

Microsoft<sup>®</sup>  
**Exchange Server 2007**

**Meeting the E-Mail Compliance Challenge  
With Microsoft Exchange Server 2007**

White Paper

Published: October 2006

For the latest information, please see <http://www.microsoft.com/exchange>

---

**Abstract**

Microsoft Exchange Server 2007 helps organizations meet compliance requirements for e-mail and messaging, including: data retention and discovery, controlled access to data, and policy and procedure enforcement. This white paper discusses the compliance issues organizations face, especially those in the financial services and healthcare industries, and how Microsoft Exchange Server 2007 enables companies to quickly implement comprehensive compliance capabilities to address these requirements.

## Contents

Introduction.....	1
Organizations at Risk .....	3
Compliance Requirements for E-Mail and Messaging.....	5
Message Retention .....	6
Controlled Access.....	6
Information and Process Integrity .....	7
Fulfilling Compliance Requirements – Microsoft Exchange Server 2007 and Exchange Hosted Services .....	8
New Compliance Features Within Exchange Server 2007 .....	8
Industry Compliance Scenarios for Exchange Server 2007 .....	11
Corporate Policy Controls .....	12
Microsoft Exchange Hosted Archive – Off-site Message Archiving for Compliance.....	13
Selecting the Right Compliance Solution .....	16
Summary .....	18

## Introduction

Compliance with regulations continues to be top of mind for executives across all industries, but especially those in the heavily-regulated financial services and healthcare sectors. With the proliferation and continued modification of federal, state, local, and international legislation, ensuring compliance throughout the organization with mandates such as Sarbanes-Oxley, SEC Rule 17A, Gramm-Leach-Bliley, and the Health Insurance Portability and Accountability Act (HIPAA) has created an unparalleled burden upon enterprises.

In a recent research report, “The Costs of Compliance in the U.S. Securities Industry,” the Securities Industry Association (SIA) estimates that the annual total cost of compliance will exceed \$25 billion for 2005, up from \$13 billion in 2002 – for the securities industry alone.\* In the healthcare industry, the American Hospital Association estimates that hospitals will spend \$22 billion over five years complying with the 2003 HIPAA privacy rule.† Compared to compliance costs, the penalties of non-compliance can be far greater. From fines to prison terms to de-listing from stock exchanges, non-compliance comes with a steep price tag.

Unfortunately, there’s one area of the business that many companies have not yet brought into compliance: electronic communications. With the bulk of business communications today happening electronically, it’s imperative that e-mail and instant messaging be managed and monitored to ensure compliance. In order to comply with a range of current mandates, organizations must be able to track, manage, secure, and retrieve business communications data.

Part of what hinders compliance is the increasing complexity and cost to add compliance capabilities to existing e-mail and messaging systems. That’s changing with the availability of Microsoft Exchange Server 2007. Designed to enable organizations to quickly implement and enforce comprehensive e-mail compliance measures, Exchange Server 2007 includes new and expanded messaging management features built into the software. With the option of Microsoft Exchange Hosted Services for outsourced messaging security and management, even companies with limited IT capabilities can bring their e-mail into compliance.

This paper covers typical e-mail compliance requirements enterprises are faced with and how Microsoft Exchange Server 2007 provides a robust, yet cost-effective solution to companies’ compliance challenges.

---

\* “The Costs of Compliance in the U.S. Securities Industry,” Survey Report, February 2006, Securities Industry Association  
† Conkey, Christopher, *The Wall Street Journal*, April 21, 2005



## Organizations at Risk

In a recent e-mail usage study, IDC estimates that the size of business e-mail volumes sent annually worldwide will exceed 3.5 exabytes in 2006.<sup>‡</sup> Exactly what percentage of this volume compromises compliance regulations affecting the organizations sending and receiving the e-mail is not known. However, a significant number of companies are still lacking comprehensive e-mail policies and procedures that address compliance and corporate guidance rules.

