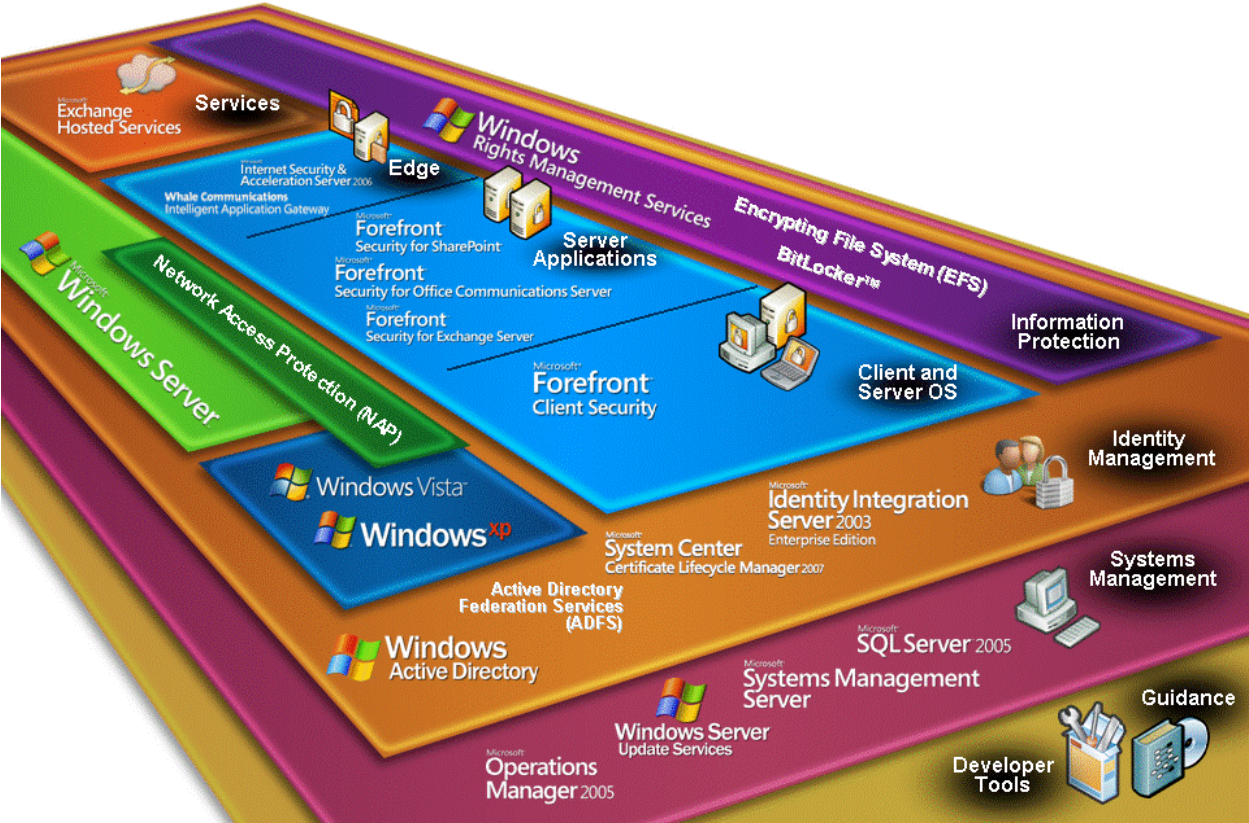
To address these issues, Contoso decided to implement Intelligent Application Gateway 2007 (IAG). With IAG, Contoso provided SSL VPN access by using Web protocols, which enables remote users to connect securely to internal SharePoint sites and other resources from many locations. Additionally, IAG provides robust and granular end-point security checking to determine whether clients meet specific requirements for access.

With IAG, Contoso administrators could define conditions that determined what activities were permitted on the SharePoint site based upon the end-point security of the client computer. For example, Contoso administrators prevented SharePoint integration with Office applications on the end-point computer, unless the Attachment Wiper client component was present. Otherwise, office documents could be displayed in a Web browser but not cached. Additionally, Contoso administrators prevented uploading and downloading operations (including import and export) to the SharePoint site, unless the clients met specified conditions.

IAG 2007 did not replace ISA 2006. Contoso still uses ISA for outbound access and to publish its public Web site and other applications, such as DNS. IAG 2007 has replaced, however, some functionality previously supplied by the VPN provided by ISA. And because of the advanced security features of IAG 2007, both SharePoint and OWA access now occur through it.¹⁵

The following graphic shows the relationships among the various technologies that Contoso has implemented to achieve core infrastructure optimization and defense in depth security.

¹⁵ For more information on ISA 2006 and IAG 2007, see <http://www.microsoft.com/forefront/edgesecurity/default.aspx>.



Sample Engagement

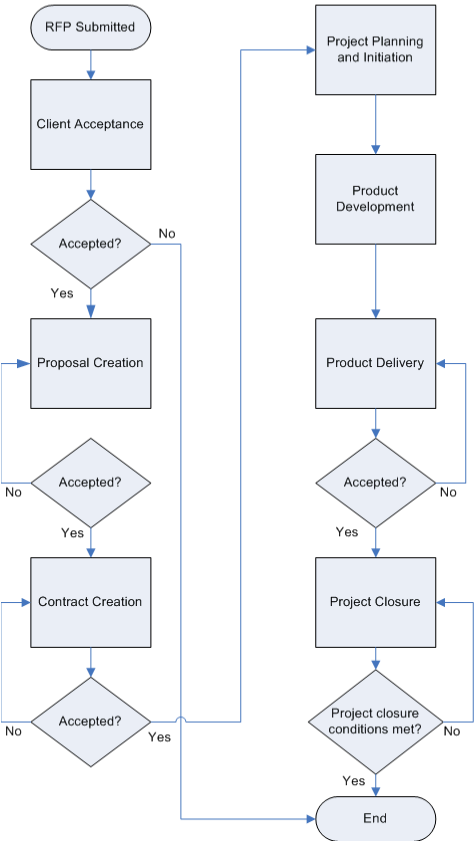
Contoso is currently engaged by Northwind Traders to provide tax planning and management consulting services for the operations of the U.S. division of Northwind Traders, an international firm that specializes in transportation, export and import of a wide range of products.

The French subsidiary of Northwind Traders, based in Paris, has entered into negotiations with Wide World Importers International regarding a potential purchase of Wide World Importer’s European operations, whose head office is located in Strasbourg, France. Ben Smith, the CEO of Northwind Traders, contacts the engagement manager at Contoso, Alice Ciccu, with a Request for Proposal (RFP) for an additional engagement outside the present scope of work. Specifically, Ben would like Contoso to prepare a tax impact analysis of the purchase. Alice explains that Contoso will need to perform internal checking to ensure that no ethical conflict exists before it can respond to a formal Request for Proposal for the new project.

High-Level Process Overview of Project Scenario

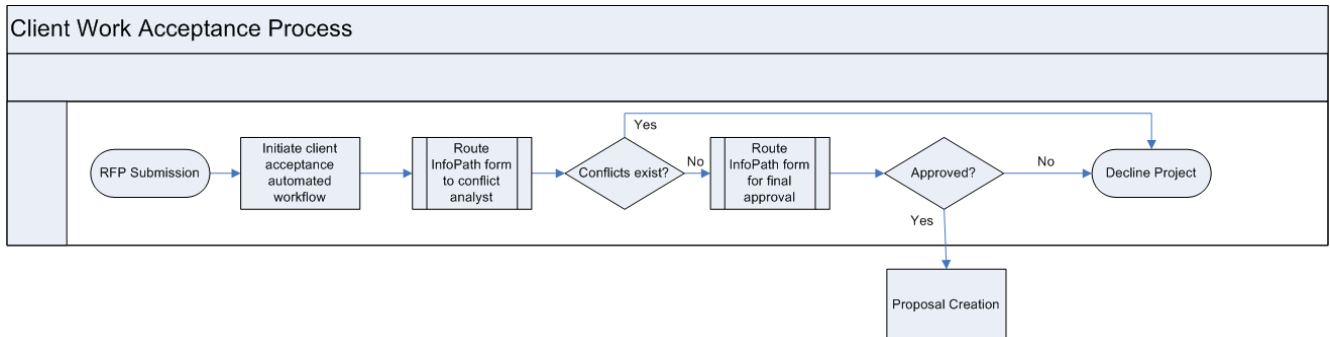
Assuming that Contoso has no conflicts and can perform the work, the project will have a number of distinct phases from start to finish, as indicated in the following simple flowchart that indicates the major project phases from beginning to end. The scenario vignettes that follow correspond to and provide details on each of the project phases.

Sample Engagement Process Overview



Client Work Acceptance Process

Contoso's business rules require that all potential work undergo a client acceptance process. One of the primary purposes of this process is to ensure that no conflicts exist that would compromise Contoso's fiduciary duties to its clients. The diagram below shows the major steps of this process.



Alice is aware of the current work Contoso does for Northwind Traders. However, before initiating a new work approval process to respond to the RFP, she needs to determine what other work Contoso might be doing for Northwind Traders and if it has or is currently doing work for Wide World Importers International.

SharePoint Enterprise Search / Security Trimming

Alice performs a search by using the SharePoint server to see what other work has been or is being performed for Northwind Traders and Wide World Importers. Before the implementation of SharePoint, Alice would have needed to perform time-consuming searches across multiple locations and systems to find this information. However, because Microsoft Office SharePoint Server (MOSS) 2007 provides a content-management solution that can index and provide access to content from disparate sources, Alice can perform her initial search from a central location quickly and easily. Because SharePoint employs a technique known as “security trimming” of the search results at query time, Alice will have access only to content for which she has the appropriate permissions.¹⁶

MOSS 2007 provides enhanced search functionality and security over previous versions. For example, the improved search capability completely removes references to documents and other items from the search results that she is not authorized to view. This also removes a source of frustration for many end users who, with previous versions of SharePoint, would click on links to items only to discover they did not have permission or access to them.¹⁷

¹⁶ In many cases, it isn't possible to perform security trimming on data retrieved from Line of Business (LOB) applications, often because the back-end systems use different security mechanisms for providing access. However, with MOSS 2007, custom security trimming solutions are possible. MOSS 2007 includes a Business Data Catalog Custom Security Trimmer that allows security trimming of indexed data before the results are returned to the user. For technical information on this topic, see the MSDN web page, [Business Data Catalog Security Trimming](http://msdn2.microsoft.com/en-us/library/aa980904.aspx) at <http://msdn2.microsoft.com/en-us/library/aa980904.aspx>.

¹⁷ For a technical drill down and demos that also are suitable for non-technical specialists of new SharePoint search features, see “[ITPRODSK-103: SharePoint Search Technical drill down](http://www.microsoft.com/technet/community/events/moss2007/dsk-103.msp)” at <http://www.microsoft.com/technet/community/events/moss2007/dsk-103.msp>.

Integration with Line of Business Applications /Business Data Catalog

Based on her search, Alice sees no obvious items that could potentially place Contoso into a conflict of interest. She subsequently accesses a SharePoint site to initiate a new work-approval process.¹⁸ Through this site, she can generate a form that includes relevant information, much of which is pre-populated by data pulled from various sources, such as Contoso's ERP and CRM systems, based on values that Alice selects from drop-down lists embedded in the form. This integration with the line of business systems is made possible by the web services interfaces of the Business Data Connector.

Windows Workflow Foundation and InfoPath Customization

Alice completes the form, providing both required and optional information. Upon submitting the form, the workflow process is initiated by routing an email message and Outlook task item to Contoso's conflict analyst. At any time, Alice can view the status of the new work-approval request in the appropriate document library at the SharePoint site. Additionally, when checking the status of the request, she sees that key metadata has been extracted from the InfoPath form and promoted into the SharePoint list.

Workflow integration with Outlook Tasks / Personalized InfoPath view

Contoso's conflict analyst opens the task item in Outlook and clicks on the embedded link. The conflict analyst's view of the form is customized to provide information relevant to his role and is different from Alice's view. For example, the form pulls in additional information from both the line of business systems and, using Web Services, from Dunn & Bradstreet. The conflict analyst reviews this information and performs his own search. Because he has a greater degree of access to corporate information, he discovers a number of sensitive projects and documents that Alice did not find in her initial search. However, none of these projects, in his professional opinion, constitutes a conflict of interest, since the new work affects a subsidiary outside of the U.S. and for which Contoso is not performing any work. After determining that no conflicts exist, the conflict analyst approves the request.

Upon approval by the conflict analyst, another workflow process is initiated by routing an email message and Outlook task item to the managing partner responsible for the Northwind Traders account. As with the conflict analyst's view of the InfoPath form, the managing partner's view is customized to suit her role by providing only high-level information and notes from the conflict analyst.

When the managing partner approves the form, Alice receives an email message indicating that the approvals are complete and she can initiate the next phase of the work. If Alice is out of the office, she can receive this message on her smart phone or connect to the SharePoint site through a secure connection.

¹⁸ By using Visual Studio® 2005, SharePoint Services 2007, and SharePoint Designer 2007, organizations can add custom workflows to any content to ensure compliance by having the appropriate people sign off on documents and other information. Out of the box, SharePoint Services provides workflows for approval, collect feedback, collect signatures, disposition approval, issue tracking and translation management. For a comparison between workflow development between Office SharePoint Designer 2007 and Visual Studio 2005 Designer for Windows Workflow Foundation, see "[Workflow Development for Windows SharePoint Services](http://msdn2.microsoft.com/en-us/library/ms414613.aspx)" at <http://msdn2.microsoft.com/en-us/library/ms414613.aspx>. Also see the white paper, [Understanding Workflow in Windows SharePoint Services and the 2007 Microsoft Office System](http://www.microsoft.com/downloads/details.aspx?FamilyId=DBBD82C7-9BDE-4974-8443-67B8F30126A8&displaylang=en) at <http://www.microsoft.com/downloads/details.aspx?FamilyId=DBBD82C7-9BDE-4974-8443-67B8F30126A8&displaylang=en>

Technologies

- Office Outlook 2007
- SharePoint Server 2007
- SharePoint Designer 2007
- InfoPath 2007
- Windows Mobile® 5.0/6.0

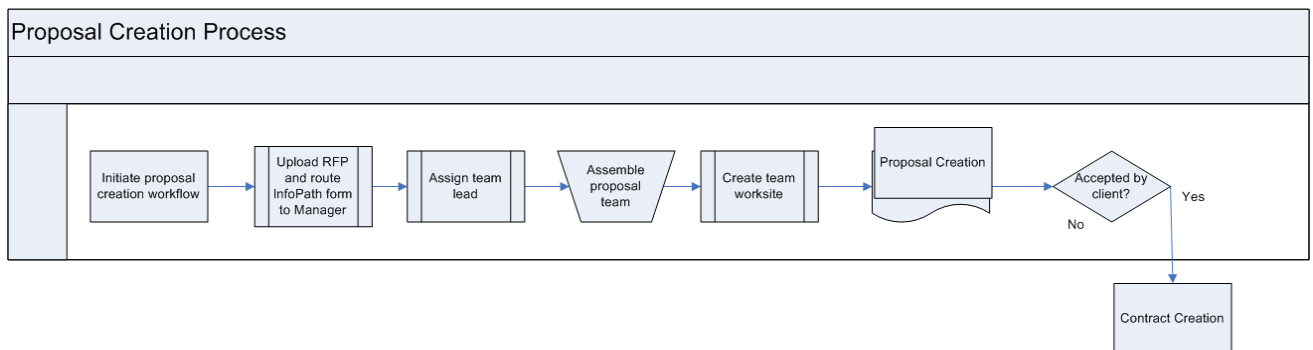
Product Features

- Document Libraries
- Business Data Catalog (MOSS 2007)
- Web Services
- Mobility
- Document Library Metadata Lists
- Workflow (integration with Outlook and Outlook Tasks)
- InfoPath Personalization

Proposal Creation Process

Proposal writing is a complex activity and involves managing multi-part documents, coordinating actions among team contributors, having access to approved templates and content, and having access to government regulations and client requirements. Before Contoso upgraded its infrastructure and communications and collaboration environment, the proposal creation process was a lengthy and cumbersome process. Fortunately, the investments Contoso has made in its infrastructure and collaboration environment have begun to pay significant dividends for this situation. Proposal content creation is accelerated and the timelines for proposal creation are significantly shorter through the use of SharePoint sites and integration with Microsoft Office and Line of Business applications, allowing for easy re-use of proven content, enhanced communications capabilities and other benefits.

Like the client-acceptance process, the proposal-creation process is characterized by automated procedures and workflows to ensure compliance with internal business processes and rules. The following diagram illustrates the major phases of this process.



Now that Alice has approval to begin work on the response to the RFP, she needs to ensure that the response is completed in a timely manner. Northwind Traders has used an RFP process to ensure that its requirements for the tax impact analysis are properly detailed and scoped, even though Contoso is the only firm it is currently considering for this work. As such, the RFP process reflects the company's own internal business rules and processes that must be followed.

Customized team sites / SharePoint application templates

Normally, the Contoso sales team, using its own SharePoint site, manages responses to RFPs. Alice will need the sales team to prepare the response to the RFP. To pass the work to the sales team, she accesses Contoso's RFP Management SharePoint Site, where the sales team can list and view RFP project issues and tasks. The site also includes project status reporting, the ability to assign new tasks, Gantt charts and other tools to assist with RFP assembly and tracking. Contoso created this site because they wanted a better-controlled process for managing and tracking RFP assembly. The site itself is based on the Project Tracking SharePoint application template and uses SharePoint Designer¹⁹ to create workflows without having to write code.

¹⁹ The Project Tracking workspace template is one of 40 application templates that are available for Windows SharePoint Services v 3. These application templates make it easy for organizations to deploy custom SharePoint sites to meet their business needs. While Contoso could have used the Request for Proposal application template, the Project Tracking template

Rights Management Services integration with SharePoint

At the RFP Management site, Alice fills in an InfoPath form to ensure that the proper metadata, including the due date, is associated with the RFP document she uploads. When the RFP is added to the document library, it is automatically protected with a Rights Management Server (RMS) Company Confidential template.²⁰ Upon completion of the form and addition of the RFP to the document library, an email with the appropriate information is sent to the sales manager, Arlene Huff.

From Outlook, Arlene clicks on the link embedded in the email, which takes her to the appropriate area of the RFP Management site. Arlene decides to assign the proposal creation to Frank Lee, a sales team lead with experience in this kind of proposal.

Windows Mobile 6.0 integration features

Frank Lee is out of town, but receives an email on his smart phone, which is running Windows Mobile 6.0, indicating he has a new proposal to create. Frank wants to get started on the project right away, so he clicks on an embedded link within the email. This action takes him to the SharePoint document library where he reviews the RFP. Even though the RFP is RMS-protected, Frank can still review the document because his smart phone is running Windows Mobile 6.0.²¹

He notes that the RFP will require knowledge of French regulations and someone with the ability to translate key documents from French. He has some questions about this aspect of the project, so on his mobile device he initiates an IM session with his sales manager, Arlene Huff, to receive further clarification.

Outlook bi-directional synchronization with SharePoint

Back at the hotel room, Frank wants to do some additional reading in the RFP document library. He knows that he won't have time to finish his reading that evening and will continue his reading on the flight home. Frank establishes a secure connection, opens the SharePoint site and then selects the action to open the documents library in Outlook. By performing this action, he synchronizes his Outlook offline cached copy of the documents library with RFP documents library.²² On the plane the following day, Frank can review the documents while not connected to the network.²³

better suited their needs. For more information on these and other templates, see "[New Application Templates for Windows SharePoint Services 3.0](http://www.microsoft.com/technet/windowsserver/sharepoint/wssapps/templates/default.mspx)" at <http://www.microsoft.com/technet/windowsserver/sharepoint/wssapps/templates/default.mspx>.

²⁰ A new feature of MOSS 2007 is the ability to apply RMS protection when documents are checked out of the library. RMS permissions are applied automatically, mapped to permissions on the document library. Office System 2007 applications are RMS enabled.

²¹ Accessing the SharePoint document library requires Windows Mobile 6.0 and Exchange Server 2007. Access to RMS protected content on smart phones requires Windows Mobile 6.0 and RMS.

²² A new feature of Outlook cached mode in Office System 2007 allows bi-directional synchronization of document libraries, in addition to other SharePoint items, such as calendars, tasks, and discussions.

²³ Depending on the RMS permission settings, it is possible to open RMS protected documents without a connection to the RMS server, as long as they have been opened at least once during a period when a connection to the RMS server is available.

Frank's first task when he returns to the office is to assemble a team to research and create the proposal response to the RFP. Frank's team can complete most of the proposal unassisted, but Frank will need to seek additional expertise for areas of the proposal requiring knowledge of French regulations and the French language. To do this, he connects to the MOSS 2007 SharePoint Search Center.

SharePoint Enterprise Search and Social Networks for real-time presence indication and communications

By clicking on the People link of the Search Center, Frank can search for individuals according to various criteria, by name, title, role, skills, and so on. Frank performs a search for people who speak French and have familiarity with French regulations. The search results return the name of Thierry D'Hers, located in the Paris office. Frank notes that the presence indicator icon reveals that Thierry is online. Before contacting him via IM, Frank clicks the search- result link to view additional details about Thierry, including his people associations and colleagues.²⁴ Frank also notes Thierry's manager and sends her an email requesting that some of Thierry's time be made available for help with the proposal. From the search results, Frank adds Thierry as a colleague to increase the scope of his social network at work and then clicks on the presence indicator icon to initiate an IM chat.

During the IM chat, Frank suggests to Thierry that they conduct a voice call by using Communicator as the IP telephony client.²⁵

With his team complete, Frank can create a workspace for the proposal and include relevant documents, templates, URLs and other resources. Again, Frank uses the Search Center to find relevant information with which to populate the workspace. Again, because of the security trimming that SharePoint performs on search results, Frank only sees the results for items that he is authorized to see. Once the documents and other information are in place, Frank assigns tasks to his team so that work can commence on the proposal.

Technologies

- Office Outlook 2007
- Exchange Server 2007
- SharePoint Server 2007

²⁴ MOSS 2007 provides people finding and expertise location out of the box. To do this, MOSS 2007 indexes the information stored in the user profile store. The My Site feature of MOSS is built upon this store and contains information from different sources, such as Active Directory (DL memberships, department, manger, etc); information that users publish about themselves (interests, skills, keywords, etc.); users' photos; and a list of colleagues. Searches can be grouped by social distance, sorted by straight relevance or filtered through a number of criteria, such as department or title. The ability to mine emails and other information to capture tacit knowledge and enrich the people search to extend to individuals outside the organization is provided by a forthcoming product, the Knowledge Network (KN). The KN is currently available as an unsupported Technical Preview (English only). For more information on KN and the Technical Preview, see the Knowledge Network Team blog at <http://blogs.msdn.com/kn/>.

²⁵ A recent evaluation (March 2007) of a pre-release version of Microsoft Office Communications Server 2007 and Microsoft Office Communicator 2007 desktop Voice over Internet Protocol (VoIP) solution conducted by Psytechnics demonstrated superior voice quality compared to single-purpose IP phone. For more information, see "[Psytechnics Unveils Unique Performance Report on Microsoft's Voice Communications Technology](http://www.psytechnics.com/site/sections/news/2007/2007_03_06.php)" at http://www.psytechnics.com/site/sections/news/2007/2007_03_06.php.

- SharePoint Designer 2007
- Office Communicator 2005
- InfoPath 2007
- Windows Mobile 6.0
- Rights Management Services (RMS)

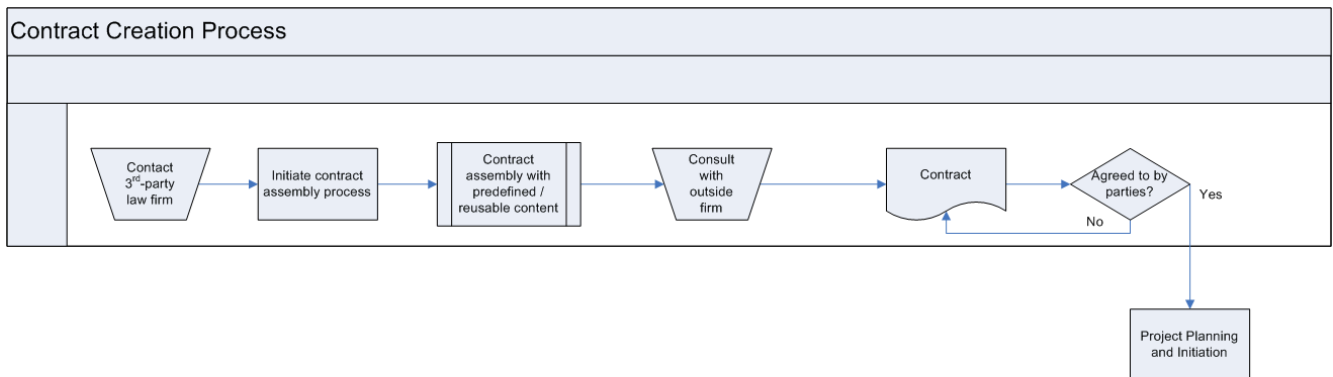
Product Features

- Document Libraries
- Business Data Catalog (MOSS 2007)
- Enterprise Search (MOSS 2007)
- My Sites (MOSS 2007)
- Social Networking Web Parts (MOSS 2007)
- Real Time Presence and Communication
- Web Services
- Mobility
- Document Library Metadata Lists
- Workflow (integration with Outlook and Outlook Tasks)
- InfoPath Personalization
- MOSS 2007 RMS integration
- Outlook 2007 offline cache mode

Contract Creation and Agreement Process

Once the proposal has been accepted by both Contoso and Northwind Traders, the next steps are to draw up and get signed agreements for a contract to perform the work. Contoso has a close relationship with a legal firm, Litware, for this and other purposes. Litware will be responsible for drafting the contract to cover the tax assessment work.

The following diagram illustrates the major phases of contract and agreement process.



Background

Litware lags somewhat behind Contoso in terms of their infrastructure optimization and software lifecycle. For example, they lack an RMS deployment and have not upgraded to any Office System 2007 products. Litware is, however, a forward-looking law firm that has made significant investments in technology to assist with business processes and security. For example, the firm has standardized on Microsoft Office 2003 Enterprise Professional Edition, deployed Microsoft SharePoint Server 2003, and implemented the Microsoft Office Information Bridge Framework (IBF).²⁶ In combination, these products create a powerful solution for content management, including the re-use of proven content.

SharePoint extranet access / ADFS

To facilitate inter-organizational collaboration between their respective organizations, Contoso and Litware have each deployed Active Directory Federated Services (ADFS) to establish a federation-trust relationship.

Litware does not have an extranet SharePoint Portal site for its clients. But Contoso can extend resource access of its extranet SharePoint site to Litware, its account partner in the federation-trust

²⁶ IBF is being superseded by Line of Business interoperability (LOBi) services, due with a future release of Office products. In the meantime, the recommendation is that organizations that have not currently deployed IBF instead use Microsoft Visual Studio Tools for Office 2005 SE (VSTO 2005 SE) and native platform capabilities, such as BDC, for the Office solution development projects. Many scenarios announced for LOBi are possible by using the Office platform. For more information, please see [the Office Business Applications team blog](http://blogs.msdn.com/oba/archive/2007/02/27/update-on-lobi-services-and-ibf.aspx) at <http://blogs.msdn.com/oba/archive/2007/02/27/update-on-lobi-services-and-ibf.aspx>.

relationship.²⁷ This means that employees in Litware can gain access to Contoso resources on the extranet site by using their Litware credentials. Contoso controls and audits access to resources.

SharePoint extranet benefits

By deploying MOSS 2007, Contoso achieves a variety of benefits over SharePoint Portal Server 2003 for its extranet. These benefits, as they relate to extranet functionality, include:

- WSS 3.0 and MOSS 2007 provides wider authentication support, including pluggable authentication based on the ASP .NET 2.0 provider model and .NET Framework 3.0; this means that new technologies such as Windows CardSpace™ can be leveraged to provide a means for authenticating external users.²⁸
- Users can upload or email documents, messages and calendar items directly into the extranet site for access by external users.
- Jobs can be created that will automatically copy flagged content from intranet sites to extranet sites so that users do not have to post content twice.
- Web-based forms can be leveraged to allow InfoPath use without the need to deploy client components to extranet users.
- There is more granular access for extranet sites to make it easier for some parts of the site to require a login, while other parts do not.
- There is broader support for auditing of site access, both for security and marketing purposes.²⁹

In addition to the need to facilitate inter-organizational collaboration, another driver for this solution was the need to meet compliance requirements for confidential data. In the past, Contoso often used unsecured transports, such as unencrypted email, to exchange information with external parties.

Public Key Infrastructure benefits / Windows Certificate Services

As part of the solution to provide encryption (confidentiality) for email and other information, Contoso has deployed its own Certificate Authority (CA) hierarchy to issue digital to provide data confidentiality, integrity and non-repudiation. In addition to the business need to secure information in transport, Contoso needed to ensure security for custom code, such as macros, that ran in its environment.

²⁷ For an overview of ADFS, see "[Overview of Active Directory Federation Services \(ADFS\) in Windows Server 2003 R2](http://www.microsoft.com/WindowsServer2003/R2/Identity_Management/ADFSwhitepaper.mspix)" at http://www.microsoft.com/WindowsServer2003/R2/Identity_Management/ADFSwhitepaper.mspix. For technical information on setting up MOSS 2007 with ADFS, please see "[Configuring Multiple Authentication Providers for SharePoint](http://blogs.msdn.com/sharepoint/archive/2006/08/16/configuring-multiple-authentication-providers-for-sharepoint-2007.aspx)" at <http://blogs.msdn.com/sharepoint/archive/2006/08/16/configuring-multiple-authentication-providers-for-sharepoint-2007.aspx> and "Configure Web SSO authentication by using ADFS (for Office SharePoint Server 2007)" at <http://technet2.microsoft.com/Office/en-us/library/61799f9a-da01-4c11-b930-52e5114324451033.mspix>. Also see [SharePoint documentation, Plan for Authentication](http://technet2.microsoft.com/Office/en-us/library/073bfc71-7b01-4b77-bdc3-ac018889d54b1033.mspix?mfr=true) at <http://technet2.microsoft.com/Office/en-us/library/073bfc71-7b01-4b77-bdc3-ac018889d54b1033.mspix?mfr=true>.

²⁸ For general information on CardSpace, please see "[Introducing Windows CardSpace](http://msdn2.microsoft.com/en-us/library/aa480189.aspx)" at <http://msdn2.microsoft.com/en-us/library/aa480189.aspx>.

²⁹ For a more comprehensive list of SharePoint extranet benefits, see [Extranet Support in SharePoint 2007](http://blogs.msdn.com/bobgerman/archive/2006/04/27/584732.aspx) at <http://blogs.msdn.com/bobgerman/archive/2006/04/27/584732.aspx>

According to Contoso policy, all custom code must be digitally signed to verify its authenticity before it is allowed to run. By establishing its own CA, Contoso can sign code with certificates that it issues from the CA.

Although Contoso's Certificate Authority is primarily intended for internal use, Contoso uses a third-party vendor to provide a publicly trusted root CA for its internal CA. This means that the certificate of its CA is signed by an entity that is recognized as a Trusted Root by default. This configuration makes it easier for Contoso's certificates to be trusted by other organizations.

Contoso also can cross-certify its CAs with other organizations so that each organization in the relationship can trust certificates issued by the other organization. This makes it possible, for example, to exchange SMIME encrypted emails with other organizations.

Contoso recognizes that not all partner organizations will have a CA hierarchy or be in a position to cross certify its CAs. However, Contoso can cross-certify its CA with many organizations to meet requirements, including those that various governments impose on their vendors.³⁰

Contract Drafting Process – Document Assembly

Arlene Huff, the Sales Manager, is responsible for ensuring that the contract for the proposed tax assessment work is drafted and agreed upon. After posting the proposal to the Litware site on Contoso's SharePoint extranet, she informs her contact at Litware about the need for a new contract detailing the proposed tax assessment work Contoso will perform for Northwind Traders.

Michael Holm, a lawyer at Litware, signs into the Litware's SharePoint Portal site for Contoso. Here he can access information relevant to the Contoso account, such as time and billing details, a meeting calendar, project data and other information. He also sees that he has been assigned the task for drawing up a contract for Contoso.

From within the Litware site, he clicks on the link to the Contoso extranet site. His browser is redirected to the Litware site on Contoso's extranet, using the credentials he previously provided to gain access to the Litware SharePoint Portal Server site. At the Contoso extranet site, he is presented with a customized page, where he finds a link to the proposal document. Michael downloads the document for later review. Because Litware and Contoso have federated their RMS infrastructures, he can open the IRM-protected document, as long as he has been assigned appropriate RMS permissions and can connect to the Litware RMS server.³¹ He signs out of the Contoso site and is redirected to the Litware SharePoint portal site.

The contract will contain a significant amount of boilerplate content, so Michael expedites the drafting process by finding the appropriate boilerplate and inserting it into a model contract document that he uses as a baseline. It's important to ensure, however, that the boilerplate he uses is up-to-date and has

³⁰ For a technical overview of Public Key Infrastructure (PKI) implementation, see the white paper, "[Best Practices for Implementing a Microsoft Windows Server 2003 Public Key Infrastructure](http://www.microsoft.com/downloads/details.aspx?FamilyID=0bc67f4e-4fcf-4717-89e8-d0ee5e23a242&displaylang=en)" at <http://www.microsoft.com/downloads/details.aspx?FamilyID=0bc67f4e-4fcf-4717-89e8-d0ee5e23a242&displaylang=en>. For specific information on the topic of CA cross-certification, see the white paper, "[Planning and Implementing Cross-Certification and Qualified Subordination Using Windows Server 2003](http://www.microsoft.com/technet/prodtechnol/windowsserver2003/technologies/security/ws03qswp.mspx)" at <http://www.microsoft.com/technet/prodtechnol/windowsserver2003/technologies/security/ws03qswp.mspx>.

³¹ A more extended example of RMS usage can found in the Product Delivery scenario below.

been pre-approved for use. In the past, this was a difficult task at Litware. Content was stored in many locations, often only on the lawyers and paralegals' hard drives, making it largely inaccessible to the firm as a whole and creating elevated risk that outdated or non-approved language would find its way into important legal documents.

These difficulties and risks have been mitigated dramatically with Litware's investment in SharePoint Portal Server 2003, IBF and other technologies. Lawyers, paralegals and other staff spend more time focusing on their areas of professional expertise and less time engaged in searching for information and other "clerical" work.

Content management / Integration with Word Task pane

Michael's first task is to find a model contract document that he can use as a template. His next task is to find additional boilerplate content that he'll use to assemble the document. To find this content, he can search SharePoint for the content, or he can search for the model and boilerplate content from within Word by using the task pane. In this case, the controls in the task pane allow him to display content based on the metadata defined in Litware's Information Bridge Framework (IBF) solution.

Content categorization and reuse

Michael decides to use Word to begin the document assembly process. He opens a new Word document and clicks on the document assembly icon. In the custom task pane that subsequently opens, he can see an index of the content repository displaying a hierarchy of content categories. He traverses this index and finds a candidate for the baseline content. He examines the content in the preview pane to ensure that the document will meet his purposes and then clicks a menu item to generate a new document.

This baseline document is pre-populated with content pulled from the content repository and uses an approved template that includes, for example, appropriate headings, section numbering schemes and so on. The document also contains a number of variables, which act as placeholders for dynamic information, such as the names of the parties involved in the contract, the location where contract will be enforced, and so on. When Michael updates any of these variables (for example, one of the Company Name variables), all instances of the variable are automatically updated in the document. Furthermore, because of the integration with Litware's Line of Business applications through the IBF, Michael can be assured of their accuracy.

In the contract, Michael needs to add clauses and language that are specific to France. Again, he uses the custom task to locate these elements and inserts them into the document. In a matter of minutes, Michael has created a baseline document that includes much of the required content. He can now complete the contract by applying his professional expertise and judgment in crafting specific wording for additional sections as needed.

Document security

While drafting specific contract language, Michael realizes that he needs additional research to complete a section. He assigns a section of the document to a junior lawyer, and asks her to perform the research and draft preliminary language. In assigning this section, Michael assigns permissions through Word to the document such that the junior lawyer can read the entire document, but update only the appropriate section.

In adding specific wording to the contract, Michael notices that some of this content could be re-used in other, similar contracts. He submits the specific sections for approval. Once these sections have been approved, Michael can add them to the content repository.

Mobile Access

At home for the evening, Michael wants to do a quick check on the progress the junior lawyer has made on her assigned section of the document. On his home computer, he opens Internet Explorer® and connects to the Outlook Web Access (OWA) site for Litware's Exchange server. The OWA site is published through Internet Security and Acceleration Server 2006. ISA 2006 provides a number of unique benefits for both security and productivity.

ISA Server 2006 security benefits

When Michael connects to the external URL for the OWA site, he is presented with a Web form to perform Form-Based Authentication (FBA). The IEA server generates and authenticates the form itself, rather than the Exchange Server. Once authenticated, Michael can access the Exchange Server using the credentials he supplied in the form. Because of the capability to authenticate users at the ISA Server 2006 firewall, no anonymous access to the OWA web directories is required for Form-Based Authentication to the Exchange Server, which would be the case with other firewall solutions.

Furthermore, using an ISA Server 2006 functionality known as SSL bridging, when Michael's browser establishes an encrypted SSL session with the ISA 2006 server, ISA decrypts this session so that it can perform application layer inspection on the HTTP traffic. ISA 2006 then establishes an encrypted session with the Exchange Server.

Single sign on with ISA Server 2006

ISA 2006 also provides single-sign on (SSO) capabilities. When Michael subsequently visits Litware's SharePoint Portal Server site, he does not have to enter his credentials again.

Link Translation with ISA Server 2006

When Michael connects to the SharePoint site through ISA, he notices that the URLs that point to internal resources have been modified so that they refer to fully-qualified domain names (FQDNs), such as <http://www.litware.com/sps>, that are accessible from the Internet, rather than <http://litware/sps> (which is accessible on the internal network only). This translation of links occurs automatically at the ISA server without the need to configure the SharePoint Server to provide URLs in SharePoint that are accessible from the Internet. By performing this link translation automatically, ISA 2006 ensures that internal resource names are not exposed on public networks.³²

Using Exchange Hosted Services for Email Encryption

Litware often uses the services of a law firm based in Europe to assist with international legal issues. Michael decides he needs some additional help from the European law firm based in France to finish a section of the contract.

³² For further information on form-based authentication, application layer filtering, single-sign on (SSO), SSL bridging, link translation and other features of ISA Server 2006, see the [Microsoft ISA Server 2006 Evaluation Guide](http://www.microsoft.com/isaserver/prodinfo/guide.mspx) at <http://www.microsoft.com/isaserver/prodinfo/guide.mspx>.

Document metadata removal to protect confidentiality

Before sending the document to the partner law firm, Michael needs to ensure that he takes efforts to preserve the confidentiality of companies that will be signing the contract. He further needs to ensure that document metadata does not unintentionally leak details that could compromise confidentiality and the privacy of individuals, for example, through tracked changes or reviewers' comments. To remove the hidden metadata, Michael uses the Remove Hidden Data add-tool, available for Office XP and Office 2003.³³

Michael will maintain client confidentiality by removing references to the companies' identifiable information in his correspondence. Because encryption of email correspondence between Litware and its clients and partners also is necessary to maintain confidentiality and regulatory compliance, Litware has invested in Exchange Hosted Services to provide this and other services, such as hosted spam and anti-virus filtering, email archival and email continuity.³⁴

Email confidentiality with Exchange Hosted Services

The sending of encrypted emails is completely transparent to the sender. Michael sends an email to the European law firm asking for advice on the language of a particular section of the contract. For the outbound email to the European law firm, Litware's Exchange Server automatically establishes a Transport Layer Security (TLS) encrypted tunnel with the Microsoft global network where the message is encrypted according to rules configured in the Microsoft Exchange Hosted Services module. The recipient's email address is used as the public key to encrypt the email. The private key that is required to decrypt the email is bound to the public key and is stored in a secure environment on the Microsoft network.

When the lawyer at the European law firm opens the email, he clicks on an html link in the email. Using a Web browser he verifies his identity and sets a password to gain access to the encrypted email by using a Web-based method. The private key to open the email is made available when the recipient opens the email. The recipient can respond to the message with confidence that the reply will be encrypted.

Technologies

- Office 2003
- Exchange Server 2003

³³ For information on the Remove Hidden Data tool, see [Control Metadata in Your Legal Documents](http://office.microsoft.com/en-us/help/HA011400341033.aspx) at <http://office.microsoft.com/en-us/help/HA011400341033.aspx>. Had Michael been using Office System 2007, he could have used the new Document Inspector feature to remove this data. Document Inspector can be customized to provide added functionality. For more information on Document Inspector, see [Customizing the 2007 Office System Document Inspector](http://msdn2.microsoft.com/en-us/library/aa338203.aspx) at <http://msdn2.microsoft.com/en-us/library/aa338203.aspx>.

³⁴ A primary advantage of Microsoft Exchange Hosted Encryption is that no PKI or client components are required on the part of the organization to send and receive encrypted emails with third parties. Additional benefits of Exchange Hosted Services include elimination of email viruses and spam before they reach the corporate network, email archival and email continuity. For more information on email encryption and on email antivirus and spam filtering, archival and continuity services provided by Exchange Hosted Services, see "[Microsoft Exchange Hosted Services](http://www.microsoft.com/exchange/services/default.mspx)" at <http://www.microsoft.com/exchange/services/default.mspx>.

- SharePoint Server 2007
- SharePoint Portal Server 2003
- Information Bridge Framework (IBF)
- SQL Server™ 2000, service pack 3, for IBF
- Window Server 2003 with Active Directory
- ISA Server 2006
- Exchange Hosted Services
- InfoPath

Product Features

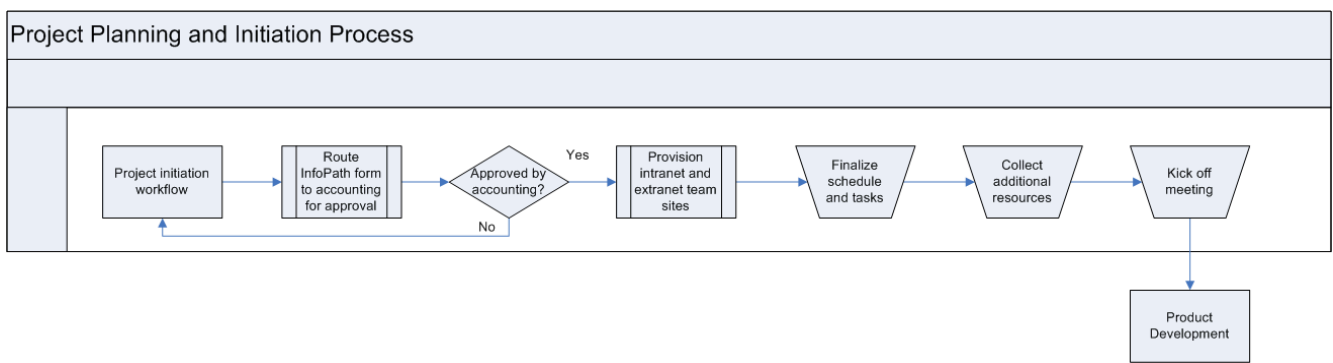
- Active Directory Federation Services (ADFS)
- MOSS Extranet functionality
- Web Services
- Document Libraries
- Document Assembly
- Integration of Office with LOB applications (IBF)
- Single-sign on (ISA Server)
- SSL bridging (ISA Server)
- Forms-based authentication (ISA Server)
- Application-layer filtering (ISA Server)
- Link Translation (ISA Server)
- SharePoint integration with ISA Server 2006

Project Planning and Initiation

Once Contoso and Northwind Traders have agreed upon and signed the contract, Contoso can begin work on the project. Alice Ciccu, the engagement manager at Contoso, subsequently receives an email notification that the contract to perform the tax assessment work for Northwind Traders has been accepted.