For instance, only 35% of employers have an e-mail retention policy in place, according to a report by the American Management Association and the ePolicy Institute.<sup>§</sup> In the same survey, 43% of regulated employees report that they either do not adhere to regulatory requirements governing e-mail retention, or are unsure if they are in compliance.

This lack of comprehensive and enforceable e-mail policies and controls impacts companies large and small, both public and private. The following examples from the financial services sector demonstrate the risk of non-compliance:

- In May 2006 the Wall Street Journal reported that the SEC filed a civil injunctive action against Morgan Stanley for failing to produce tens of thousands of e-mails during a Commission investigation, with the result that Morgan Stanley agreed to settle the dispute with a \$15 million civil penalty payment.<sup>\*\*</sup>
- In March 2004, the SEC penalized Banc of America Securities (BAS) for “repeated document production failures during a pending investigation” because the company “failed promptly to produce electronic mail” pertaining to ongoing litigation. As part of the settlement, BAS agreed to a censure and a \$10 million civil penalty

For healthcare organizations, HIPAA violation penalties can also be extremely expensive, in fines, lawsuits, and potential loss of business. The Healthcare Information and Management Systems Society, representing more than 15,000 individual members and about 220 companies, surveyed 400 health care firms in 2005. Only 18% of the providers and 30% of the insurers that responded to the poll said they would be compliant by the April 2005 deadline.

The American Health Information Management Association conducted a survey in January 2005 among privacy, security and compliance officers. Just 44% of the 1,140 respondents said they were close to achieving compliance, with only 18% stating their companies were fully compliant with the HIPAA security rules.<sup>††</sup>

Part of what is delaying organizations' full compliance with regulations is identifying exactly what capabilities are required for e-mail compliance. Even

---

<sup>‡</sup> “IDC Examines the Future of Email As It Navigates Security Threats, Compliance Requirements, and Market Alternatives,” IDC Press Release, December 22, 2005

<sup>§</sup> “2004 Workplace E-Mail and Instant Messaging Survey,” American Management Association and The ePolicy Institute

<sup>\*\*</sup> “SEC Accepts Morgan Stanley’s Email Settlement, and more,” Wall Street Journal, May 11, 2006

<sup>††</sup> “Health Care Lags on HIPAA Security Rules,” Vijayan, Jaikumar, Computerworld, April 11, 2005

for companies with a good understanding of what is needed to comply, the complexity and cost of implementing and enforcing e-mail controls and procedures has been a daunting task.

## Compliance Requirements for E-Mail and Messaging

What do organizations need in order to make e-mail communications compliant? The most important component is a corporate e-mail policy. Based on relevant laws for their industry, compliance or risk officers should create corporate messaging policies that include compliance measures.

In addition to compliance with external legislation, companies also need to mitigate the risk of corporate liability and financial loss resulting from improper e-mail usage and lack of retention policies for corporate communications. Leveraging best practices and legal guidelines, organizations need to create and enforce corporate e-mail and messaging policies that address areas of potential liability such as: disclosure or transfer of intellectual assets, discrimination, harassment, client/attorney privilege, and other measures of due diligence protection against criminal and civil liability.

Compliance officers will find that most laws and corporate guidelines require the following e-mail capabilities in order to ensure compliance with e-mail policies:

1. **Message Retention** – Companies need the ability to automatically retain e-mail messages for the amount of time required by relevant legislation. Search and retrieval of retained e-mails is another core capability, particularly for legal discovery. According to a recent survey, one in five employers has had e-mail subpoenaed.<sup>‡‡</sup> Without the proper policies and procedures for retention and destruction of e-mail, as well as a search mechanism, companies can incur tremendous costs. These costs range from the resources invested to recover and process e-mail from back-up files to potential fines, settlements and judgments against the company due to failure to produce required evidence in a timely manner.
2. **Controlled Access** – A major component of many privacy and corporate integrity laws is the protection of private information, as well as preventing unauthorized access to certain types of data. Companies must be able to secure e-mail transmission and prevent unauthorized disclosure by e-mail of certain types of data.
3. **Information and Process Integrity** – A number of regulations require procedures and controls to be in place to ensure integrity of certain processes and types of data. For e-mail compliance, this could mean applying handling instructions to relevant classifications of e-mail, automatically sending copies of e-mails to compliance officers, or enforcing an “ethical wall” scenario (a screening mechanism to protect against conflict of interest situations).