To plan and initiate the project, Alice now needs to create the team project site, find team members, assign tasks, find relevant content and perform other activities related to project planning and initiation. These other activities include, among other things, generating a unique activity code for the engagement and obtaining budget approvals.

The following diagram illustrates the major steps for the project planning and initiation phase of the engagement.



Windows Workflow Foundation and InfoPath customization

For project planning and initiation, Contoso, working with a third-party developer, has implemented a custom solution to automate the tasks associated with the work for this phase. The custom solution includes custom workflows and InfoPath forms, in addition to a custom document management and retention solution. Prior to deploying MOSS 2007, Office System 2007 and the custom solution for project initiation, Contoso faced delays in initiating projects and risked information loss.

Again, Alice starts her task by logging on to the SharePoint site and launching an InfoPath form. The form provides a number of fields for required and optional information. Data validation is performed on the form to ensure that information is entered correctly and accurately, minimizing the risk to data integrity.

Integration with LOB applications

She populates some of the data required for the form by selecting items from drop-down lists, which changes values in a number of fields and causes other fields to be displayed dynamically as a result of data she enters. Alice enters details about the tax assessment project, including client name, project type, budget items, start and end dates, and other information. After reviewing the form for accuracy, she clicks the Submit button. By doing so, she initiates a custom workflow. The first step is to route the InfoPath form to the finance department for approval.

Nancy Flood, a financial analyst for Contoso, notices a new task has appeared on the To Do bar in Outlook 2007.³⁵ She opens the task item and clicks on the embedded link. She is subsequently directed to the InfoPath form that Alice completed. However, as in a previous example, her InfoPath form displays additional fields and information, based on her level of access and role. She enters information required for the finance department and then clicks the custom Approve button in the form.

After Nancy has approved the form, a unique activity engagement code is created and assigned to the project. The form is then routed back to Alice for the next step in the workflow process: the creation of the team site for the engagement.

Alice receives an email notification that the project has been approved and assigned a unique engagement code. From the email, Alice clicks on the embedded link to a Project Initiation InfoPath form, which is pre-populated with data from previous steps in the workflow, such as the client name, project name and project engagement code. She reviews the information and then selects a number of items from drop-down lists, such as Risk and Advisory from the Practice List, Tax Risk Management from the Service Line list and Tax Impact Analysis from the Engagement List.

At the bottom of the form, she clicks on Next and is presented with a form where she can select her core team members from a number of drop-down lists that describe roles. Some values in this form are pre-populated with the names of people who are automatically assigned for review and quality assurance. After clicking on Next at the bottom of this form, she sees another form where she specifies the documents that must be present for the engagement to be closed. She completes this form and clicks on Submit.

Team site provisioning and customization

When she clicks Submit, a complex business process occurs in the background to create the team site. The customized template used to create the site is based on Alice's earlier choice to select Tax Risk Management from the Service Line drop-down list in an earlier form. The site template contents include standard records and document templates, based on the type of engagement, and a baseline project plan. Additionally, the team site creation process assigns permissions to the team members based on their selected roles and also sends emails to the team members informing them of their roles and providing a link to the site.³⁶

Exchange Server 2007 compliance features

In addition to creation of the engagement site, as part of the project initiation, a number of policies are applied to the Exchange Server 2007 organization to meet compliance requirements. The policy enforcement mechanisms include the automated distribution of email folders to team members for the

³⁵ One of the desirable features of Outlook 2007 integration with MOSS 2007 and SharePoint Service v 3 is the bi-directional synchronization of task, calendar and other items. This means that SharePoint tasks that are assigned to you appear automatically in the Outlook 2007 To-Do bar, as well as the Daily Task List in Calendar. For more information on this feature, see "[Overview of Microsoft Windows SharePoint Services and Outlook 2007](http://office.microsoft.com/en-us/outlook/HA100832471033.aspx#4)" at <http://office.microsoft.com/en-us/outlook/HA100832471033.aspx#4>

³⁶ Workflows are highly customizable in MOSS 2007. Consequently, it would be possible at this or other appropriate junctures to include steps that would automatically route a resource assignment request to the scheduling organization to assign and approve personnel for the project.

purpose of records retention and archival, automated journaling of email based on policy conditions, the establishment of email “ethical walls” that prevent email communication between team members and others in Contoso that might be in potential conflict of interest, and other mechanisms available in Exchange Server 2007 to meet compliance requirements.³⁷

From the Contoso engagements portal home page, Alice sees a number of tabs for her frequently used information. Alice clicks on a My Clients tab on the portal home. In the tree view of the My Clients site, which displays a hierarchical view of her clients, Alice expands the Northwind Traders node, and notes that her Team Workspace has been created. Additionally, she also notes an engagement site for a consolidated tax return for Northwind Traders for the most recent fiscal year. Another engagement manager, Rob Verhoff, owns the consolidated tax return engagement site; however, she has access to read the site and recognizes that its content will be useful for her own engagement.

Alice clicks on the Team Workspace she created for the tax-impact analysis and sees the default view, which includes web parts that show information about the engagement: client summary and billing information (pulled from Line of Business applications), a list of default engagement tasks, documents and team members.

Alice needs to add to the Team Workspace before arranging a project kickoff. She needs to find relevant knowledge objects, such as documents and best practice workbooks for various tax jurisdictions, and personnel who possess specific expertise that is currently missing from her team. She also needs to make some adjustments to the tasks and schedule.

Using the MOSS 2007 Search Center, she enters query terms to find people who are fluent in French and have an in-depth knowledge of French regulations. Like Frank Lee, who created the response to the RFP, she discovers that Thierry D’Hers in the Paris office possesses the relevant qualifications.

Unified communications with Office Communicator

Through the presence indicator, she notes that Thierry is online and initiates an IM conversation with him through Communicator. Thierry would like to include his manager in a voice conference call and suggests that they use their desktop phones, which are integrated with Communicator.³⁸

After establishing the call using their integrated desktop phone, Thierry uses Communicator to invite his manager to the conference and follows a wizard to establish the conference.

Now that Thierry is part of the team, Alice adds him to the Team Workspace site for the engagement and assigns him appropriate permissions.

³⁷ For more information on the compliance features of Exchange Server 2007, see the white paper, [Meeting the E-Mail Compliance Challenge With Microsoft Exchange Server 2007](#), at <http://www.microsoft.com/exchange/evaluation/compliance.msp>.

³⁸ Microsoft Office 2005 Communicator enables integration of instant messaging with telephony, in addition to file transfer, application sharing and video conferencing, and is core piece of a unified communications strategy to lower costs and increase productivity. For more information on the strategies, technologies and benefits of unified communication, see [“Microsoft Unified Communications”](#) at <http://www.microsoft.com/uc/Default.msp>. Note that phone conferencing is possible only by using desktop phones, not computer-to- phone or phone-to-computer conversations.

To complete her preliminary work on the engagement site, Alice uses the search center to find the appropriate knowledge objects to add to the site. She sends an email to Rob Verhoff requesting that he grant Read access to the Northwind Traders consolidated tax review engagement site.

Alice must travel to a conference the following day. Because she will not have access to the corporate network for much of the day, she synchronizes her Outlook 2007 calendar and task items with the SharePoint site. Finally, before ending for the day, Alice requisitions an extranet Client Workspace for collaboration with Northwind Traders.

The next day, Alice is on a flight to attend a conference. She still needs to do some work on the tasks and scheduling. She opens Outlook 2007 and makes adjustments to the tasks, deleting some tasks not required according to the firm's policies, and modifying others.

Intelligent Application Gateway benefits

Later that evening in her hotel room, she connects to the hotel's broadband network to complete her work on the project initiation. To do this, she will need to connect to the Contoso network. Her past experiences with access to the corporate network from hotels or client networks used to be less than satisfactory. For example, some hotels lacked robust hardware that could provide adequate support for traditional VPN protocols, such as L2TP over IPSec or PPTP, or they actively blocked the VPN protocols. Even when she could establish a VPN connection, she often lost when other hotel guests established VPN connections, although this cause remained a mystery to her. These issues have disappeared, however, since Contoso's recent implementation of Microsoft's Intelligent Application Gateway (IAG) 2007.

Alice opens Internet Explorer and, in her Favorites list, clicks on the Intelligent Application Gateway (IAG) 2007 portal link. She authenticates to the IAG portal site, where a Web page provides her with a variety of connectivity options. Before choosing one of the connectivity options, she needs to change her soon-to-expire Active Directory password. She does this easily by launching the Credentials Management application for the IAG portal page. When she changes her password here, the password changes in Active Directory and then synchronizes with her other accounts through Microsoft Identity Integration Server 2003. She then chooses a connection option on the IAG portal to connect to the internal network. This establishes a Secure Sockets Layer (SSL) VPN connection to the corporate network that is tunneled in HTTPS.³⁹ She then opens Outlook and synchronizes her content.

Returning to the IAG portal page, Alice clicks on a link that provides access to the SharePoint site. She opens the team engagement site and notes that the extranet client site she requisitioned earlier is now available in a Web part on the site. She realizes that she still needs to finalize the schedule for the

³⁹ The Microsoft Intelligent Application Gateway (IAG) 2007 appliance provides three types of SSL VPN connectivity options: 1) Web proxy publishing of Web applications. This option provides pure browser access and, through the content translation gateway, removes the need for a client component. 2) Socket /port forwarding with SSL Wrapper client component. This option enables access for non-Web applications, such as Native Outlook, Telnet, Citrix and others, and uses ActiveX and Java applet controls for SSL tunneling. 3) Full and transparent VPN access to the corporate network through the Network Connector, which uses the SSL Wrapper component. This last option is similar to Secure Socket Tunneling Protocol (SSTP), which will be available on the next version of Windows Server, Windows Server 2008, and Windows Vista SP1 (not yet released at the time of this writing). For more information on SSTP, please see the [SSTP routing and remote access blog](http://blogs.technet.com/rrasblog/archive/tags/SSTP/default.aspx) at <http://blogs.technet.com/rrasblog/archive/tags/SSTP/default.aspx>.

project kickoff meeting. After checking participant availability, she schedules the meeting and synchronizes the Outlook and SharePoint calendars.

Now that Alice has assembled the team and created the engagement site, which includes documents and other knowledge objects, project tasks, milestones and other necessary supporting elements, she needs to inform her supervisor (the managing partner responsible for the account) of the project status. Alice opens an InfoPath form from the engagement site and completes it. When she submits the form, it is automatically routed to her supervisor, who will give the final approval to proceed.

Finally, before retiring for the evening, Alice connects a headset to her laptop computer and checks her office voice mail through Outlook 2007. While listening to her voice mail, she realizes that she had forgotten to forward calls from her desktop phone to her cell phone before leaving on her trip. She launches Communicator and configures her desktop phone to forward calls to her cell phone.

Technologies

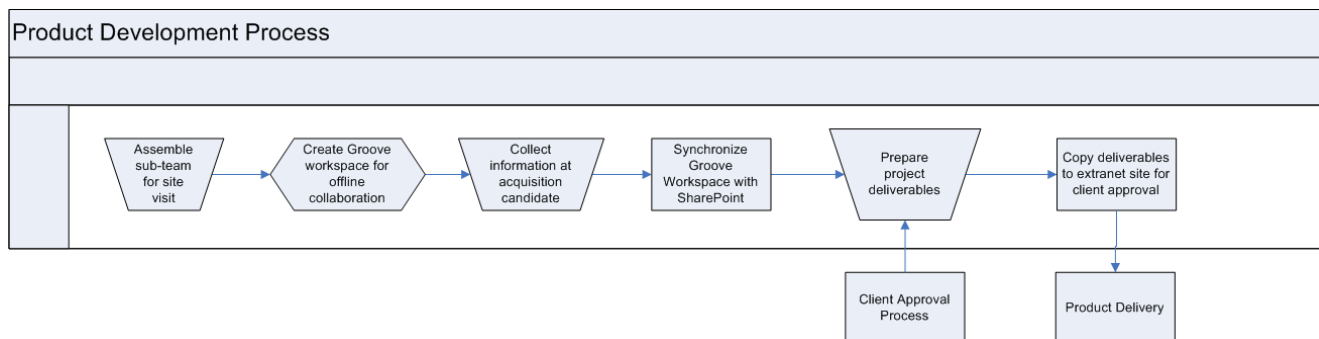
- Office Outlook 2007
- Exchange Server 2007
- Office SharePoint Server 2007
- Office SharePoint Designer 2007
- Office Communicator 2005
- Intelligent Application Gateway (IAG) 2007
- InfoPath 2007

Product Features

- Document Libraries
- Business Data Catalog (MOSS 2007)
- Enterprise Search (MOSS 2007)
- My Sites (MOSS 2007)
- Social Networking Web Parts (MOSS 2007)
- Real Time Presence and Communication
- IM and telephony integration
- Voice mail integration
- Workflow (integration with Outlook and Outlook Tasks)
- InfoPath Personalization
- Outlook 2007 offline cache mode
- Remote Access (SSL VPN)

Product Development

The product development phase of the engagement requires a number of different activities that need to be orchestrated. The following diagram illustrates major parts of this phase of the project.



At the kickoff meeting for the engagement, Thierry D’Hers is assigned an action item that requires him to assemble a small sub team to visit the CFO and Controller of World Wide Importers, the acquisition candidate, at its Strasbourg head office. The goal of the visit is to gather any recent information regarding the disposition of assets and the overall financial health of World Wide Importers. Because no formal purchase offer is yet on the table, this information gathering is preliminary to a formal due diligence process. Notwithstanding this, his visit will be informed by an awareness of the sensitive and proprietary nature of the information he will access.

To prepare for the information-gathering meetings at World Wide Importers, Thierry will need access to colleagues in close geographical proximity who possess the relevant skills and knowledge. He also will need to find appropriate baseline documents, spreadsheets and other knowledge objects to ensure that his team gathers information efficiently, accurately and completely at the acquisition candidate site.

SharePoint Search customization

To begin his preparation for the trip to the Strasbourg office, Thierry logs onto the SharePoint site. He clicks on the Search tab on the portal home. In the Search page that subsequently displays, he clicks on the Knowledge Center tab, a custom tab that was added to limit the scope of queries.⁴⁰ By clicking on this tab, Thierry can use advanced search features to find information by querying on various metadata associated with the objects in Knowledge Center repository.

Thierry finds a variety of template documents, spreadsheets and guidelines related to information gathering at an acquisition candidate site. He downloads and saves these files to his local hard drive. He opens a template document in Word 2007 that contains a number of variables that allow him to populate the document with information, such as the names and addresses of the client and acquisition candidate, pulled from Contoso’s Line of Business applications to ensure accuracy.

Colleague Tracker Web Part / Social Networking

⁴⁰ With SharePoint Services 3.0 and MOSS 2007, searches can be customized easily by limiting the scope of queries or adding data sources, such as file storage areas and databases, without having to write any code.

After completing preparatory work on the documents, he returns to the Contoso SharePoint portal home page. On the SharePoint home page, Thierry sees the Colleague Tracker web part, which lists a customizable list of colleagues. Thierry has organized the Colleague Tracker Web part so that it provides a category for peers who are located in the EU. In the Colleague tracker, Thierry identifies a peer based in Louvaine, Belgium, who would be a useful team member. Through the presence indicator, he sees that his colleague is online and starts an IM conversation with him to confirm availability.

Collaboration with Groove®

Thierry still needs to find another individual to help gather information. He returns to the Search page to find people who are geographically near him and have the appropriate skills. Once he finds these individuals, he can add them to his Colleague Tracker list.

Thierry's next step is to share the preparatory information with his new team. He invokes the Groove® Launchbar from his desktop to create a Standard Workspace. He moves the preparatory information he has collected and modified into the Workspace, and invites the two colleagues who will comprise the remainder of his team to participate in the Workspace. Once they accept the invitation, the content is synchronized and Thierry's team can perform additional work on the documents, while either offline or online. When content is resynchronized, Groove will detect any potential conflicts (if, for example, two people both modify the same document at the same time) and provide methods for resolving them.

Digital signature support in Word 2007

Before traveling to Strasbourg, Thierry receives an email from the Controller of World Wide Importers that asks him to sign an attached confidentiality agreement. After receiving approval from Contoso's legal department, Thierry opens the document in Word 2007 and sees a notification that he is required to provide a signature. He reviews the agreement again, double clicks on the signature line and is presented with the Sign dialog box. He clicks on Select Image to insert a picture of his handwritten signature, and then clicks on Sign in the dialog box to add a digital signature. This last action causes the document to be signed with a digital certificate that has been issued to Thierry by the Contoso CA.⁴¹ If the document is changed later, the digital signature would become invalid.⁴²

At World Wide Importers, Thierry and his team are provided with a meeting room to examine paper records that are supplied to them for the purposes of their information gathering. Network access is available only to World Wide Importer employees by using 802.1x Extensible Authentication over LAN Protocol (EAPOL), which provides port-based authentication for both wired and wireless networks. Consequently, any devices that plug into a network port at World Wide Importers must provide the appropriate credentials in the form of digital certificates issued by the World Wide Importers Certificate

⁴¹ Digital signatures can assert authenticity (identity of the sender), data integrity and non-repudiation. They can, in some instances and jurisdictions, have the same legal force as actual handwritten signatures. However, assertions are not fact, and the degree to which these assertions can be relied upon is based on the amount of trust the recipient (relying party) places in the Certificate Authority (CA) that issues the signing certificates, the measures an organization takes to protect its CA and the practices it employs for issuing certificates. A relying party, the recipient of the signed communication, needs to take these and other factors into consideration before making an explicit and informed decision to trust the certificate.

⁴² For example, if the recipient of the document needs to convert the document to an earlier version of Office, the signature will be rendered invalid.

Authority in order to transmit data on the LAN.⁴³ Because Thierry's team are not issued certificate from World Wide Importers, they do not have network access in the meeting room.

Windows Vista Meeting Space

A number of World Wide Importer employees are present to answer questions and to provide assistance to Contoso's team for the duration of their visit. To collaborate on the information gathering process in the meeting room, the group, including the World Wide Trader employees, establishes a Windows Vista Meeting Space session by using an ad hoc wireless network.⁴⁴ One World Wide Importer employee remembers that on his hard drive he has a presentation that would provide some useful information to Thierry's team and would provide a good starting point for the information gathering. Through Meeting Space, he delivers this presentation to the group.

Groove synchronization

Back at their respective hotel rooms for the evening, Thierry's team continues to work on their assigned documents. These documents are automatically synchronized with one another via Groove when they go online and connect to Contoso's Groove Relay server. (Groove clients try to synchronize in a peer-to-peer manner, whenever possible. However in situations where this is not possible, for example, when clients are offline or are on different networks, the clients will contact the Groove relay server, which provides store and forward data transfer capabilities.)

While traveling home from the meetings, one of Thierry's team members falls asleep on the train and wakes to find his briefcase is missing. The briefcase contains the employee's laptop and smart phone. In the past, this event would have been disastrous because of the confidential information that is stored on the laptop and the smart phone.

BitLocker full volume encryption

However, a number of factors mitigate the risk to data confidentiality resulting from the unfortunate loss of the laptop and smart phone. The first is that the BitLocker feature of Vista provides full-volume encryption of the data on his laptop. The BitLocker protection on the employee's computer relies on multifactor authentication provided by the hardware-level protection of the Trusted Platform Module (TPM) version 1.2 and a PIN. For the BitLocker encryption to be compromised, the thief would have had to install malware before BitLocker was enabled or know the PIN.⁴⁵ Fortunately, the night before, the employee had synchronized his data through Groove, and the project information was not lost.

⁴³ In many situations, IPSec is a more secure alternative to 802.1x EAPOL. A more robust alternative is Network Access Protection (NAP), which makes it possible to perform health checks before allow LAN access. NAP will be available with Windows Vista and Windows Server 2008. For more information, see [Network Access Protection](http://www.microsoft.com/technet/network/nap/default.mspx) at <http://www.microsoft.com/technet/network/nap/default.mspx>.

⁴⁴ Windows Meeting Space is a new feature of Windows Vista that allows users to share files, applications and even desktops with one another. Because Meeting Space is based on peer-to-peer technologies, it does not require the presence of a server.

⁴⁵ For more information on these and other features of BitLocker, see [BitLocker Drive Encryption Technical Overview](http://technet2.microsoft.com/WindowsVista/en/library/ba1a3800-ce29-4f09-89ef-65bce923cdb51033.mspx?mfr=true) at <http://technet2.microsoft.com/WindowsVista/en/library/ba1a3800-ce29-4f09-89ef-65bce923cdb51033.mspx?mfr=true>. Also see the [Data Encryption Toolkit for Mobile PCs](http://www.microsoft.com/technet/security/guidance/clientsecurity/dataencryption/default.mspx) at <http://www.microsoft.com/technet/security/guidance/clientsecurity/dataencryption/default.mspx>.

Windows Mobile security features

The second factor that mitigates risk to confidentiality is the smart phone's Windows Mobile 6.0 operating system, which has enhanced security features that Contoso has implemented. The storage card on the mobile device is encrypted. Contoso Administrators can issue kill bit commands to the device to perform a remote wipe. However, because communication needs to be established with the cell phone to issue kill bit commands, Contoso does not want to rely on this method alone to protect data confidentiality on mobile devices. It also requires that mobile devices be configured to perform a local reset and wipe of the data after a pre-configured number of unsuccessful attempts to unlock the phone.⁴⁶

Groove security features and integration with SharePoint

With his team's tasks complete, Thierry needs to close down his team. Within Groove, Thierry sends his team members a message that he will "uninvite" them from the Groove workspace. In the message, he reminds them to securely destroy (digitally shred) any documents that they may have copied outside the Groove workspace, as per Contoso policy and the terms of the agreement with World Wide Importers regarding the disposition of confidential data. Once he uninvites his team, the Groove workspace is automatically removed, along with the files it contains, from the participants' computers.⁴⁷ Finally, Thierry adds the SharePoint Files tool to his Groove workspace and automatically synchronizes the Workspace content with the document library in the team engagement site.

Although Thierry still has some more work to do with the information he has obtained from World Wide Importers, the initial data he collected is available for the team to use. In reviewing the documents that Thierry has posted to the engagement site, Lorraine decides to ask another team member, Mike Fitzmaurice, to analyze the risks and benefits of World Wide Importers' management of shipping container leases and purchases, as well as various real estate transactions.

SharePoint Alerts

Mike opens one of the documents that Thierry has placed on the engagement site. He sees that the document is still a work in progress and that Thierry needs to do some more work on it. Rather than spend time on this document now, Mike sets an Alert on the document so that he will be notified when someone other than he changes it. He then moves on to work on the other documents that Thierry has added to the workspace.

⁴⁶ For more information on the security features of Windows Mobile 5.0 with the Messaging and Security Pack Feature (MSPF), see the white paper, [Mobile Messaging and Business Application Solutions with Windows Mobile: Addressing Key Questions](http://www.microsoft.com/windowsmobile/business/strategy/mobilemessaging.mspx) at <http://www.microsoft.com/windowsmobile/business/strategy/mobilemessaging.mspx>. Note that Windows Mobile 6.0 supports these and other features as well.

⁴⁷ Groove has a number of enhanced security features to ensure data confidentiality and integrity. Data in Groove workspaces is encrypted and only accessible with the appropriate authorization. For example, Groove supports the use of smart card authentication. Data is digitally signed to ensure integrity. Finally, when a user is uninvited, a new cryptographic key is generated for the Groove data encryption and sent to remaining members to ensure that the uninvited member does not have access to current or subsequent workspace data. For more information on Groove security features, see the Groove [Security FAQ](http://www.groove.net/index.cfm?pagename=Security_FAQs) at http://www.groove.net/index.cfm?pagename=Security_FAQs.

Another task that Mike performs is a review of Northwind Traders' tax-related data. Because Contoso has performed tax-related activities for Northwind Traders in the past, Mike knows that he can locate this data in the records management repository. To find this information, Mike clicks on the custom Retained Records tab on the Contoso portal home page.

SharePoint Records Center site template / Enterprise Content Management

The records management repository is based on the Records Center site template provided by MOSS 2007.⁴⁸ Managed by Contoso's internal legal department, this site was planned with the assistance of various stakeholders, including the compliance officers, managers, information workers and the IT department. The legal department determines how files are routed to the records center based on *Content Type* (a new addition to Windows SharePoint Services 3.0 and MOSS 2007 and discussed in more detail below), tracking who can access records, what actions are audited, when content expires, and what happens when content expires, for example, launching a disposition approval workflow.⁴⁹ The legal department also determines what metadata must be present for a document to be successfully submitted to the records center. If the required metadata is not present, the submitter will be prompted to provide it. This control helps to ensure that records are stored accurately and completely.

SharePoint Content Type

Content Type is an important new feature of WSS 3.0 and MOSS 2007. It is central not only to appropriate routing of documents transferred to the records center, but also to enforcing policies, such as retention periods, for the documents themselves. Importantly, Content Type overcomes barriers to providing a solution for automating the classification of documents, which in turn helps organizations achieve better compliance.

Every document in a document library or list item in a list has the same schema, making it difficult for the system to distinguish between, for example, public and confidential documents within the same library. By attaching a Content Type to individual documents or list items, it is possible to specify a schema for the document or list item that is independent from other items in the library or list. Because policies also can be attached to content of a particular type, documents and other objects can have appropriate policies, such as workflows, expiration dates, resulting actions, and others applied to them. This makes it possible to achieve higher degrees of automation in managing information, reducing the risk of error and increasing the integrity of information.⁵⁰

⁴⁸ Records Management is just one of the key components of the Enterprise Content Management (ECM) solution provided by MOSS 2007. Other components include Document Management, Forms Management and Web Content Management. For more information on the topic of ECM and Microsoft solutions, see the white paper [Enterprise Content Management: Breaking the Barriers to Broad User Adoption](http://office.microsoft.com/en-us/sharepointserver/HA102063591033.aspx?pid=CL100796281033) at <http://office.microsoft.com/en-us/sharepointserver/HA102063591033.aspx?pid=CL100796281033>

⁴⁹ The Disposition Approval workflow is a default workflow available out of the box with MOSS 2007. For more information on the Disposition Approval workflow, see [Use a Disposition Approval Workflow](http://office.microsoft.com/en-us/sharepointserver/HA101544291033.aspx?pid=CH101782961033) at <http://office.microsoft.com/en-us/sharepointserver/HA101544291033.aspx?pid=CH101782961033>

⁵⁰ For more information on the Content Type feature, see [Introduction to Content Types](http://msdn2.microsoft.com/en-us/library/ms472236.aspx) at <http://msdn2.microsoft.com/en-us/library/ms472236.aspx>.

The records center comprises a number of libraries that are each associated with different records policies and represent the various categories of records. Mike knows he can find the data he is looking for in the Client Supplied records category. He clicks on the item in the Web Part in the records center, locates and opens a client-supplied Excel® workbook for the last fiscal year. This spreadsheet lists capital gains and losses for the European subsidiary of Northwind Traders.

Document Information Panel

When Mike opens the workbook, he notes a policy statement that appears at the top of the document in the information panel, which indicates how long the record will be retained and other relevant information. Examining the workbook, Mike notices that one of the transactions should not be recorded because the sale date occurs in the next fiscal year.

Records center auditing and document version control

Normally, once documents have become records and deposited in the Retained Records site, they are not modified. However, in this case, the record is one that has been supplied by the client and must be modified. In any event, the audit settings on the document library keep a detailed record of actions performed in the library, including who viewed an item in addition to information on events related to the modification of objects in the library. Furthermore, MOSS 2007 will preserve versions of the document so that when the document is updated, both versions will be preserved.⁵¹

Mike closes the workbook and then clicks on the workbook object in the document library to invoke the drop-down list. From there, he checks out the document.

Real-time collaboration with Live Meeting

Mike needs to discuss this document, as well as a number of other issues, with Northwind Traders. He schedules a Live Meeting session and invites participants from Northwind Traders and the engagement team.⁵² During the Live Meeting session, Mike shares the Excel workbook he previously checked out from the Retained Records site. Following feedback from the Northwind Traders attendees, Mike updates the workbook to correct the data and adds a note indicating the date and time when the change was authorized and by whom. The Live Meeting session is being recorded, so Mike also will have a supporting record to indicate that the change he made to the client-supplied data was authorized at the meeting.

Site customization and personalization

⁵¹ The Records Center site template has a number of built-in features to ensure data security. For example, the system does not modify data, ensuring that records uploaded and subsequently downloaded are identical, byte for byte. It automatically makes versions of any changes made to documents and audits specific types of changes, preventing intentional or unintentional data tampering. Records managers can add and maintain metadata separate from the underlying document. This makes it possible to update metadata associated with the document without modifying the document itself. Changes to this metadata can be audited as well.

⁵² Live Meeting is a Web conferencing service that allows real-time online collaboration with attendees in diverse locations. For more information on the features and benefits of Live Meeting, see the [Microsoft Office Live Meeting Guide](http://office.microsoft.com/en-us/livemeeting/HA102020561033.aspx?pid=CL101731541033) at <http://office.microsoft.com/en-us/livemeeting/HA102020561033.aspx?pid=CL101731541033>.

During the Live Meeting session with Northwind Traders, Mike and Alice introduce the client extranet site that was created for this engagement to the Northwind Traders participants. Mike shares out his Internet Explorer in the Live Meeting session to explain the various elements of the client extranet site. Mike and Alice point out that the extranet site is very similar to the internal engagement site; for example, it includes a Web part showing the engagement tasks. The content displayed in the extranet site is targeted for external consumption, however, so it limits display of content items to only those that are acceptable for external use by external Northwind Traders employees. The site also uses audience-targeting features that will display Web parts appropriate for the current user.

Mike and Alice explain that they would like any additional client documents to be uploaded to this site. Additionally, they explain that they will initiate workflows from the client extranet site to obtain necessary approvals from Northwind Traders for the final deliverables. Also, they explain that Northwind Traders can view project timelines and status reports on the extranet site.

Don Hall, the Northwind Traders CFO, mentions that Northwind Traders is working on a project to use CardSpace to authenticate customers to its Web site. He wonders whether it would be possible for Contoso and Northwind Traders to explore the possibility of piloting a project to allow Northwind Traders employees to use CardSpace to authenticate to the client extranet site. Alice agrees to send a message to the Contoso CIO to ask him to get in touch with his counterpart at Northwind Traders about this topic.

Document versioning

After the meeting, Mike returns to the Retained Records site and checks in the revised workbook. Because he has changed a significant piece of information in the workbook, during the check-in process, he designates that the revised workbook is a new major version, rather than a minor version.⁵³ After checking in the document to the Retained Records site, Mike copies it to the client extranet workspace, where the document will form part of the supporting materials for the client deliverables.

Meanwhile, Alice Ciccu, the engagement manager, realizes she could benefit from some assistance on the engagement in the form of additional research and review of spreadsheet formulas. An intern, Monica Brink, who was hired to provide assistance in updating the Wikis, blogs and other information that comprises the centralized encyclopedia for Contoso employees, joins the team for the remaining duration of the engagement.

When Monica was hired, she was provided with a laptop that was installed with the base operating system, in this case, Windows XP SP2. However, to perform her duties, she needs access to Office System 2007 applications, so that she can directly interact with information stored on the SharePoint site within applications such as Word and Excel without having to download the information. For example, she can directly edit blogs by using Word 2007 and can configure Outlook 2007 to receive Really Simple Syndication (RSS) feeds from the Contoso portal.

SoftGrid: Software as a Service

⁵³ Versioning on document libraries can be configured to preserve only major version or both major and minor versions. Additionally, security can be configured so that only a subset of users can access minor versions. For more information on document versioning available in WSS 3.0 and MOSS 2007, see [Track Versions of a File in SharePoint Library](http://office.microsoft.com/en-us/powerpoint/HA102085851033.aspx) at <http://office.microsoft.com/en-us/powerpoint/HA102085851033.aspx>

Rather than install Office System 2007 applications on her laptop, the IT department uses SoftGrid to deploy a virtualized version of the applications she needs. Contoso chose to implement SoftGrid as part of their ongoing efforts to gain tighter control over and reduce costs associated with software deployment, software inventory and licensing, and desktop security, among other benefits.

SoftGrid allows Contoso to implement software as a service (SaaS). The applications that Monica needs are streamed, on-demand in real-time, from the SoftGrid server and executed locally. Because the streamed applications are also cached locally, Monica has access to them even when she is not plugged into the Contoso network.

SoftGrid benefits

The virtualized applications are centrally managed and provisioned to her, based on her Active Directory group memberships. Consequently, her access to the virtualized applications will end when her Active Directory account expires at the end of her internship.

Even though the applications run locally, they execute in an isolated “sandbox” that protects the underlying operating system and prevents collisions with other locally installed applications. Any damaged applications can be refreshed instantly through SoftGrid. As a consequence, Contoso has significantly reduced the time it takes to test application compatibility before deployment.⁵⁴

Granular SharePoint permissions

Through an automated provisioning process, Monica is granted limited access rights to the engagement site. Because Monica has only the SharePoint View Item permission on the document library containing the worksheets, Monica can view workbooks only in a Web browser or the Excel snapshot viewer, but cannot download the workbooks or see the details that underlie the data. Additionally, she only can see only portions of the workbook that have been marked as viewable during the publication process. Because one of her tasks is to assist in the review of formulas used in the workbooks, she needs additional access and requests that Mike Fitzmaurice grant her additional permissions.

Mike Fitzmaurice subsequently grants Read permissions to Monica for the workbooks he is working on for the tax analysis. The Read permissions allow her to download a copy of the workbooks and see the data and underlying details. However, she cannot save changes to the workbook back to the centralized copies of the workbooks. This provides her with sufficient access to assist Mike with a review of formulas that the workbooks employ. If her role in assisting with the workbooks expands, Mike can grant her additional access.

Excel Services benefits

Prior to deploying Excel Services, a new feature of MOSS 2007, Contoso encountered many challenges managing its spreadsheets. The integrity and confidentiality of the data in the workbooks was a particular concern. Many copies of workbooks were circulated via email and other mechanisms, making it often impossible to know which workbook was the authoritative version. Additionally, there were very real risks that copies of the workbooks could inappropriately expose proprietary data and methods. With Excel Services, Contoso can maintain single, authoritative versions of workbooks that serve as official business documents.

⁵⁴ For an overview of Microsoft SoftGrid, see the white paper, [Application Virtualization: The Next Frontier](http://download.microsoft.com/download/e/4/4/e4442c9f-30d9-41f3-9876-82bbfc5aa4e6/datasheet-sgav.pdf) at <http://download.microsoft.com/download/e/4/4/e4442c9f-30d9-41f3-9876-82bbfc5aa4e6/datasheet-sgav.pdf>.

Excel Services is a server-based technology that allows Contoso to centralize its workbooks to provide a means for sharing them securely among multiple users, and to provide a means for better ensuring integrity and confidentiality of spreadsheet-based data. When an end user opens a workbook, the server loads a read-only instance of the workbook in memory and creates a session for the users. If multiple users open the workbook at the same time, none of their activities, such as filtering views, affect other users. And, despite the read-only nature of the workbooks, workbook authors can make cells editable so that users can perform calculations and modeling for themselves. Authors also can select objects in the workbook they want to be public, for example, pivot tables, charts, sheets, lists, etc. Calculations are performed on the server and, depending on the permissions, are hidden so that confidential information is not exposed.⁵⁵

Auditing for compliance

Importantly, Excel Services improves Contoso's ability to meet compliance requirements.⁵⁶ Because Excel Services is integrated with SharePoint, spreadsheet access events, such as open, create, modify and delete, can be stored in a central audit log to provide accountability and transparency.⁵⁷

⁵⁵ For more information on Excel 2007 and Excel Services, see the [Excel 2007 Information Center](http://msdn2.microsoft.com/en-us/office/aa905419.aspx) page at <http://msdn2.microsoft.com/en-us/office/aa905419.aspx>.

⁵⁶ For more information on the topic of Excel Services and regulatory compliance, see the white paper, [Spreadsheet Compliance in the 2007 Microsoft Office System](http://office.microsoft.com/en-us/excel/HA102132911033.aspx?pid=CL100570551033) at <http://office.microsoft.com/en-us/excel/HA102132911033.aspx?pid=CL100570551033>.

⁵⁷ Out of the box, auditing occurs at the document library level, not at the cell level, within the spreadsheet. It is possible, however, to develop a custom solution that could provide cell-level, client-side auditing capability. For a brief, general description of what such a solution might entail, see the section titled "Extensibility Scenario: Spreadsheet Integrity" in the white paper, [Compliance Features in the 2007 Microsoft Office System](http://www.microsoft.com/downloads/details.aspx?FamilyID=D64DFB49-AA29-4A4B-8F5A-32C922E850CA&displaylang=en), at <http://www.microsoft.com/downloads/details.aspx?FamilyID=D64DFB49-AA29-4A4B-8F5A-32C922E850CA&displaylang=en>.

This white paper also provides scenarios that show how to develop solutions that allow client-side auditing of documents checked out of SharePoint libraries to provide a complete audit trail of document usage. Custom audit solutions can be built that allow the detection of suspicious activity that indicates potential spoliation (deliberate destruction of data). Also, the extensible format of 2007 Office System allows the creation of a separate document part that stores audit information, making it possible to preserve the audit trail of a document when it is removed from SharePoint.

Technologies

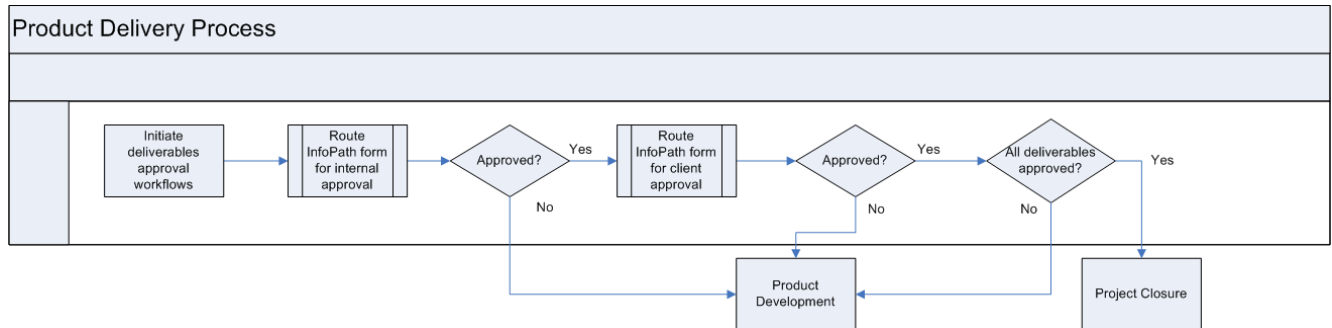
- Office Communicator 2005
- Office Outlook 2007
- Exchange Server 2007
- Groove
- Office Live Meeting
- Office SharePoint Server 2007
- Office SharePoint Designer 2007
- Rights Management Services (Windows Server 2003)
- SoftGrid
- InfoPath 2007
- Windows Mobile 6.0
- Windows Vista

Product Features

- Application Virtualization (SoftGrid)
- Auditing
- BitLocker full volume encryption
- Business Data Catalog
- Content Type metadata
- Enterprise Content Management
- Document Versioning
- Enterprise Search and Search Customization
- Excel Services
- Mobile Device Security
- My Sites
- Offline Collaboration (Groove)
- Real-time Collaboration (Live Meeting)
- RMS Integration with SharePoint
- Social Networking Web Parts
- Real Time Presence and Communication
- Workflow
- InfoPath Personalization

Product Delivery

Like other project phases, the product-delivery phase relies on automated workflows to ensure compliance with business rules and that all necessary approvals are gathered before the project can be completed. The following diagram shows the major steps in this phase.



Mike completes work on an Excel spreadsheet that provides details of recent capital asset transactions at World Wide Importers, based on the data from Thierry D’Hers and his team. At this point, he needs to initiate a workflow to get final approval for the workbook from Alice Ciccu, the engagement manager, and Don Hall, the CFO of Northwind Traders.

Send To menu customization

To initiate the workflow from the extranet client site, Mike first needs to copy the IRM-protected snapshot version of the spreadsheet to the appropriate document library on the extranet client site. It’s easy for Mike to copy files from document libraries on the internal engagement site to the appropriate libraries through the addition of a custom Send To destination that appears on the short-cut menu for documents in the library.

Using a custom Send To destination on short-cut menus for documents offers a number of advantages. By using the menu, users do not need to remember (or cut and paste) URLs that point to the destination. This also helps to eliminate errors and reduce the risk to data confidentiality. Also, when copying the file by using the Send To short-cut item, the copy maintains a relationship with the source file, making it possible for users to choose to update the copy with changes made to the source file.⁵⁸

Mike clicks on the workbook document to access the Send To short-cut menu to copy the file to the client extranet site. When he clicks on the short cut, he sees the destination address and document name, which he can change if he desires. On this page, he also can configure a notification to be sent to him when someone checks in the document, and can configure an alert when changes are made. Mike decides to leave the document settings as they are and copies the document to the extranet destination.

RMS integration with SharePoint

⁵⁸ Adding a custom Send To destination does not require any programming and can be configured by site administrators or list managers. For more information on the topic of the custom Send To menu items, see [Specify a Send To destination for a library](http://office.microsoft.com/en-us/sharepointtechnology/HA101208501033.aspx) at <http://office.microsoft.com/en-us/sharepointtechnology/HA101208501033.aspx>.

The document library that contains the source document has Information Rights Management (IRM) protection.⁵⁹ Documents are stored in unencrypted format, which allows them to be crawled for searches without the need for custom solutions. However, when someone downloads or checks out the document, IRM encryption and permissions are automatically applied at that time.

The IRM permissions result from two sources, from permissions the user has made to the document library or list, and from the specific IRM restrictions configured for the library or list (such as whether or not users are allowed to print documents). For example, if a user has Full Control permissions to a library, he will have Full Control IRM permissions on the document, which allows him to manage the IRM permissions on the document itself. Likewise, when a user has only View Item permissions, he will have Read IRM permissions to the document and can read but not copy or edit its contents.

The IRM restrictions that can be applied to the library or list also include whether to allow printing and/or programmatic access to the document. The IRM restrictions also can be configured to force users to acquire a new license to consume IRM-protected content after a specified number of days, and to remove IRM protection after a specified date. For example, if a company needs to protect information up to a certain date, it can use the latter setting to make the content publicly available at that time.⁶⁰

Because IRM protection travels with the document, even when copied from one library to another, Mike will need to perform some additional steps to ensure that the copied document on the client extranet site has the appropriate permissions so that the target audience can open it. For example, Mike will need to remove IRM protection from the document if the intended audience can't consume IRM-protected content. Fortunately, Contoso and Northwind Traders have established an RMS trust between their organizations by subscribing to the GigaTrust RMS Federated Service.⁶¹ This makes it possible for users in either company to exchange and consume IRM-protected content, regardless of its source.