---

<sup>‡‡</sup> “2005 Electronic Monitoring & Surveillance Survey from American Management Association (AMA) and the ePolicy Institute,” ePolicy Website

The following overview provides a sample of the types of laws that pertain to organizations and their business data and communications in the form of e-mail and messaging.

## Message Retention

There are several regulations, particularly within the financial services industry, that require companies to retain business communications, including e-mail and instant message (IM) communications.

### **SEC Rule 17a**

From the U.S. Securities and Exchange Commission (SEC), this mandate establishes retention policies for brokers, dealers, and exchange members. The rule requires original copies of all communications be preserved for a period of no less than three years, with the first two in an easily accessible location.

### **NASD Rule 3010**

The National Association of Securities Dealers (NASD) Rule 3010 requires that broker-dealers and others implement specific capabilities for the sampling and review of messages sent out by broker-dealers. Other applicable NASD rules are Rules 3110 and 2210, which also establish retention regulations.

### **Other Regulations**

Other regulations that mandate retention of e-mail and messages include New York Stock Exchange rules, The Universal Market Integrity Rules for Canadian Marketplaces, and the Companies Act in the U.K.

### **Controlled Access**

There are a broad range of both U.S. and international laws pertaining to the usage and protection of private information. As of this writing, 23 states have passed data protection laws modeled on California's Senate Bill 1386 (SB 1386) which mandates public disclosure of computer security breaches involving private data of California residents. So far this year, at least 26 more bills have been introduced in 13 states.

### **Health Insurance Portability and Accountability Act (HIPAA)**

HIPAA requires that all health care organizations adopt medical information security, privacy, and data standards for patient information. The legislation also applies to companies with employee health records. Health data must be isolated and inaccessible to unauthorized access and the transmission of health information must be physically, electronically, and administratively safeguarded to ensure the confidentiality of data.

### **Gramm-Leach-Bliley Act (GLBA)**

The Gramm-Leach-Bliley Act requires financial institutions to safeguard clients' private information. It imposes HIPAA-like standards for protecting customers' information. As part of its implementation of the GLB Act, the Federal Trade Commission (FTC) issued the Safeguards Rule under section 501(b), requiring financial institutions under FTC jurisdiction to secure customer records and information.

### **The European Union Data Protection Directive of 2002**

This regulation updates legal standards for the processing of personal data and the protection of privacy. The law sets stringent restrictions on which personal information can be collected and stored. It also dictates rules for passing personal data to non-EU countries.

Information and Process Integrity

These regulations require organizations to create, evaluate, and monitor internal controls affecting how certain types of data are handled.

### **Sarbanes-Oxley Act**

This law mandates that public companies must control, protect, and retain information related to financial data that must be publicly disclosed. Companies must ensure that effective internal controls are in place to protect financial reporting data handled via e-mail.

### **Rule 21 CFR 11**

Primarily focused on pharmaceutical and other Food and Drug Administration (FDA)- controlled industries, CFR 21 defines requirements for electronic records, electronic signatures, non-repudiation, authenticity, and other controls.

### **USA PATRIOT Act**

This law requires financial services and insurance companies to implement anti-terrorism and anti-money-laundering regulations, including capabilities to identify customers and flag suspicious transactions. Broker-dealers must implement and document customer identity verification procedures; e-mail communications to establish a new account could fall under this rule.

### **Other Process-Related Regulations**

Based on Sarbanes-Oxley, other countries are introducing similar legislation, among them Belgium, Canada, France, Japan, the Netherlands, and the UK. A sample of other regulations that mandate process controls include international laws such as Bill 198 in Ontario, The European Union Markets in Financial Instruments Directive, Basel II, and U.K.'s Combined Code of Corporate Governance 2003.