Mike accesses the client extranet site and opens the copy of the worksheet. From within the document, he adds IRM appropriate permissions for both Northwind Traders and Contoso employees. Mike sees that he also needs to add explicit IRM permission even for Contoso employees who have IRM permissions on the document library containing the source document. He gives Don Hall, the Northwind Traders CFO, full-control permissions to the document, since Don is ultimately responsible for accepting the deliverables from Contoso. He then configures other IRM permissions as appropriate for

⁵⁹ Note that it is **not** possible for Excel Services to load IRM-protected workbooks. Even if a workbook is loaded into Excel Services and then subsequently IRM-protected, you will get an error message if you try to perform any action that requires Excel Services, such as open a snapshot. However, one way to take advantage of both IRM and Excel Services is to open a snapshot of a workbook that isn't protected with IRM and then save the snapshot into an IRM-protected document library. As with many products and product features that confer significant security benefits, IRM requires careful planning before implementation.

⁶⁰ For more information on the topic of IRM permissions in SharePoint, see [Information Rights Management in Windows SharePoint Services Overview](http://msdn2.microsoft.com/en-us/library/ms458245.aspx) at <http://msdn2.microsoft.com/en-us/library/ms458245.aspx>. Also see [Apply Information Rights Management to a List or a Library](http://office.microsoft.com/en-us/sharepointserver/HA101541481033.aspx) at <http://office.microsoft.com/en-us/sharepointserver/HA101541481033.aspx>.

⁶¹ For more information on this and other services available from GigaTrust, see the white paper, [GigaTrust: Breaking Down the Barriers to Deploying Windows Rights Management in the Enterprise](http://www.gigatruster.com/docs/GigaTrust_White_Paper.doc) at http://www.gigatruster.com/docs/GigaTrust_White_Paper.doc.

review.⁶² As an alternative, when users with insufficient permissions open IRM-protected content, they see an option to notify an administrator to request permissions.

To initiate a workflow to receive client approval for the document, Mike clicks on Workflows from the Office Button within the document. In the Workflows dialog box, he sees a number of options available for the document. He starts the Client Approval workflow. In the Client Approval dialog box, he accepts the default values for the approvers, Alice Ciccu and Don Hall, and the due dates, and clicks Start.

Alice Ciccu sees a new task assigned for her in the To Do bar of her Outlook client. She opens the task item and clicks on the link to the document on the client extranet site. Using Windows authentication to connect to the extranet, the single sign-on experience is completely transparent to her. Because Mike explicitly granted her appropriate IRM permissions on the extranet copy, she can open the document to review and modify it if necessary. When she opens the document, she notes that the Document Information Panel in the worksheet identifies the IRM policy as Client Confidential. After reviewing the worksheet, she clicks on the button to edit this task in the Document Information panel, adds some comments and clicks Submit.

After Alice has completed her task in the workflow, the system sends an automated email to Don, with information for completing the final tasks in the client approval workflow. At Northwind Traders, Don opens the email and clicks on the embedded link to open the document on the Contoso client extranet site.

SharePoint support for multiple authentication methods

To gain access to the document in the extranet client site, Don will need to provide appropriate authentication credentials. but since he is not a Contoso employee, he cannot authenticate to the site using Windows authentication. However, MOSS 2007 supports the use of multiple authentication methods to allow internal and external users to connect to Internet-facing sites, making it possible to configure the extranet site to support Windows authentication for internal users and another method, such as Forms Based Authentication (FBA), for external users.

Windows CardSpace

In previous versions of SharePoint, users could not gain access to SharePoint sites without using a Windows identity. However, WSS 3.0 and MOSS 2007 are based on ASP .NET 2.0 and .NET Frameworks 3.0 technologies. ASP .NET 2.0's pluggable authentication provider capability allows the use of security principals (user objects) stored in Active Directory, SQL Server, LDAP directory, or any directory that uses an ASP .NET 2.0 Membership Provider for authentication. The Membership Provider can be customized so that SharePoint can provide enhanced authentication support for heterogeneous environments.⁶³

⁶² To change IRM permissions on an IRM document copied to a different library, Mike needs a high degree of permissions on both libraries, regardless of whether or not IRM protection is enabled on the destination library.

⁶³ For information on this topic and on how to configure a site to support more than one authentication method, see the MSDN blog, [Configuring Multiple Authentication Providers for SharePoint 2007](http://blogs.msdn.com/sharepoint/archive/2006/08/16/configuring-multiple-authentication-providers-for-sharepoint-2007.aspx) at <http://blogs.msdn.com/sharepoint/archive/2006/08/16/configuring-multiple-authentication-providers-for-sharepoint-2007.aspx>.

As per Don's earlier request, the IT departments at Contoso and Northwind Traders have been collaborating to provide an authentication solution for extranet clients based on Windows CardSpace (formerly known as InfoCard).

When Don opens the email to complete the workflow, he clicks on the embedded link to allow him to access the document. His browser opens and is directed to a Web page where he sees a form that asks him to submit an information card; he is not asked to present any credentials in the form of a username or password. He clicks Submit on the Web page form. On his Windows Vista desktop, the Windows CardSpace dialog box opens.⁶⁴

CardSpace security features

He notes that his underlying desktop appears "grayed out," a visual indication that CardSpace is running in a separate, private desktop to provide protection against malware, which might be running in his desktop session in an attempt to compromise his privacy and the security of his information.

In the Windows CardSpace dialog box, he sees a number of information cards. With the exception of the managed card that Northwind Traders issued to him for the purpose of authenticating with the Contoso extranet site, all of these cards are grayed out. This indicates that these cards do not meet Contoso's requirements for authenticating at the client site.

A lock icon on the information card indicates that Don has optionally PIN protected the information for the Contoso log in.⁶⁵ He unlocks the card with the PIN and clicks Send in the Windows CardSpace dialog box.

Upon clicking Send, the information represented by the card is bundled into a token comprising XML data, encrypted, digitally signed and time stamped. When the Web site receives the encrypted message, it decrypts the token with the site's private key and examines the digital signature and timestamp. This process ensures both the confidentiality and the integrity of the message, and verifies by means of the time stamp that the message is not a form of replay attack.⁶⁶

Once Don has authenticated to the client extranet Web site by using a cryptographically strong token to verify his identity, he can open the workbook for review and approval. Seeing that the workbook meets his requirements, he approves it, completing the workflow for the document. After Don has updated the document, Mike receives an email notification regarding the approval. As well, when Mike visits the document library, he can see that a Client Approval column provides a visual indication that the document was approved.

⁶⁴ The client requirements for CardSpace are Windows Vista, Internet Explorer 7.0 with .Net Frameworks 3.0, or Firefox 2.0 with a CardSpace add-in.

⁶⁵ It's also possible to protect the card with an X.509 certificate stored on a smartcard, if higher levels of security are desired.

⁶⁶ For a general introduction to CardSpace, see [Introducing Windows CardSpace](http://msdn2.microsoft.com/en-us/library/aa480189.aspx) at <http://msdn2.microsoft.com/en-us/library/aa480189.aspx>. For a number of useful links to more detailed information on CardSpace, see the [Windows CardSpace \(formerly "InfoCard"\)](http://msdn2.microsoft.com/en-us/winfx/aa663320.aspx) Web page at <http://msdn2.microsoft.com/en-us/winfx/aa663320.aspx>.

Technologies

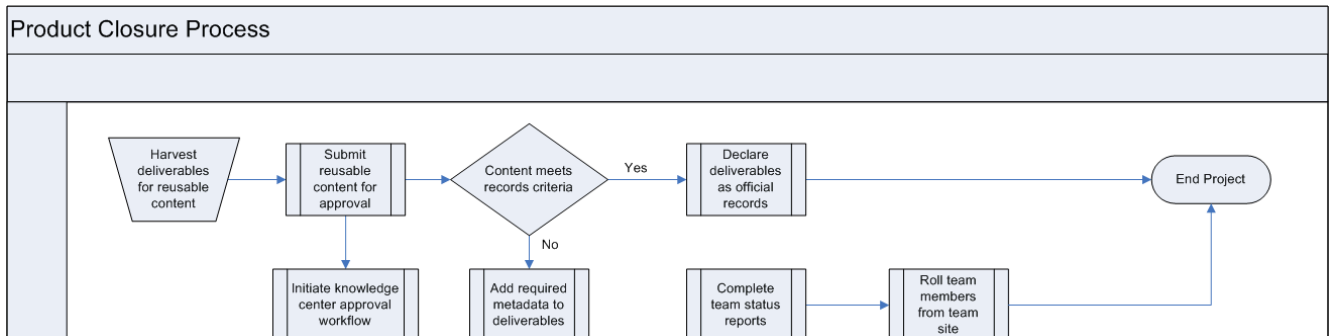
- Windows CardSpace
- Exchange Server 2007
- Office SharePoint Server 2007
- Office SharePoint Designer 2007
- Rights Management Services (Windows Server 2003)
- InfoPath 2007
- Windows Mobile 6.0
- Windows Vista

Product Features

- Pluggable Authentication Providers (ASP .NET 2.0 Membership Providers)
- Enterprise Content Management
- Excel Services
- RMS Integration with SharePoint
- RMS Federation
- Workflow

Project Closure

The project-closure phase requires a number of workflows that must be coordinated before the closure can be approved. The following diagram illustrates these major steps.



With all the deliverables approved by the client, Alice Ciccu needs to close the engagement. This process involves a number of general steps, including:

- Working with her team to harvest the client deliverables and internal work papers that contain best practice content for placement in the Contoso Knowledge Center. The Knowledge Center is a MOSS 2007 Enterprise Document Repository that provides a central location for reusable content.
- Providing performance feedback in response to individual self-assessments that team members perform as they roll off the project.
- Converting project documents to records by submitting them for retention and archival in the Retained Records repository. These documents include the client deliverables, work papers marked as prepared by the client, internal work papers, memos, email and other records associated with the project. The Retained Records repository is implemented with the Records Center template, which implements the Records Center Web service.

Closing an engagement is a complex process, with many specific tasks that Alice and her team will need to perform successfully.

Official records declaration and disposition

Records disposition, in particular, is a critical task that must meet compliance requirements. Official records must be stored securely, accurately and completely in an unaltered state that preserves their integrity. Records disposition often require cumbersome processes, policies and ever-increasing amounts of information.

Organizations and their employees must appraise engagement and other documents to determine the need to archive them as official records, and to determine their ultimate disposition with regard to their classification or reclassification and their scheduled archival lifetime, which can be measured in years for some content types. The scope of information is broad and includes content generated both internally and externally, as well as different formats, such as email, spreadsheets, and so on.

The disposition of records also requires mechanisms to provide notification to agents of primary responsibility prior and subsequent to the destruction of records, and to provide a means to survey records routinely for reappraisal, reclassification and destruction. Finally, records disposition requires

the ability to place holds on specific content so that the integrity of records can be assured during, for example, a discovery process resulting from a civil law suit or an internal or external audit process.

Contoso adopting the infrastructure optimization model to provide a guide for achieving higher levels of optimization. One of its goals was to reduce risk of errors associated with complex and critical tasks, such as records appraisal and disposition. To this end, Contoso has been working to automate as many processes as possible and, at the same time, to make those processes subject to business rules and other requirements in as transparent a manner as possible.

Workflow

To close the project, Alice initiates a master workflow, which includes a number of recommended and required procedures and sub-workflows. Some of the steps that Alice and her team need to perform are manual, while others are automated.

The first wrap-up task that Alice and her team performs is the identification and harvesting of content for reuse and storage in Contoso's Knowledge Center. Based on recommendations from her team and her own appraisal, Alice identifies a number of documents that are suitable for storage in the Knowledge Center as best practice documents.

Content classification and storage for reuse

On the engagement site, Alice locates one of the documents that she and her team have identified as reusable content. She clicks on the document to invoke the drop-down menu, clicks on Send To, and then selects Other Location to begin the submission process. On the page that appears, she enters the location for the Knowledge Center and clicks OK.

To verify and complete her submission, she navigates to the Knowledge Center site and locates her document. She sees a visual indication that the document requires a check in, requires an approval, and is missing required metadata. She clicks on the document and selects Edit Properties from the drop-down menu. She completes the properties form by filling in the missing values. These include such items as the knowledge opportunity type, a numeric indication of the relative reuse value of each submission component based on a standard valuation guideline, Client, Project type, Task, authors, contributing Roles and comments to indicate what best practice opportunity is associated with the document.

Upon completion of the form, Alice checks in the document. This action invokes a workflow that routes an approval request for the document to the Knowledge Center approvers.

Once Alice and her team have harvested the engagement site for reusable content and completed submissions to the Knowledge Center, the next step is to roll team members off the project. Before this can happen, each team member must complete a self-assessment. Alice will then need to review and comment on each assessment.

Navigating to the engagement site, each team member launches an InfoPath form that shows a number of fields to provide a self-assessment, and a checklist to verify that all corporate policies regarding end-of-project activities have been followed correctly. For example, the form asks to verify if they have removed any project-related content from their local hard drives or from any unmanaged locations.

Exchange Server 2007 compliance features and SharePoint integration

The form also requires that team members verify that they have copied any project-related emails to the Exchange folders that were pushed out to them at the project-initiation phase. When emails are copied or moved to these folders, they are classified according to company policies and specific policy-driven actions occur as a result. For example, copies of emails that should be treated as records are sent to the records center repository.⁶⁷

When team members complete and submit the form, a workflow process notifies Alice that she needs to review the self-assessment.

Alice reviews the self-assessments of each team member, adds comments and submits the form. Upon submission of the form, assessment information is routed automatically to Human Resources, team members are notified of Alice's comments, and their permissions to access the engagement site are removed.

Persistent document security with RMS

This last step ensures that team members cannot consume any IRM-protected content that they may have deliberately or inadvertently stored in an unmanaged location after a specified interval defined by the IRM settings on the engagement site. This has the effect of putting confidential content on a "bungee cord" and pulling it back from team members by removing access even to their locally stored copies as per company policy.

Once the assessment and evaluation phase of the project end tasks are complete, Alice needs to ensure that all project documents are converted to records and stored in Contoso's Retained Records site. Alice can perform this task manually by using the Send To menu that she accesses from individual documents.

The Send To menu for objects on the engagement site has been extended to include an action to send documents to the Retained Records site. When this command is used, the document is declared as a record and is copied to the records center repository, along with its metadata, its audit history and its source location. The original document is left intact in its active location and can be used or deleted as necessary.

Automation of records declaration

Declaring documents as records manually by using the extended Send To command is useful, but is not a scalable solution for large numbers of documents. However, because the SharePoint object model allows for a high degree of customization and automation, the Contoso developers can automate the declaration of records. In this case, they developed end-of-project workflows that call the SendToOfficial method, which automatically declares documents as records without manual intervention on the part of users.⁶⁸

⁶⁷ This is only one example of the Exchange Server features that assist organizations in meeting their compliance requirements for message retention, controlled access, and data and process integrity. For more information on the compliance features of Exchange Server 2007, see the white paper, [Meeting the E-Mail Compliance Challenge With Microsoft Exchange Server](http://www.microsoft.com/exchange/evaluation/compliance.msp) at <http://www.microsoft.com/exchange/evaluation/compliance.msp>.

⁶⁸ For more information on programmatically declaring documents as records by using the SharePoint object model, see [Records Center Overview](http://msdn2.microsoft.com/en-us/library/aa979542.aspx) at <http://msdn2.microsoft.com/en-us/library/aa979542.aspx>.

Business rule enforcement for records

Alice initiates a sub-workflow to declare project documents as records.⁶⁹ When copied to the records center, the documents are routed within the records center according to their content type. Documents that lack a matching content type classification are deposited to the records center as unclassified records. When this occurs, a records center administrator is alerted to review the documents for further action. Furthermore, as part of this process and as a means to enforce business rules, Alice will be alerted to any documents that do not possess all the required metadata for their declaration as records. She then will be prompted to complete the missing data before attempting to resubmit them.

Having completed the records declaration for the engagement, Alice can close the project by initiating a final sub-workflow that submits her final status report to HR and her manager.

Technologies

- Exchange Server 2007
- Office SharePoint Server 2007
- Office SharePoint Designer 2007
- Office InfoPath 2007

Product Features

- Enterprise Content Management
- Records Center template
- Content Types metadata
- Exchange Server 2007 integration with SharePoint
- InfoPath Personalization
- Workflow

⁶⁹ IRM protection settings on document libraries need to be taken into consideration when copying documents to different libraries. For example, it might be necessary to remove IRM protection from a document library before sending its contents to a different library. This might be accomplished programmatically by manipulating the `IrmRMSEnabled` property on the document library or list. For information on the SharePoint object model as it relates to IRM, see [SPIrmSettings Class](http://msdn2.microsoft.com/en-us/library/microsoft.sharepoint.administration.spirmsettings.aspx) at <http://msdn2.microsoft.com/en-us/library/microsoft.sharepoint.administration.spirmsettings.aspx>.

Conclusion

Enabling organizations to achieve more efficient collaboration, better communication and increased user acceptance, while at the same time increasing security and more effectively meeting compliance requirements, is a primary goal in Microsoft's ongoing efforts to provide solutions to its customers.

Microsoft recognizes that organizations will find it challenging to identify technological and business process solutions that improve their ability to collaborate internal and externally while working to improve their security and meet compliance requirements. Many organizations will initially find these challenges to be daunting and overwhelming, in particular when attempting to map their business needs to technological solutions.

While the complexity and scope of these challenges should not be underestimated, they become more manageable through the adoption of frameworks and methodologies that incorporate industry-standard best practices. To provide guidance for meeting and overcoming these challenges, Microsoft has developed the Infrastructure Optimization Model (IOM). By adopting this framework model, organizations will find the journey to increased business efficiency and security to be manageable and realizable.

The IOM provides a distillation of best practices from sources such as industry standards, other framework models and field experience. The IOM provides a clear map and set of directions to assist organizations in making incremental changes over time that will eventually allow them to achieve full control over IT costs, increased automation, increased security and better communications. Ultimately, through the IOM, organizations can harness their IT infrastructure to enable business processes to the point where IT is a strategic asset, rather than a cost center.

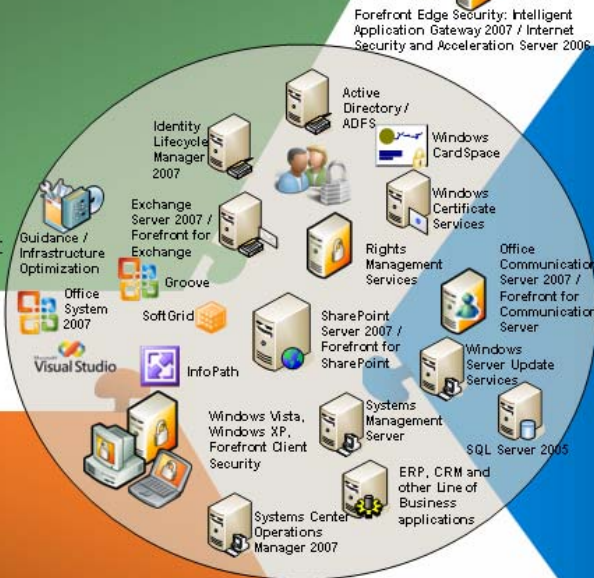
Organizations that are trying to implement solutions to solve complex and specific business challenges, such as meeting compliance requirements, managing content across the enterprise, providing secure and available access for remote users, or enabling better communication and collaboration, will benefit from both current and next-generation Microsoft products.

Out of the box, Microsoft products provide ready-made solutions for a large number of business requirements and usage scenarios. For example, Microsoft Office SharePoint Server 2007 provides enterprise search, document and records management, versioning control, workflow controls and auditing. Where custom solutions are required, the highly extensible architecture of Microsoft products allows organizations to develop and deploy solutions in a cost- and time-effective manner. The extensible architecture, in addition to the security, usability and other benefits of Microsoft products, allows organizations to achieve better business agility and profitability through enhanced communication, collaboration and security.



- Service Delivery Management**
- Client Acceptance
 - Proposal Management
 - Engagement Management
 - Team Workspace
 - Content Creation & Control
 - Enterprise Content Management

- Practice Performance Management**
- Time and Billing
 - HR Administration
 - Talent Management
 - Knowledge Management
 - Client Relationship Management
 - Practice Management



- Client Experience Management**
- Client Workspace
 - Data Exchange
 - Survey and Respond



Appendix A: What Are Professional Service Firms?

Professional service firms are knowledge-intensive organizations that provide their clients with broad or specialized knowledge, expertise, experience, judgment and solutions on a fee-for-service basis. The value that professional services firms bring to their clients resides in the knowledge, experience and consequent professional judgment that would be otherwise difficult or impractical to acquire in-house, especially the knowledge and judgment that can only be acquired through wide and deep range of experience, and which cannot be easily codified.

Professional service firms also can provide value in their independence from the client firm. For example, professional services firms can provide independent verification of financial statements or an independent audit of a public company's assessment of controls that relate to year-end financial statements, as required by section 404 of the Sarbanes Oxley Act (SOX).

In narrow terms, professional service firms provide their services to clients through employees who are members of legally accredited professional associations, such as architects, attorneys, engineers and accountants. These accredited employees are governed by codes of ethical practice that are external to and in addition to those of the professional services firm, and they must fulfill a variety of requirements specific to their profession to acquire and maintain their professional designation.

This narrow definition, however, does not entirely encompass the far-ranging scopes of practice of professional services firms. For example, professional services firms can provide management consulting, human resources staffing and information technology services. Professional service firm employees who provide expertise in these areas may or may not possess formal and legally-recognized professional accreditation, although they may refer to themselves as "professionals."

Although professional service firms provide a wide range of broad or specialized services, the services provided by such organizations, in general, tend to fall into one or more of the following:

- Accounting and audit
- Human resources and staffing
- Legal
- Management consulting
- Information Technology
- Engineering

Other knowledge-intensive organizations, such as software development organizations, also provide solutions to customers. However, in this case, these companies provide single solutions and products that are purchased and implemented by a variety of clients with little or no modification.

In contrast, a professional services firm will provide solutions that are tailored to meet the needs of individual clients. Consequently, what distinguishes a professional services firm is that it provides solutions that must be customized to unique client needs and requirements. And, a significant part of the value a professional services firm brings to its clients is the experience and professional judgment of its employees.

Depending on the services provided and the client, professional services firms may be governed by regulatory requirements or formal codes of ethical practice.

Intra-Organizational Challenges Faced by Professional Service Firms for Secure Collaboration

Managing knowledge and information within the professional services firm itself is a significant challenge. Although clients have unique requirements, the professional services firm will deal with clients who may have significant overlapping requirements. In these cases, professional service firms achieve efficiencies by capturing the knowledge and experience of similar past and current engagements, allowing them to leverage their intellectual capital and know-how.

Consider a professional services firm that specializes in providing IT security solutions. Some of its clients may have done little or no threat- and risk-analysis, and furthermore will have inadequate, underdeveloped or no security policies. The professional services firm will achieve efficiencies by developing standardized methodologies for threat- and risk-analysis and boilerplate document templates for corporate security policies that could be used at its various clients as starting points for collaborative solutions. Rather than inventing methodologies and documents for each client, the professional service firm can leverage past experience and knowledge.

Professional service firm employees must have access to the right tools and services so that they can create and find appropriate knowledge and documents easily within their own firms. Needless to say, professional services firms experience significant challenges in codifying, storing, organizing and indexing their own knowledge so that their intellectual capital and know-how can be leveraged to achieve efficiencies for each client engagement. This is an especially significant problem if employees are using email or their desktops to collaborate on and to store documents, rather than a central repository, such as Microsoft Office SharePoint Server (MOSS) 2007.

Content is expanding, causing employees to spend ever-increasing time searching for, sifting through and organizing information. As a result, productivity falls.

Employees like to use email, local desktop file storage and file shares to collaborate on and to store documents, rather than a centralized, indexed and auditable repository. For many organizations, email is the prevailing and de facto standard for document collaboration, especially when the teams are small and the immediate and apparent benefits of collaboration via email strongly favor bypassing onerous controls. Email is not practical, however, when the teams are large. Managing the volume of emails within a large team can impose a heavy clerical burden, especially when email is used as the primary tool for collaboration.

To make matters worse, professional service employees have access to an increasing number of communication channels that potentially can be used as a means to bypass policy. These channels include Web mail, instant messaging, peer-to-peer file-sharing applications, and recently emergent Web 2.0 applications, such as Wikis and RSS feeds (blogs, newscasts, etc).⁷⁰

⁷⁰ First coined by O'Reilly Media in 2004, the definition of "Web 2.0" remains ambiguous and open to criticism. In general, Web 2.0 refers to a set of Internet technologies and applications that promote collaboration, information sharing and social interaction. Examples of Web 2.0 applications include Skype and Wikipedia; protocols used include Simple Object Access Protocols (SOAP); data formats generally require the use of XML.

Instant messaging is making significant progress in replacing email as the vehicle of choice for text messaging and, to a lesser extent, for transferring files. Applications such as Skype make it possible to make voice calls and even, with software add-ons, do video conferencing.

Many of these applications are tunneled in Web protocols (HTTP and HTTPS), making it easy for them to be used across the corporate firewall. In the absence of effective outbound content filtering, the potential for information loss increases. Furthermore, in the context of the Safeguard rule of the Gramm-Leach-Bliley Act or similar legislation, which includes provisions for protecting non-public information, these unauthorized communications channels create additional concerns. For example, firms may be concerned that these unauthorized or uncontrolled channels present a compliance risk for the leakage of information.

The widespread use of email, unsanctioned communication channels and local hard disk storage for document collaboration magnifies the problems experienced by professional services in managing knowledge. Not only is it difficult to locate the appropriate documents, multiple versions of the same document can exist. This introduces additional risks, as copies of documents might not be subject to internal controls, policies and workflows. For example, there may be a lack of consistency among document versions, or documents might contain metadata that violate client privacy and confidentiality. Also, it is difficult, if not impossible, to determine who accessed a document and when that access occurred. This lack of auditability can have profound consequences, especially in the context of the numerous regulatory requirements for the professional services firm and its clients.

Complicating this situation is the fact that many organizations store information in a variety of file formats and use different applications and application versions to access and process that information.

Documents are edited and turned around at ever-increasing rates within teams of people. Keeping track of multiple versions of documents that contain edits for approval means that highly paid employees experience an ever-increasing clerical workload, reducing productivity and adding to employee dissatisfaction. In many cases, the revisions do not add significant value to the documents, magnifying the counterproductive effects of excessive revision cycles.

Even when technological controls are in place to provide centralized repositories for information, employees will bypass controls if they are too onerous, too awkward to use, or generally interfere with getting the job done. Employees will simply email the document to a corporate or private address or copy the document to the local hard drive so that they can work on it freely. Many employees will not let burdensome controls or policies get in the way of their ability to do the work. In fact, user acceptance of any solutions for collaboration and document management must be a key criterion for selection – users need solutions that are intuitive and do not require extensive training.

Local file storage has strong appeal for information workers. Quick and efficient, it works when disconnected from the network. Also, it offers significant productivity benefits for the individual user, when considered from the point of view of document search and document retrievals. Information workers do not need to engage in time-consuming and confusing searches through multiple collaborative workspaces to find previous documents to reuse. They simply search their hard drive. This benefit does not, however, extend to the company as a whole.

It is easy to understand how email is frequently the de facto standard for document collaboration within and between organizations. Easy to use and available, it supports attachments, integrates with calendars and contact lists, supports groups in the form of distribution lists, and feels natural to use.

And, given the increasing mobility of the professional services firm's workforce, email is usually available outside the firewall without needing to connect to the corporate network by means of a VPN.

The increasing mobility of professional service firm employees creates further challenges for document collaboration. These employees must be able to work on documents even when they are disconnected from the corporate network. And, from the point of view of the remote user, the client experience is not seamless. Once a document is updated locally, the user must connect to the network and then manually copy the document to its appropriate location. Furthermore, protecting documents outside the corporate firewall is a major challenge. In many instances, these documents must be secured on the remote user's device to mitigate risks associated with theft of the device or other forms of loss. This means that additional security measures, such as Encrypted File System (EFS), must be implemented.

Much of the value of a professional services firm is expressed in the form of intangible assets: the knowledge and experience it controls. Loss of intellectual capital and know-how, whether in the form of employees or codified information, is a serious concern. The loss of skilled and knowledgeable employees is compounded if these employees also can copy the codified knowledge of the firm and use it elsewhere. Unfortunately, if knowledge can be codified, it can be copied and disseminated easily.

Information loss and leakage represents a threat to a professional services firm's assets in a variety of ways. In cases where the information leakage violates client privacy and confidentiality, there is a significant risk to the reputation of the firm, resulting in significant loss of business. If the information leakage also violates regulatory requirements, such as those codified in the Health Insurance Portability and Accountability Act (HIPAA) or the Gramm-Leach-Bliley Act (GLBA), significant civil or criminal penalties can ensue.

Inter-Organizational Challenges Faced by Professional Service Firms for Secure Collaboration

When professional services firms perform work for their clients, they face additional challenges for document collaboration. These challenges arise from two primary causes: 1) ethical, regulatory and legal obligations; and 2) technological challenges that prevent effective communication and collaboration across organizational and company boundaries.

Ethical, Regulatory and Legal Obligations⁷¹

The complexity of the challenges for document collaboration across organizational and company boundaries are magnified by a number of ethical, regulatory and contractual requirements. Often, these requirements need to be enforced with technological controls. For example, it may be necessary to enforce "ethical walls" throughout enterprise systems, which require strong identity, access and auditing controls. In terms of communication and collaboration, individuals on either side of an ethical wall should not have the capacity to communicate with one another, nor should they have access to documents and other information that they are not authorized to view, according to these requirements.

In general, the ethical, regulatory and legal requirements have as their explicit or implicit goals the protection of the client and the general public from harm. These requirements can be summarized as follows:

⁷¹ Disclaimer: nothing in this white paper should be seen as constituting legal advice. This white paper provides only summary information about compliance. Please consult a lawyer or accredited auditor for specific questions regarding compliance.

- Need to avoid conflict of interest

Professional services firms might have multiple relationships with client organizations. If so, they must be kept separate from one another. For example, a professional service firm might provide services to two or more clients that are in direct competition to one another. The concern is that proprietary information for one client could be used to give an advantage to its competitor. Also, it is important to ensure that employees of the professional service firm do not use non-public information to gain a financial benefit (insider trading). Furthermore, in avoiding situations that can give rise to conflicts of interest, professional services firms must abide by expectations imposed by the concept of “fiduciary duty” (see below).

- Need to maintain client confidentiality

The need to maintain client confidentiality can be wide ranging. Firms that provide legal services to clients, for example, need to follow strict client-confidentiality guidelines, which do not permit even disclosure of the relationship with the client, except under certain circumstances.⁷² In other cases, confidentiality requirements extend only to proprietary data that the professional services firm obtains in order to do its work. When confidential information is provided to the firm on a “need-to-know” basis, the firm must ensure that only the appropriate personnel can view the data, and avoid situations that can give rise to conflicts of interest. When firms are assisting with Merger and Acquisition activity, confidentiality requirements can be extremely strict to avoid the possibility of harm to companies and the possibility of insider trading.

- Need to abide by contractual agreements for non-competition

Because many professional service firms have multiple and broad scopes of practice, conflicts can arise when a scope of practice overlaps with the client’s business. Typically, the potential for conflicts are mitigated by non-competition agreements that both parties sign. Professional service firms must abide by both the letter and spirit of the non-compete agreements to ensure that proprietary and confidential client information is not used to gain a competitive advantage over the client firm. Quite often, non-competition agreements impose an obligation to meet due diligence requirements.

- Need to take and demonstrate due diligence and due care, according to the higher standards of fiduciary duty.

To meet regulatory and other requirements, organizations must exercise an appropriate level of due diligence and due care in meeting their obligations. Failure to meet these obligations can result in civil or criminal penalties. In general terms, “due diligence” refers to the obligation to investigate and monitor with the goal of discovering and identifying risks; “due care” refers to the obligation to be accountable for mitigating identified risks. In legal terms, these two terms are essential elements of “Standard of Care.” Depending on the activities of the firm, it may be subject to a higher standard of care. For example, accounting professionals that perform work for public companies under SOX legislation are required to meet the higher standards of care imposed by the Public Company Accountability Oversight Board (PCAOB) than they would if

⁷² American Bar Association, Model Rules of Professional Conduct, Rule 1.5, Confidentiality of Information at http://www.abanet.org/cpr/mrpc/rule_5_4.html.

they were working for a private company. It should be noted that, in some cases, demonstrating compliance with an industry-wide and accepted “standard of care” is not a defense. The firm also must show that it took every reasonable precaution to avoid harm.

Fiduciary duty is the highest standard of care that a fiduciary must exercise toward its beneficiary. Loyalty to the beneficiary on the part of the fiduciary is implicit. In this context, professional services firms must be extremely diligent to ensure that they avoid situations where personal interests conflict with their fiduciary duty, where fiduciary duties conflict with other fiduciary duties, and where they profit from the fiduciary relationship without explicit knowledge and consent.

- Need for independence (in both fact and appearance)⁷³

The need to be and appear independent from the client firm has both an ethical and legislative impetus. For example, the Sarbanes-Oxley Act explicitly prohibits companies that perform independent audits for public companies from having other, specified relationships with their audit clients, such as providing management consulting services. And, even when certain relationships are allowed, such as tax planning for audit clients, many firms choose not to provide these services to avoid the appearance of being insufficiently independent.

Given the international scope of business and the growing complexity of regulatory environments, clients increasingly need guidance and advice that cross professional boundaries. For example, a firm may provide both legal and accounting services to a particular client. Obviously, professional services firms that can provide an integrated service have a competitive advantage in the marketplace. However, these integrated services can lead to perceptions that the professionals lack independence, and can cause potential harm to clients. For example, in the U.S., law firms and multi-disciplinary practices that provide legal services must ensure that they follow the American Bar Association (ABA) rules that forbid fee sharing.⁷⁴

Summary of Technological Challenges for Inter-Organizational Collaboration

The complex challenges that professional service firms face for document collaboration within their own organizations are magnified when they perform work for clients. The added complexity of the inter-organizational challenges results, in general, from three main causes: 1) the geographic disparity between the professional services firm and the client; 2) the technological disparity between the professional services firm and the client; and 3) the legal, ethical and regulatory obligations that the relationship with client imposes on the professional services firm.

The key technological challenges for inter-company collaboration are summarized below:

- **Enabling decentralized collaboration for mobile professional services employees**

Professional services firms need to find ways to enable decentralized collaboration without giving up required controls for the data.

⁷³ See, for example, Public Company Accountability Oversight Board, Bylaws and Rules, Auditing Standard 2 at http://www.pcaobus.org/Rules/Rules_of_the_Board/Auditing_Standard_2.pdf

⁷⁴ American Bar Association, Model Rules of Professional Conduct, Rule 5.4, Professional Independence of a Lawyer at http://www.abanet.org/cpr/mrpc/rule_5_4.html.

Professional services firm employees are, to a significant extent, mobile and often must perform work in the field away from the central office. Employees cannot always rely on being able to connect to the central office with their laptops or other devices, and must have the capacity to perform their work in a disconnected environment. Often, these mobile employees are part of a larger team both within their own firm and within the client firm. Moreover, the team environments are often fluid and employees frequently move between collaborative contexts.

Regulatory compliance requirements complicate the collaborative challenges for mobile workers. Information that is subject to regulatory requirements requires controls to ensure auditability and accountability for information usage to mitigate risks to information integrity and confidentiality. These controls must apply to information, even when the mobile worker copies it to a local device for legitimate purposes.

A further issue for mobile workers is that they often need to interact with clients on the client network and within different computing contexts. Devices need to assume a contextual identity and security profile that is based on the network they are connected to and their role.

- **Providing seamless collaboration across organizational boundaries**

Ensuring that intra- and inter-company collaboration on electronic data can occur seamlessly is a growing demand, as electronic data often needs to move between professional services firms and their clients.

- **Meeting requirements for secure information storage**

Professional services firms have a variety of contractual, regulatory and legal obligations to maintain sensitive client information securely. Often, the information must be available only on a “need-to-know” basis to appropriate individuals within the firm. Given that much information may be stored across a number of different storage contexts, such as local devices, file shares and workspaces, it is necessary to ensure that access to the information is available only to authorized individuals and that such access is auditable.

- **Meeting requirements for information retention**

Professional services firms have obligations regarding the collection, retention and destruction of information. Often, these obligations are policy-driven and met with administrative controls. For example, auditors will remove documents from their local devices to comply with written policies once an engagement has been completed. However, administrative controls in the form of written policies alone are often not sufficient. Given a stricter regulatory environment and the growing complexity of policies regarding records retention, it is important to enhance administrative controls governing records retention with technological ones. These controls need to be scalable to address different levels of compliance and scrutiny.

- **Meeting privacy requirements**

Professional services firms interact with clients across a wide range of jurisdictions with differing legislative requirements regarding the privacy of information. It’s important to ensure that personal information is shielded and made available only according to the requirements of the client service and in compliance with the appropriate jurisdiction.

Appendix B: Overview of Compliance and Government Regulations

Professional service firms face a two-fold challenge meeting regulatory, contractual and ethical requirements: 1) ensuring that they meet requirements as they apply to their own firms and 2) ensuring they meet requirements of their client, as appropriate for the work they are doing.⁷⁵

In response to recent and well-known scandals and more general concerns related to the potentials for fraud, corporate malfeasance, and theft or loss of personal information, many governments have enacted legislation and regulations to protect against the misuse and loss of electronic data and to improve the visibility, accuracy and timeliness of the reporting of corporate activities. A wide variety of legislation and regulations now in effect throughout the world place a significant burden on many organizations. While the overhead is often high to meet the new requirements, there are advantages to meeting them beyond simple cost avoidance in the form of criminal and civil penalties.

A primary reason that organizations should not view compliance as only overhead or as simply a cost center is that, by meeting regulatory compliance requirements, organizations can streamline their operations and improve their business processes. These requirements often are long-recognized best practices that have been expressed in a legislative framework. For example, the three pillars of information security, Confidentiality, Integrity and Availability of data (also known as the CIA triad), often inform the legislation's goals. These three pillars are discussed in more detail below.

Implementing the controls required to achieve regulatory compliance has advantages over and above the explicit goals of the regulations, for example, making it possible to work more efficiently in a wide range of jurisdictions. Furthermore, by meeting compliance requirements with automated processes and controls, and by providing security services, IT departments become well integrated and aligned with the various business units.

Consequences of Non-Compliance

The consequences of non-compliance vary widely, according to the legislation, precedent and jurisdiction. The immediate and obvious consequences can include:

- Criminal penalties in the form of fines or jail time
- Civil penalties in the form of lawsuits

⁷⁵ Although this and subsequent sections emphasize regulatory compliance, "compliance" also should be viewed here in a broad sense to include legal obligations, which can arise from a wide range of sources, including laws, rules, regulations, precedents, litigation and contracts. For example, professional service firms need to abide by service level agreements (SLAs) and other requirements that are determined by contracts with their clients. Further, "compliance" should be seen to include ethical obligations, in addition to the "legal" obligations noted earlier. The same general principles regarding identification of compliance requirements, and developing business processes and technological controls to meet those requirements and mitigate risk, apply regardless of whether the compliance requirements are ethical, contractual or regulatory.

Less obvious, but nonetheless important, consequences include:

- Limited access to markets
- Limited ability to do business in specific jurisdictions
- Loss of reputation
- Loss of customer or partner trust

Common Characteristics of Regulatory Compliance

Although regulatory compliance legislation varies widely in scope and intent, they share common characteristics, some of which are informed by key principles of information security.

- **Confidentiality**

Organizations need to ensure that confidential information is shared only with authorized individuals on a need-to-know basis, and that intentional or unintentional disclosure of confidential information does not occur. Confidentiality provides assurance of this. Inappropriate disclosure of confidential information can occur by email, data sharing, printed documents, word of mouth, observation and other means. To ensure confidentiality, information should be classified appropriately, with the necessary measures to mitigate risk of disclosure. Confidentiality also implies control or possession of data.

- **Integrity**

Organizations need to ensure that data is authentic, correct and complete. Data integrity provides assurance that the data can be trusted. Loss of integrity can occur intentionally, in the case of data tampering, or unintentionally, in the case of accidental errors entering data. Additionally, copying or emailing documents and other files can create risks to data integrity (and confidentiality). If an organization bypasses controls, it may not have the capacity to verify that the copied data has not been changed and still possesses its original integrity. Authenticity is implicit in the concept of data integrity; that is, the source and the originality of the data are verifiable.

- **Availability**

Organizations need to ensure that data, applications and systems are available to those who need them when they need them. Availability provides assurance that required data and systems are accessible and germane. For professional service firms that operate within regulations specified by legislation, such as Sarbanes-Oxley (SOX), “availability” has special implications – accurate financial information must be available in a timely manner, as required by regulators, financial officers, investigators, auditors and court subpoenas.

- **Non-repudiation**

Non-repudiation is sometimes seen as a fourth pillar of information security.⁷⁶ Non-repudiation refers to the assurance that the person who claims to have created, modified or transmitted data is, in fact, that person, and is unable to deny that she is responsible for the data's content or transmission. Non-repudiation is possible only when digital certificates are employed to sign data.

It is important to note that, because of the high degree of assurance required for non-repudiation, only digital certificates that require two-factor authentication (usually in the form of a smart card and a pass phrase or PIN) can be used to assert non-repudiation with the necessary degree of certainty. Additionally, the principle of non-repudiation assumes that the Certificate Authority (CA) that issues the digital certificates is itself a trusted entity. This, in turn, requires a properly designed and implemented Public Key Infrastructure (PKI).

- **Records Retention, Disposition and Destruction**

Organizations must increasingly meet a wide variety of complex requirements to maintain records for specified periods of times and make these records available upon request. The requirements for record retention arise from a number of sources, such as legislation, civil case law, and internal and external business requirements.

Privacy legislation often will mandate rules for the retention (and destruction) of personal data. For example, the Data Protection Act of the British Parliament specifies that personal information may be kept no longer than it is necessary, except for research or historical purpose.

Firms that provide tax services to clients must abide by rules specified by the IRS and other equivalent agencies in different jurisdictions to retain tax-related information for specified periods of time, often different periods of time depending on the category of tax-related information.

With the rise of instant messaging (IM), voice over IP (VOIP), and other new forms of digital communication, organizations also need to consider whether to log and retain records from these forms of communication to meet business or regulatory requirements.

In attempting to find a balance between what to retain and what to discard or destroy, organizations may find that they need to retain information for longer periods than are required by legislation or business practices. For example, information that is subject to subpoena and legal discovery in court cases will need to be retained for periods determined by the outcome of civil or criminal cases. Furthermore, this information must be stored in such a manner that threats of tampering with the information are mitigated, and that it is possible to determine when the access occurred and who accessed and modified the information.

⁷⁶ There is some debate about the adequacy of the CIA triad model to describe the aims of information security. This has led to a variety of suggested changes to the model. For example, the Parkerian Hexad, named after its originator Don Parker, adds the three elements of control or possession of information, authenticity and utility to the triad to supplement the elements of confidentiality, integrity and availability, respectively. For more information, see <http://infosecuritymag.techtarget.com/articles/1999/parker2.shtml>.