## Fulfilling Compliance Requirements – Microsoft Exchange Server 2007 and Exchange Hosted Services

Microsoft Exchange Server 2007 is a secure, reliable enterprise-class messaging server with built-in compliance capabilities that delivers an integrated, cost-effective and manageable e-mail compliance solution. Addressing the e-mail compliance needs of organizations in financial services, healthcare, and other regulated industries, the built-in capabilities of Exchange Server 2007 help simplify compliance with company policies and regulatory controls by allowing organizations to filter, examine, change, journal and archive any message in their system.

For instance, Exchange Server 2007 enables compliance officers and e-mail administrators to address the message retention, controlled access, and process and data integrity challenges of compliance by:

- Establishing automatic retention to enforce archival and deletion policies
- Creating mail flow rules for enforcing encryption and routing policies
- Streamlining the message audit process with powerful new tools and cross-mailbox search

While Exchange Server 2007 provides a robust toolset for companies to create e-mail compliance solutions that meet their particular industry and business needs, it also integrates seamlessly with Microsoft Exchange Hosted Services. Exchange Hosted Services provide offsite protection for filtering, archiving, encryption, and availability outside of the corporate network.

### New Compliance Features Within Exchange Server 2007

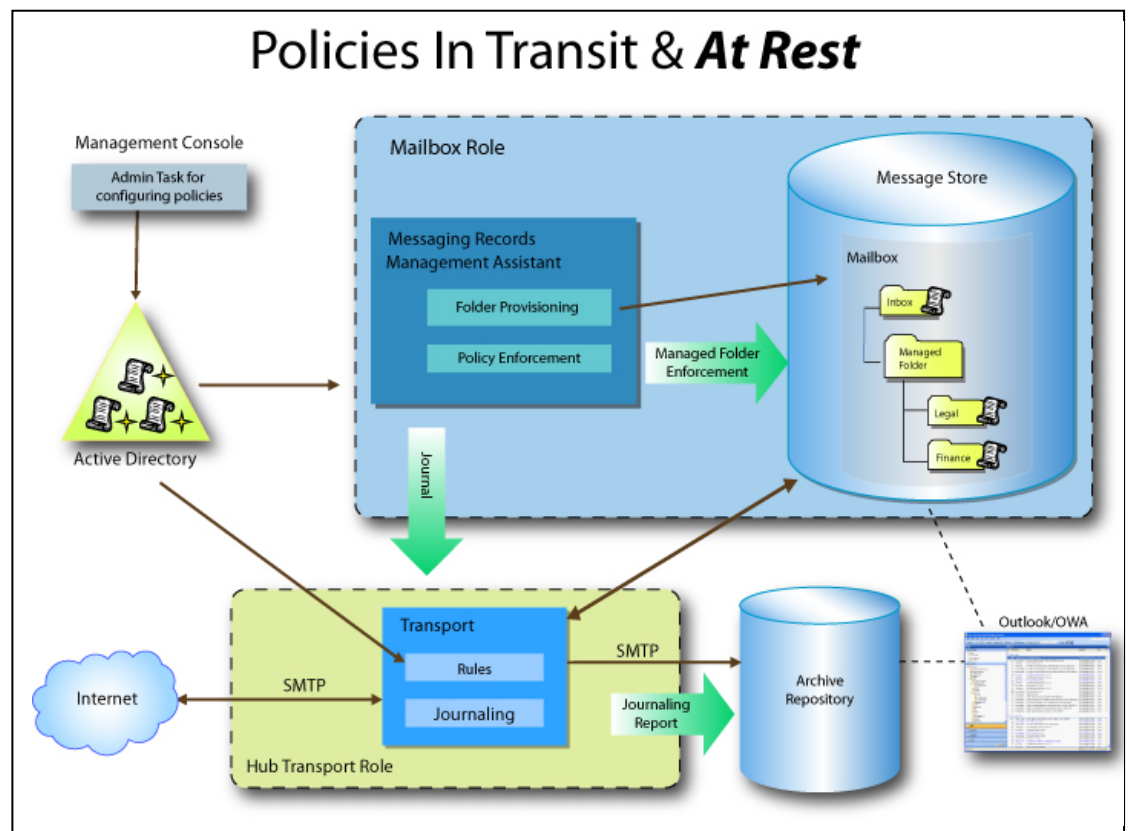
Exchange Server 2007 provides a robust set of new and enhanced features specifically designed to enable compliance/risk officers and e-mail administrators to manage and enforce compliance with company and regulatory e-mail policies across the entire organization. These features, combined with Exchange Server 2007 topology changes, enable mail flow controls to be implemented globally across the enterprise.