- **Auditing and Logging**

Organizations cannot rely strictly on technological controls or written policies and procedures to ensure appropriate access to data. Access to sensitive or confidential data or systems needs to leave an audit trail to show who or what created, viewed or modified the data and when that event occurred. Auditing and logging are essential to ensuring the confidentiality and integrity of data.

Logs that record access to systems, applications and data must be maintained securely and in such a way as to mitigate the risks of tampering or altering. Logs can create significant overhead in terms of resource usage, such as disk space. Indiscriminate auditing can create additional risks due to the high volume of auditing information, making it difficult to isolate important events from ordinary ones. Organizations should be selective regarding the events they will audit, log and analyze, and to automate these tasks whenever possible. Consequently, as with data confidentiality, a data classification system designed to label confidential or sensitive data is essential.

Comprehensive audit trails assist in the determination of the scope of disclosure of confidential data. In cases where the disclosure violates regulatory requirements, knowing what data is compromised, who had access to the data, and what occurred to the data can reduce fines and other penalties.

Logging cannot protect information against inadvertent or malicious modification that compromises data integrity. While these technological controls alone are not sufficient to prevent loss of integrity, detailed logging can help determine the scope of the impact to the integrity of the data so that the issue can be better understood and corrected.

Summary of Key Compliance Regulations

Depending on their scope of practice and activities, professional service firms can be subject to any number of regulations. For example, if a professional services firm is performing an audit that requires a valuation of human resources, it might need access to medical insurance and other records. In such instances, it could be subject to HIPAA and privacy legislation, depending on the jurisdiction. The following section describes in summary some key compliance regulations that may affect professional services firms and their clients.

- **Sarbanes-Oxley Act**

The Sarbanes-Oxley Act (SOX), also known as the Public Company Accounting Reform and Investor Protection Act of 2002, defines standards for accounting and financial practices of publicly traded firms. These standards are designed to ensure the accuracy and timeliness of financial reporting to protect the public and company shareholders from the harm caused by errors, omissions and malfeasance. The act contains a number of important provisions that have far-reaching effects:

- It establishes the Public Company Accounting Oversight Board (PCAOB), which has the mandate to establish and enforce the standards of care that outside accounting firms must follow in their roles as auditors of public companies. The PCAOB also has the authority to regulate non-audit activities, such as tax consulting, of audit firms for their clients. The PCAOB is subject to oversight powers of the Securities and Exchange Commission (SEC).

- It requires CEOs and CFOs to certify financial statements and makes them responsible for ensuring the accuracy and completeness of such statements. Penalties for non-compliance can result in heavy fines or jail time.
 - It explicitly prohibits or limits certain categories of work, such as financial system design, or legal or expert services unrelated to the audit, that audit firms might perform for their audit clients. It also makes other, unspecified categories of non-audit work subject to pre-approval by an audit committee.⁷⁷ These prohibitions are designed to assure auditor independence by ensuring that auditors do not function as management, do not serve as advocates and do not audit their own work.
 - It requires management to establish “internal controls over financial reporting” and provide an assessment report on these controls. Furthermore, outside auditors subject to standards of the PCAOB must attest to management’s assessment report.
 - As part of the responsibility for internal controls over financial reporting, management must “[p]rovide reasonable assurance regarding prevention or timely detection of unauthorized acquisition, use or disposition of the registrant’s assets that could have a material effect on the financial statements.”⁷⁸ Any information that could have a negative impact on the company if an unauthorized disclosure occurs – an extremely broad definition of “assets” – must be monitored and protected under this provision.
- **Gramm-Leach Bliley Act**

Although the primary purpose of the Gramm-Leach Bliley Act (GLBA) is to open up competition within the financial services industry, it also contains significant provisions for the protection of non-public information (NPI). Under the Safeguard rule of the act, financial institutions, whether they receive customer information directly or indirectly, must develop and implement a written security plan that contains information on the administrative, technical and physical controls for protecting NPI. Furthermore, the act stipulates the use of controls, such as encryption, access controls and so on, to protect NPI. However, like HIPAA, it does not specify particular technologies for implementing these controls. The legislation also mandates the monitoring of systems where NPI is stored. Failure to comply can result in heavy penalties.

- **Health Insurance Portability and Accountability Act**

A primary goal of the Health Insurance Portability and Accountability Act (HIPAA) is the protection of electronic health-related information of patients. Another goal is to improve the efficiency of the transfer of health-related information. The act applies to any entity, including insurance companies, which maintain health-related information of patients, regardless of whether they provide medical services. Like the GLBA, HIPAA, does not stipulate the use of particular technologies to achieve the goal of confidentiality of electronic patient information. Under the provisions to protect the confidentiality of patient health records, stiff penalties,

⁷⁷ See the SEC’s “Final Rule: Strengthening the Commission’s Requirements Regarding Auditor Independence” at <http://www.sec.gov/rules/final/33-8183.htm>.

⁷⁸ See the SECs “Final Rule: Management’s Reports on Internal Control Over Financial Reporting and Certification of Disclosure in Exchange Act Periodic Reports” at <http://www.sec.gov/rules/final/33-8238.htm>.

including jail time, can result from either the intentional or unintentional disclosure of patient health information.

- **Data Protection Act (European Union)**

The Data Protection Act of the British Parliament implements the European Union “Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data.” The act creates provisions for protecting the privacy of individuals and personal data, and places restrictions on organizations that collect this information. The act specifies that personal data can be used only for the purposes for which it is collected. The data collected must be appropriate, relevant, not excessive, accurate and up-to-date. The data also must be processed according to the individual's rights. Importantly, the act also specifies that data can be kept no longer than is necessary, except for research and historical purposes. Furthermore, the act also stipulates that the data must secure and not transferred to another country outside the EU, unless that country can provide assurances of a sufficient level of protection to the affected individual's rights and freedoms. This latter stipulation has caused the U.S. Chamber of Commerce to develop a legislative framework, known as Safe Harbor, to assist U.S. organizations to comply with the EU directive.⁷⁹

- **Personal Information Protection and Electronic Documents Act**

The Canadian Parliament created the Personal Information Protection and Electronic Documents Act (PIPEDA) in part as a response to EU privacy legislation. The act provides the legal basis for the collection, disposition and disclosure of personal information for commercial purposes. It enshrines the 10 privacy principles of the Canadian Standards Association Model Code, but contains a number of exceptions to those principles. The 10 privacy principles are similar to those embodied in the Data Protection Act (European Union). For example, the act stipulates that data can be used only for the purposes for which it is gathered, and that data must be stored securely and retained only for a necessary period.

The definition of “personal information” in PIPEDA is extremely broad. It includes information about an identifiable individual, but does not include the name, title, business address or telephone number of an employee of an organization.”⁸⁰ The legislation stipulates that individuals must give their consent any time personal information is transmitted to a third party, and that organizations must disclose the personal information it stores to the affected individuals upon request. This creates a heavy burden on organizations that must comply with the legislation. Further complicating matters is the fact that PIPEDA does not apply consistently across the country. When Canadian provinces have similar legislation, such as in British Columbia, Alberta, Manitoba and Quebec, the provincial legislation is in effect.

⁷⁹ See http://www.export.gov/safeharbor/sh_overview.asp

⁸⁰ Personal Information Protection and Electronic Documents Act at http://www.privcom.gc.ca/legislation/02_06_01_01_e.asp

Appendix C: General Overview of the Infrastructure Optimization Model: Basic, Standardized, Rationalized and Dynamic

Microsoft has formulated an Infrastructure Optimization Model (IOM), which can be leveraged to provide functional descriptions of professional services firms' common goals for securing information. This framework model can help customers optimize their IT infrastructure, reduce operational costs and complexity, and improve their IT management processes for manageability and security.

Microsoft's IOM forms a core part of its Dynamic Systems Initiative (DSI), which provides guidance to businesses that need to better align their business processes with IT. Related to the Information Technology Infrastructure Library (ITIL), the IOM is based on models proposed by the Gartner Group and MIT, and a distillation of Microsoft's experience in managing its own infrastructure and assisting its enterprise customers.

The IOM describes four levels of increasing infrastructure and business process maturity: basic, standardized, rational and dynamic.

In very general terms, the IOM defines the characteristics of each level – basic, standardized, rational, and dynamic – as a function of the degree of automation, security, usability and utility inherent within the IT infrastructure, and the degree to which that IT infrastructure aligns with and serves the needs of the business. Each higher level of maturity offers significant benefits, not the least of which is lower costs associated with the IT infrastructure. The four levels are summarized below:⁸¹

- **Basic**

The basic level is characterized by the predominance of manual, redundant and uncoordinated processes, with minimal centralized control and rudimentary asset management. Hardware and software inventories, including licenses, are minimal or non-existent, with little centralized control over purchasing. The value of assets that are less tangible, such as intellectual content, is either unknown or crudely estimated. Additionally, IT policies are either non-existence or have minimal enforcement with regard to security, regulatory compliance, backups, desktop and application standards, and other common IT and business standards.

IT is primarily a cost center that provides inadequate levels of support for the business units to meet their specific requirements, and organizations operating at this level find managing information and the IT infrastructure difficult and costly:

- Deployment of software, patches and services are high touch.
- Information storage is decentralized and ad hoc, resulting in difficulties in finding it.

⁸¹ Infrastructure optimization can be viewed from three perspectives: application platform, business productivity and core infrastructure. These perspectives each have their own optimization models and formal designations, such as Application Platform Infrastructure Optimization Model (APIOM) and Business Productivity Infrastructure Optimization Model (BPIOM). For the purposes of brevity and simplicity, this summary section merges these perspectives to some degree. For more information on these specific perspectives, please see <http://www.microsoft.com/business/peopleready/coreinfra/default.mspx>.

- There is little overall sense of the tactics that should be employed to improve business processes supported by IT because of a lack of control and knowledge of the hardware and software that comprises the infrastructure.
- There is a confusing mix of operating systems and applications.
- As they grapple with meeting their own needs, various business units install different applications with redundant functionality. For example, there might be different anti-virus solutions or productivity software on the desktop.
- Mailboxes are often choked with spam.
- There is a lack of “single sign on” for applications.
- The response to security threats and exploits is, for the most part, reactive and results in significant (and often sudden) downtime and loss of productivity.

From the point of view of collaboration and communication, organizations operating at this level experience significant productivity deficits and other difficulties:

- Information storage is decentralized and ad hoc, causing employees to engage in time-consuming and inefficient searches across multiple locations and devices.
- Information is created needlessly as a result of inefficient searches for information that could potentially be reused.
- Information is formatted on an ad hoc basis with no regard to common standards and templates for professional levels of presentation, causing additional editing and formatting for presentations at the end stage, if such editing occurs at all.
- Project management is a manual, ad hoc process.
- Reporting is a time-consuming and manual process.
- Due to a lack of common tools, collaboration is often an analog process that occurs through time-consuming and costly face-to-face and telephone meetings.
- Little or no information is shared across “islands of productivity.”
- Standardized Web portals for collaboration are lacking, and portal sites are created on a purely ad hoc basis.
- Instant messaging is not implemented to enable intra- or inter-organization communication to enhance collaboration.
- Shared calendars and scheduling capabilities are limited or non-existent.

The basic level creates a high degree of business and security risk due to ineffective policy enforcement, and a lack of centralized controls and processes. For example, documents have little or no version control, and the integrity of information is difficult to determine because of insufficient auditing. Also, there is a lack of standard workflows to support approval processes. For organizations that must operate within legal or ethical constraints, this could have profoundly negative consequences.

- **Standardized**

The standardized level represents a number of incremental improvements to the basic level. Organizations have begun to realize benefits of baseline standards and some policies.

This level is characterized by more centralized control, and increasing automation and coordination of processes. For example, organizations have a better sense of assets, both in the form of hardware and software inventories, including licenses, and less tangible assets, such as intellectual content. Purchasing of hardware and software is centralized, standardized, and subject to recommendations, based on evaluations.

Organizations that achieve this level aspire to achieve higher levels of optimization. They recognize the value of “best practices” and are attempting to adopt them. These best practices include formal risk assessments and analysis⁸² and the adoption of guidelines and prescriptions as described by this and other framework models, such as Microsoft Operations Framework (MOF)⁸³, ITIL, Control Objective for Information and related Technology (COBIT), ISO 17799 (now ISO 27001), and so on.

IT is, however, still largely reactive to security threats and exploits, and its “defense-in-depth” implementations are limited.

Overall, IT provides better support for business units in meeting their requirements than in the basic level. From the IT infrastructure’s point of view, organizations that achieve the standardized level exhibit the following attributes:

- Deployment of software, patches and services are medium touch with medium to high cost.
- Some automation of patch management for servers and desktops through Windows Software Update Services (WSUS) has been achieved.
- The perimeter is locked down with centralized policies at the firewall.
- A single antivirus solution is implemented at the desktop and server level.
- Periodic scans for malware are conducted at the desktop and server level.
- Laptops have personal firewall enabled, but desktops are still at risk.
- Active Directory is leveraged to provide better single sign on, but some applications still require different credentials.
- A unified solution to capture spam has been implemented.

⁸² The importance of risk analysis should not be underestimated. Controls should mitigate real – not imagined or perceived – risk. Without knowing the real risks, organizations might implement either excessive or insufficient controls to mitigate risk. A risk analysis can help organizations identify cost-effective methods to mitigate risk. For example, a change to a business process could be just as effective, if not more effective, in mitigating an identified risk as a more expensive technological control.

⁸³ Microsoft Operations Framework (MOF) builds on and extends the Information Technology Infrastructure Library (ITIL) to provide a set of prescriptive guidelines for IT service management and improving operations. For more information on MOF and its relationship to ITIL, see [MOF: An Actionable and Prescriptive Approach to ITIL](http://www.microsoft.com/technet/solutionaccelerators/cits/mo/mof/mofitil.msp) at <http://www.microsoft.com/technet/solutionaccelerators/cits/mo/mof/mofitil.msp>. MOF also integrates with COBIT, Six Sigma, and other frameworks and methodologies.

From the point of view of collaboration and communication, organizations at this level begin to realize various productivity and risk mitigation benefits that result from higher availability and lower vulnerability of data, even though information workers experience more restrictions at the desktop level. For example:

- Standards and templates have been developed for information storage, retrieval and presentation.
- Centralized and normalized file sharing allows for more efficient searches, information discovery and retrieval.
- Information and templates are distributed via file shares or email within collaboration teams.
- Web portals are still ad hoc and provincial with little central management, but are a preferred method for information storage, retrieval and distribution within collaborative teams.
- Data loss is mitigated through centralized backups of some, but not all, data.
- Standardized productivity applications, such as MS Office, allow for easier implementation of standards and automated processes.
- Employees use instant messaging internally for collaboration.
- Employees share calendars and scheduling tools internally.
- Limited project management tools are implemented.

While security and business risks are mitigated at the standardized level, they remain significant. Information confidentiality and integrity are vulnerable, lacking “defense-in-depth” strategies that extend from the firewall to the servers, desktops and laptops. Furthermore, while IT is more efficient, it is still a cost center because is not proactive and does not align closely with the business units’ requirements to reduce costs, improve productivity, improve collaboration and communication, and improve ethical and regulatory compliance. For example, reporting for regulatory compliance requirements remains largely a time-intensive and manual process. Also, employees have limited or no capability for streamlined inter-organization collaboration, and remote workers need better support.

- **Rationalized**

Organizations at this level experience significantly lower costs through improved standards, automation and proactive responses to threats and exploits, and a higher degree of centralized control. Policies, standards and processes have matured to the point where they assist productivity, collaboration, security and compliance requirements for the business units. IT is responsive to business unit needs and is closer to the goal of becoming a strategic asset.

Organizations at this level have a firm handle on asset management, including intellectual content, in addition to software, hardware and licenses. For example, they have adopted standards for categorizing data to meet business and regulatory requirements, and to better ensure confidentiality, integrity and availability. Furthermore, they have a wide range of technological controls and business processes to better enforce administrative controls of written policies or regulations. Additionally, best practices of security and business processes,

as described by framework models such as MOF, ITIL, COBIT, and so on, have been formally adopted and pervasively inform the infrastructure.

At the rationalized level, the benefits easily outweigh the incremental costs of implementing new technologies to support business processes driven by risk assessments and business requirements.

From the perspective of the IT infrastructure, organizations that achieve the rationalized level have the following attributes:

- Deployment of software, patches and services is low touch, low cost and highly automated. For example, the zero touch Systems Management Server deploys images.
- Desktop and laptop images are standardized and include “defense-in-depth” elements, such as anti-malware and personal firewall. For example, Microsoft Forefront Client provides centrally administered and controlled protection for desktops, laptops and servers against viruses and other malware.
- The messaging and collaboration infrastructure is protected from viruses and other malware. For example, Antigen for Exchange and Antigen for SharePoint are implemented.
- Strict security and policies are enforced pervasively throughout the infrastructure, from the perimeter firewalls to the servers, desktops, laptops and other devices.
- Secure remote access is supported for a variety of remote access scenarios.

As organizations achieve the rationalized level of maturity, communication and collaboration play a significant, active role in meeting business goals through increased agility, flexibility and usability. Although information workers experience less control over configurations related to security, they have more control over the tools, applications and information they need to be productive. In particular, the appropriate information is available to the right individuals when they need it. Communication and collaboration attributes of this level of maturity include:

- Centralized project management
- The ability to collaborate among disparate groups, both inside and outside the firewall
- Ability for inter-organizational collaboration, for example, via trusted relationships with partners
- Centrally managed and integrated Web portals that provide document version control, workflow approval processes and central storage of files
- Enhanced search capabilities, including searches across team sites and advanced searches for line of business (LOB) and people
- Policy-driven rights management and document protection solutions that protect intellectual property and content, for example, through the implementation of Microsoft’s Rights Management Services
- The ability to encrypt content to meet confidentiality requirements
- Pervasive and secure control of Instant Messaging for intra-organization communication

- Accessible email that is published securely over the Internet for a wide variety of devices, including PDAs and cell phones
- Email supports compliance and meets legal discovery needs
- Increased confidentiality, integrity and availability of information.
- Self-service reporting
- Standardization of data audits

When an organization reaches this level, it can focus on making incremental changes to its infrastructure that will provide the greatest benefits as determined by a formal analysis of risk and business requirements. For example, the organization could implement Active Directory Federated Services (ADFS) to enable better inter-organizational collaboration or Microsoft Identity and Integration Services (MIIS) to enable better single sign on. Both ADFS and MIIS yield benefits far in excess of the incremental costs of implementing these technologies, because they allow the current infrastructure to be more fully leveraged to achieve business benefits.

- **Dynamic**

Whereas at the rationalized level IT is a business enabler, at the dynamic level IT is a strategic asset. And, while organizations will face many challenges in centralizing and upgrading technologies to achieve this level, they will be also at the same time be able to establish a better balance between requirements, investments, and returns.

The dynamic level is characterized by high degrees of automation; increased service levels; fully controlled costs; deep integration of fully automated business processes, often within the technology itself; integration between users and data, desktops, and servers; pervasive collaboration within the organization; the capability for inter-organizational collaboration; and nearly on-site levels of service for mobile users.

From the perspective of the IT infrastructure, organizations that achieve this level have the following attributes:

- Automated, central management of patches, servers, desktops, image deployment, server and desktop firewall settings, system changes and updates, and application testing
- Extremely pro-active security to enforce policies at all levels, for example policies that prescribe role-based security
- Full volume encryption for laptops
- Deep integration of Active Directory to enable single sign on
- Automated identity lifecycle management, including automatic provisioning and de-provisioning of users across multiple systems and directories
- Isolation and protection of systems to protect sensitive information and meet compliance requirements
- Secure access to internal systems and applications to external partners and clients, for example, by enabling Active Directory Federated Services

- Personalized access to Internet, extranet and intranet sites
- High levels of self-service provisioning, including password resets across multiple directories and systems, recovery of archived data, software, collaboration tools and licenses
- Automated, centralized and secure audit log aggregation from disparate and distributed sources, with the ability to trigger alerts and raise events based on custom conditions
- Policy and role-based access to systems, applications and information

From the perspective of communication and collaboration, employees can focus on business needs, as the integration of technology at the dynamic level dissolves barriers to collaboration and compliance. Intra- and inter-organizational communication and collaboration occurs more transparently and with greater security. Organizations that achieve this level have the following attributes for communication and collaboration:

- Secure document management, distribution and access across firewalls and organizations.
- Seamless collaboration with external partners and customers
- Centrally managed Web portals
- Document workspaces for collaboration across companies
- Web-based meetings
- Instant messaging across companies and public networks
- Automatic updates for messaging, calendars and contact synchronization
- Enhanced support for mobile workers, including the ability to collaborate on information while disconnected from the network
- Enhanced security for smart phones and PDAs, including the ability to lock out access to devices after unsuccessful logon attempts and to perform remote data wipes on lost or stolen devices
- Rights management solution for data on mobile devices

By achieving the dynamic level, organizations increase the confidentiality of information, while simultaneously increasing its availability and integrity. Sensitive information is available on a “need-to-know” basis only. The processes and evidence required for compliance are a natural byproduct of the infrastructure and business roles and responsibilities, freeing organizations to focus more of their efforts on providing business intelligence and analytics, improving relationships with clients and partners, and finding new business opportunities.

Appendix D: Resources and References

This section provides information on the references that were helpful in creating this white paper, as well as additional resources that will help you develop a deeper understanding of the topics.

Infrastructure Optimization Model

- For an overview of the [Dynamic Systems Initiative](http://www.microsoft.com/business/dsi/default.aspx), which includes the IOM, see <http://www.microsoft.com/business/dsi/default.aspx>.
- For information and other resources about the IOM, see the [Microsoft Infrastructure Optimization](http://www.microsoft.com/technet/infrastructure/default.aspx) Web site at <http://www.microsoft.com/technet/infrastructure/default.aspx>.
- For information on the three infrastructure optimization model perspectives, see the following Web sites:
 - [Core Infrastructure Optimization Model](http://www.microsoft.com/business/peopleready/coreinfra/default.aspx) at <http://www.microsoft.com/business/peopleready/coreinfra/default.aspx>
 - [Application Platform Infrastructure Optimization Model](http://www.microsoft.com/business/peopleready/applat/default.aspx) at <http://www.microsoft.com/business/peopleready/applat/default.aspx>
 - [Business Productivity Infrastructure Optimization Model](http://www.microsoft.com/business/peopleready/bizinfra/default.aspx) at <http://www.microsoft.com/business/peopleready/bizinfra/default.aspx>
- For information on the implementation of IOM at Microsoft, see the Microsoft IT Showcase document, [Infrastructure Optimization at Microsoft](http://www.microsoft.com/technet/itshowcase/content/iotsb.aspx) at <http://www.microsoft.com/technet/itshowcase/content/iotsb.aspx>.
- For information on reducing infrastructure costs for desktops by following optimization best practices, see the white paper, [Infrastructure Optimization: Driving Down the Costs of the Business Desktop](http://www.microsoft.com/technet/infrastructure/bestpractices.aspx) at <http://www.microsoft.com/technet/infrastructure/bestpractices.aspx>.
- For analysis of the relationships between labor costs and optimization best practices, see the following IDC white papers:
 - [Optimizing Infrastructure: The Relationship Between IT Labor Costs and Best Practices for Identity and Access Management with Active Directory](http://download.microsoft.com/download/9/f/3/9f337be9-cc5a-46d6-bcbd-27e77acdb0ed/IDC_ADIO_whitepaper.pdf) at http://download.microsoft.com/download/9/f/3/9f337be9-cc5a-46d6-bcbd-27e77acdb0ed/IDC_ADIO_whitepaper.pdf
 - [Optimizing Infrastructure: The Relationship Between IT Labor Costs and Best Practices for Systems Management Server](http://download.microsoft.com/download/8/0/8/808c50a0-87ef-4e48-ba3f-6c4cc00dd7da/IDC_sms_whitepaper.pdf) at http://download.microsoft.com/download/8/0/8/808c50a0-87ef-4e48-ba3f-6c4cc00dd7da/IDC_sms_whitepaper.pdf
 - [Optimizing Infrastructure: The Relationship Between IT Labor Cost and Best Practices for Managing the Windows Desktop](http://download.microsoft.com/download/a/4/4/a4474b0c-57d8-41a2-afe6-32037fa93ea6/IDC_windesktop_IO_whitepaper.pdf) at http://download.microsoft.com/download/a/4/4/a4474b0c-57d8-41a2-afe6-32037fa93ea6/IDC_windesktop_IO_whitepaper.pdf
- For information on the relationship between Microsoft Operations Framework (MOF) and the Information Technology Infrastructure Library (ITIL), see [MOF: An Actionable and Prescriptive](#)

[Approach to ITIL](#) at

<http://www.microsoft.com/technet/solutionaccelerators/cits/mo/mof/mofitil.mspx>.

Regulatory Compliance with Microsoft Products

Microsoft has a variety of resources that are relevant to managing the infrastructure for regulatory compliance. The following is a list of some useful compliance resources available on the Microsoft Web site:

- [Regulatory Compliance Planning Guide](#) at <http://www.microsoft.com/technet/security/guidance/complianceandpolicies/compliance/rcguide/default.mspx?mfr=true>. This guide provides comprehensive guidance on planning for compliance, and a resource list.
- For information on managing compliance for SOX and other regulations, see [Managing Regulatory Compliance with Microsoft Technology](#) at <http://www.microsoft.com/business/compliance.aspx>.
- For a comprehensive discussion and illustration of the compliance features of the Microsoft Office System 2007, see the excellent white paper, [Compliance Features in the 2007 Microsoft Office System](#) at <http://www.microsoft.com/downloads/details.aspx?FamilyID=D64DFB49-AA29-4A4B-8F5A-32C922E850CA&displaylang=en>.
- For a high level overview of compliance requirements from a developer's perspective, see the [Regulatory Compliance Demystified: An Introduction to Compliance for Developers](#) at <http://msdn2.microsoft.com/en-us/library/aa480484.aspx>.
- [Architecting Regulatory-Compliant Architectures](#) at <http://msdn2.microsoft.com/en-us/library/bb233047.aspx>. Although this resource is aimed at architects interested in building applications for the banking industry, much of the content is relevant to any organization that works in a regulated sphere.
- For information on regulatory compliance by using Excel 2007 and SharePoint Server 2007, see the white paper [Spreadsheet Compliance in the 2007 Microsoft Office System](#) at <http://office.microsoft.com/en-us/excel/HA102132911033.aspx?pid=CL100570551033>.
- For a discussion of the relationship between Enterprise Content Management and compliance, see the white paper, [Enterprise Content Management: Breaking the Barriers to Broad User Adoption](#) at <http://office.microsoft.com/en-us/sharepointserver/HA102063591033.aspx?pid=CL100626951033>.
 - A variation of this white paper, [Enterprise Content Management in Regulated Industries](#), which discusses Enterprise Content Management from the perspective of regulation in the life sciences industry, is relevant because it discusses compliance features for many regulatory environments, not just for life sciences. See this white paper at <http://www.microsoft.com/industry/healthcare/lifesciences/businessvalue/whitepaperecm.mspx>.
- [Meeting the E-Mail Compliance Challenge With Microsoft Exchange Server 2007](#) at <http://www.microsoft.com/exchange/evaluation/compliance.mspx>.

- For short demonstrations of the compliance (and other) features of Exchange Server 2007, see [Exchange Server 2007 Feature Demos](#) at <http://www.microsoft.com/exchange/evaluation/demos/default.mspx>.

Regulatory Compliance and IT Control Frameworks

The following is list of non-Microsoft Web sites that provide information on a number of relevant regulations and IT controls:

- [Sarbanes-Oxley Act](#)
<http://www.legalarchiver.org/soa.htm>
- [SEC Rules on Auditor Independence](#)
<http://thecaq.aicpa.org/Resources/Ethics+and+Independence/SEC+Rules+on+Independence/SEC+Rules+on+Auditor+Independence.htm>
- SEC [Final Rule: Management's Reports on Internal Control Over Financial Reporting and Certification of Disclosure in Exchange Act Periodic Reports](#)
<http://www.sec.gov/rules/final/33-8238.htm>
- [European Union Data Protection Directive](#)
http://www.cdt.org/privacy/eudirective/EU_Directive_.html
- [Data Protection Act 1998](#)
<http://www.opsi.gov.uk/ACTS/acts1998/19980029.htm>
- [Safe Harbor](#)
<http://www.export.gov/safeharbor/index.html>
- [Personal Information Protection and Electronic Documents Act](#) (PIPEDA)
http://www.privcom.gc.ca/legislation/02_06_01_01_e.asp
- [SB 1386](#) (California's privacy legislation)
http://info.sen.ca.gov/pub/01-02/bill/sen/sb_1351-1400/sb_1386_bill_20020926_chaptered.html
- Department of Defense (DoD) [Design Criteria for Electronic Records Management Software Applications Directive 5015.2](#)
<http://www.dtic.mil/whs/directives/corres/pdf2/p50152s.pdf>
- [Rule 26 and Other Amendments to the Federal Rules of Civil Procedure: New Challenges for Litigation Readiness](#)
<http://www.ironmountain.com/knowledge/ediscovery/rule26whitepaper.pdf>
- [American Institute of Certified Public Accountants](#)
<http://www.aicpa.org/>
- [Association of Records Managers and Administrators](#)
<http://www.arma.org/index.cfm>
- [Control Objectives for Information and Related Technologies](#) (COBIT)
<http://www.isaca.org/cobit/>

- [Committee of Sponsoring Organizations \(COSO\) Internal Control Framework and Guidance](http://fmcenter.aicpa.org/Resources/Sarbanes-Oxley+Act/Committee+of+Sponsoring+Organizations+%28COSO%29+Internal+Control+Framework+and+Guidance.htm)
<http://fmcenter.aicpa.org/Resources/Sarbanes-Oxley+Act/Committee+of+Sponsoring+Organizations+%28COSO%29+Internal+Control+Framework+and+Guidance.htm>
- [Information Technology Infrastructure Library \(ITIL\)](http://www.itil.co.uk/)
<http://www.itil.co.uk/>

Product Resources and White Papers

- [Microsoft IT: Showcase](http://www.microsoft.com/technet/itshowcase/default.msp)
<http://www.microsoft.com/technet/itshowcase/default.msp>
- [Solution Showcase for the Microsoft Office System](http://www.microsoft.com/office/showcase/default.msp)
<http://www.microsoft.com/office/showcase/default.msp>
- [Microsoft Operations Framework \(MOF\)](http://www.microsoft.com/mof)
<http://www.microsoft.com/mof>
- [Intelligent Application Gateway 2007](http://www.microsoft.com/forefront/edgesecurity/iag/default.msp)
<http://www.microsoft.com/forefront/edgesecurity/iag/default.msp>
- [Microsoft Internet Security and Acceleration Server 2006](http://www.microsoft.com/isaserver/default.msp)
<http://www.microsoft.com/isaserver/default.msp>
- [Excel Services Technical Overview](http://msdn2.microsoft.com/en-us/library/aa972194.aspx)
<http://msdn2.microsoft.com/en-us/library/aa972194.aspx>
- [Microsoft Exchange Server](http://www.microsoft.com/exchange/default.msp)
<http://www.microsoft.com/exchange/default.msp>
- [Microsoft Office Communicator 2005](http://office.microsoft.com/en-us/help/HA011992481033.aspx)
<http://office.microsoft.com/en-us/help/HA011992481033.aspx>
- [Microsoft Office Groove](http://office.microsoft.com/en-us/groove/default.aspx)
<http://office.microsoft.com/en-us/groove/default.aspx>
- [Microsoft Office Groove Security FAQ](http://www.groove.net/index.cfm?pagename=Security_FAQs)
http://www.groove.net/index.cfm?pagename=Security_FAQs
- [Microsoft Office Live Meeting Guide](http://office.microsoft.com/en-us/livemeeting/HA102020561033.aspx?pid=CL101731541033)
<http://office.microsoft.com/en-us/livemeeting/HA102020561033.aspx?pid=CL101731541033>
- [Windows Rights Management Services](http://www.microsoft.com/windowsserver2003/technologies/rightsmgmt/default.msp)
<http://www.microsoft.com/windowsserver2003/technologies/rightsmgmt/default.msp>
- [Technical Overview of Rights Management Services](http://www.microsoft.com/windowsserver2003/techinfo/overview/rmenterprisewp.msp)
<http://www.microsoft.com/windowsserver2003/techinfo/overview/rmenterprisewp.msp>
- [Enabling Information Protection in Microsoft Office 2003 with Rights Management Services and Information Rights Management](http://www.microsoft.com/technet/prodtechnol/office/office2003/maintain/rmsirm.msp)
<http://www.microsoft.com/technet/prodtechnol/office/office2003/maintain/rmsirm.msp>
- [Microsoft SharePoint Products and Technologies](http://www.microsoft.com/sharepoint/default.msp)
<http://www.microsoft.com/sharepoint/default.msp>

- [Search in Microsoft Office SharePoint Server 2007 Evaluation Guide](#)
<http://technet2.microsoft.com/Office/en-us/library/8795cba0-7a8f-4f0b-87e3-b27d5a508a9b1033.msp?mfr=true>
- [Enterprise Content Management: Breaking the Barriers to Broad User Adoption](#)
<http://office.microsoft.com/en-us/sharepointserver/HA102063591033.aspx?pid=CL100796281033>
- [Microsoft Communication and Collaboration: Working Together in a New World of Work](#)
<http://www.microsoft.com/downloads/details.aspx?FamilyId=F38AD00F-ED59-4411-BD9B-1E438DD5CC6B&displaylang=en>
- [Microsoft SoftGrid Application Virtualization](#)
<http://www.softricity.com/>
- [Application Virtualization: The Next Frontier](#)
<http://download.microsoft.com/download/e/4/4/e4442c9f-30d9-41f3-9876-82bbfc5aa4e6/datasheet-sgav.pdf>
- [Introducing Windows CardSpace](#)
<http://msdn2.microsoft.com/en-us/library/aa480189.aspx>.
- [Windows CardSpace \(formerly "InfoCard"\)](#)
<http://msdn2.microsoft.com/en-us/winfx/aa663320.aspx>
- [Windows Vista home page](#)
<http://www.microsoft.com/windows/products/windowsvista/default.msp>
- [Windows Vista Tech Center](#)
<http://technet2.microsoft.com/WindowsVista/en/library/356e60d0-225e-4f72-857a-17b1dc57a1741033.msp?mfr=true>
- [Windows Mobile White papers](#)
<https://partner.microsoft.com/US/40023719>
- [Mobile Messaging and Business Application Solutions with Windows Mobile: Addressing Key Questions](#) (white paper)
<http://www.microsoft.com/windowsmobile/business/strategy/mobilemessaging.msp>

Developer and Architect Resources

- [MSDN Solution Architecture Center](#)
<http://msdn2.microsoft.com/en-us/architecture/default.aspx>
- [Visual Studio 2005 Developer Center](#)
<http://msdn2.microsoft.com/en-us/vstudio/default.aspx>
- [Office Developer Center](#)
<http://msdn2.microsoft.com/en-us/office/default.aspx>
- [What's New for Developers in the 2007 Microsoft Office System](#)
<http://msdn2.microsoft.com/en-us/office/aa905358.aspx>

- [SharePoint Server 2007 Technical Articles](http://msdn2.microsoft.com/en-us/library/bb258891.aspx)
http://msdn2.microsoft.com/en-us/library/bb258891.aspx
- [SharePoint Server 2007 SDK: Software Development Kit and Enterprise Content Management Starter Kit](http://www.microsoft.com/downloads/details.aspx?familyid=6D94E307-67D9-41AC-B2D6-0074D6286FA9&displaylang=en)
http://www.microsoft.com/downloads/details.aspx?familyid=6D94E307-67D9-41AC-B2D6-0074D6286FA9&displaylang=en
- [SharePoint Server 2007 Presentations: Enterprise Search Deep Dives](http://www.microsoft.com/downloads/details.aspx?FamilyID=2751D5CD-8690-44B5-AE5C-D2769B227929&displaylang=en)
http://www.microsoft.com/downloads/details.aspx?FamilyID=2751D5CD-8690-44B5-AE5C-D2769B227929&displaylang=en
- [Understanding Workflow in Windows SharePoint Services and the 2007 Microsoft Office System](http://www.microsoft.com/downloads/details.aspx?FamilyId=DBBD82C7-9BDE-4974-8443-67B8F30126A8&displaylang=en)
http://www.microsoft.com/downloads/details.aspx?FamilyId=DBBD82C7-9BDE-4974-8443-67B8F30126A8&displaylang=en
- [2007 Office System Document: Developer Posters](http://www.microsoft.com/downloads/details.aspx?familyid=771AEB45-9D27-4D1F-ACD1-9B950637D64E&displaylang=en)
http://www.microsoft.com/downloads/details.aspx?familyid=771AEB45-9D27-4D1F-ACD1-9B950637D64E&displaylang=en
- [Application Templates for Windows SharePoint Services 3.0](http://www.microsoft.com/technet/windowsserver/sharepoint/wssapps/templates/default.msp)
http://www.microsoft.com/technet/windowsserver/sharepoint/wssapps/templates/default.msp
- [SharePoint Products and Technologies 2003 Software Development Kit \(SDK\)](http://www.microsoft.com/downloads/details.aspx?familyid=AA3E7FE5-DAEE-4D10-980F-789B827967B0&displaylang=en)
http://www.microsoft.com/downloads/details.aspx?familyid=AA3E7FE5-DAEE-4D10-980F-789B827967B0&displaylang=en
- [MSDN .NET Framework Developer Center](http://msdn2.microsoft.com/en-us/netframework/default.aspx)
http://msdn2.microsoft.com/en-us/netframework/default.aspx
- [Developer Introduction to Workflows for Windows SharePoint Services 3.0](http://msdn2.microsoft.com/en-us/library/ms406057.aspx)
http://msdn2.microsoft.com/en-us/library/ms406057.aspx
- [Windows Workflow Foundation \(WWF\)](http://msdn2.microsoft.com/en-us/netframework/aa663328.aspx)
http://msdn2.microsoft.com/en-us/netframework/aa663328.aspx
- [Windows Communication Foundation \(WCF\)](http://msdn2.microsoft.com/en-us/library/ms735119.aspx)
http://msdn2.microsoft.com/en-us/library/ms735119.aspx
- [Using CardSpace in Windows Communication Foundation](http://msdn2.microsoft.com/en-us/library/ms733090.aspx)
http://msdn2.microsoft.com/en-us/library/ms733090.aspx
- [Software as a Service \(SaaS\)](http://msdn2.microsoft.com/en-us/architecture/aa699384.aspx)
http://msdn2.microsoft.com/en-us/architecture/aa699384.aspx
- [Software as a Service \(SaaS\): An Enterprise Perspective](http://msdn2.microsoft.com/en-us/architecture/aa905332.aspx)
http://msdn2.microsoft.com/en-us/architecture/aa905332.aspx
- [Security Developer Center](http://msdn2.microsoft.com/en-us/security/default.aspx)
http://msdn2.microsoft.com/en-us/security/default.aspx
- [Writing Secure Code](http://msdn2.microsoft.com/en-us/security/aa570401.aspx)
http://msdn2.microsoft.com/en-us/security/aa570401.aspx

- [MSDN Windows Vista Developer Center – Security](http://msdn2.microsoft.com/en-us/windowsvista/aa905011.aspx)
http://msdn2.microsoft.com/en-us/windowsvista/aa905011.aspx
- [Security Guidelines: .NET Frameworks 2.0](http://msdn2.microsoft.com/en-us/library/aa480477.aspx)
http://msdn2.microsoft.com/en-us/library/aa480477.aspx
- [Security Guidelines: ASP .NET 2.0](http://msdn2.microsoft.com/en-us/library/ms998258.aspx)
http://msdn2.microsoft.com/en-us/library/ms998258.aspx

Security Resources

- [Microsoft Security Guidance and Solution Accelerators](http://www.microsoft.com/technet/security/guidance/default.aspx) portal
http://www.microsoft.com/technet/security/guidance/default.aspx
- [Microsoft Security Awareness](http://www.microsoft.com/technet/security/understanding/awareness.mspx)
http://www.microsoft.com/technet/security/understanding/awareness.mspx
- [Microsoft Security Risk Management Guide](http://www.microsoft.com/technet/security/guidance/complianceandpolicies/secrisk/default.mspx)
http://www.microsoft.com/technet/security/guidance/complianceandpolicies/secrisk/default.mspx
- [Microsoft Threat Analysis and Modeling v2.1.2 tool](http://www.microsoft.com/downloads/details.aspx?familyid=59888078-9daf-4e96-b7d1-944703479451&displaylang=en) (download)
http://www.microsoft.com/downloads/details.aspx?familyid=59888078-9daf-4e96-b7d1-944703479451&displaylang=en
- [Windows Server 2003 Security Guide](http://www.microsoft.com/technet/security/prodtech/windowsserver2003/w2003hg/sgch00.mspx)
http://www.microsoft.com/technet/security/prodtech/windowsserver2003/w2003hg/sgch00.mspx
- [Windows Vista Security Guide](http://www.microsoft.com/technet/windowsvista/security/guide.mspx)
http://www.microsoft.com/technet/windowsvista/security/guide.mspx
- [Windows XP Security Guide](http://www.microsoft.com/technet/security/prodtech/windowsxp/secwinxp/default.mspx)
http://www.microsoft.com/technet/security/prodtech/windowsxp/secwinxp/default.mspx
- [Security Monitoring and Attack Detection Planning Guide](http://www.microsoft.com/technet/security/guidance/auditingandmonitoring/securitymonitoring/default.mspx)
http://www.microsoft.com/technet/security/guidance/auditingandmonitoring/securitymonitoring/default.mspx
- [Server and Domain Isolation Using IPSec and Group Policy](http://www.microsoft.com/technet/security/guidance/architectureanddesign/ipsec/default.mspx)
http://www.microsoft.com/technet/security/guidance/architectureanddesign/ipsec/default.mspx
- [Data Encryption Toolkit for Mobile PCs](http://www.microsoft.com/technet/security/guidance/clientsecurity/dataencryption/default.mspx)
http://www.microsoft.com/technet/security/guidance/clientsecurity/dataencryption/default.mspx
- [Forefront Security for Exchange Tech Center](http://www.microsoft.com/technet/forefront/serversecurity/exchange/default.mspx)
http://www.microsoft.com/technet/forefront/serversecurity/exchange/default.mspx
- [Forefront Security for SharePoint Tech Center](http://www.microsoft.com/technet/forefront/serversecurity/sharepoint/default.mspx)
http://www.microsoft.com/technet/forefront/serversecurity/sharepoint/default.mspx
- [Forefront Client Security Tech Center](http://www.microsoft.com/technet/clientsecurity/default.mspx)
http://www.microsoft.com/technet/clientsecurity/default.mspx
- [Introduction to Network Access Protection](http://www.microsoft.com/technet/network/nap/napoverview.mspx)
http://www.microsoft.com/technet/network/nap/napoverview.mspx

- [How to use Group Policy to configure detailed security auditing settings for Windows Vista client computers in a Windows Server 2003 domain or in a Windows 2000 domain](http://support.microsoft.com/kb/921469)
<http://support.microsoft.com/kb/921469>