Administrators can create a policy, for example, that prevents employees from different groups within the company – e.g. brokers and research analysts – from exchanging e-mail messages with one another. Policies can be created so that e-mail messages pertaining to certain topics, based on classifications assigned by e-mail users, are automatically archived or routed to a compliance officer for review.

**Policy Management:** The new policy engine within Exchange Server 2007 is managed via the definition of transport rules, which are similar to Outlook rules and easily created within the Exchange Management Console. With Transport Rules, administrators and compliance officers can establish and

enforce regulatory or corporate policies on internal or outbound e-mail, voice mail, or fax. Transport rules provide a flexible and extensive set of conditions, actions, and exceptions to allow administrators and compliance officers to implement exact policies to enforce compliance. These policies can address retention, controlled access to data, protection of private information, and process control, among other compliance-related rules. See figure 1 on Policies in Transit and At Rest.

For example, using a wizard in the Exchange Management Console or the command line in Exchange Management Shell, rules can be written that would prohibit communication between members of distinct distribution lists, require encrypted delivery of any message containing confidential information identified through text pattern matching, append a disclaimer to any message being sent externally, or send a blind carbon copy (BCC) to the compliance officer any time a specific phrase appears in the subject or content of a message. These rules can be automatically enforced across the entire organization.



**Figure 1. Policy Management & Enforcement Within Microsoft Exchange Server 2007**

**E-Mail Retention:** The substantially-enhanced journaling capability within Exchange Server 2007 provides additional flexibility to simplify and streamline compliance. In addition to now being able to implement per-user and per-distribution list journaling, Exchange Server 2007 allows administrators to automatically journal e-mail messages based on company policies using journal and/or transport rules. Journaled/archived messages include not only the original message, but information about the sender, recipients, copies, and blind copies. Another new feature in Exchange Server 2007 is the ability to journal to any valid SMTP address, which enables support of hosted service or third-party archives. Exchange Server 2007 provides organization-wide configuration of journaling using Active Directory for streamlined administration.

**Messaging Records Management:** The new managed folders feature enables compliance officers and administrators to create message retention groups to better organize and manage e-mail messages. Managed e-mail folders feature automatic retention for e-mail items in the folder. An automated process scans the inbox and these folders to retain, expire, or journal communications based on compliance requirements. Once administrators create the folders, users make the choice as to which retention group, i.e. folder, applies to a given item and Exchange Server 2007 then enforces retention policies. Summary reports enable compliance officers to verify usage of the managed folders.

**Discovery and Audit:** Using the Microsoft standard search technology, content in Exchange Server 2007 mailboxes is fully indexed and searchable using a variety of criteria. If compliance or legal requirements require information discovery, administrators can search across multiple mailboxes within an organization with a single query, routing the results to a mailbox that can be made available via Microsoft Outlook to legal, HR, compliance officers, or others.

**Message Security:** Exchange Server 2007 ensures trusted e-mail flow, protecting sensitive information in-transit as required by certain regulations. With encryption, sender signing, and support for rights management technology, messages remain confidential both inside the organization and over the Internet.

**Process Integrity:** Configuration logging provides detailed audit trails for compliance officers and administrators to demonstrate compliance practices. Each action taken by an Exchange administrator can be logged, providing documentation of compliance policies over time. In addition, statistical reports enable managers or compliance officers to identify users who are not following e-mail policies. Another new feature within Exchange Server 2007 is message classification, which allows administrators to flag messages for special handling using preconfigured or customized classifications, such as “company confidential” and “attorney/client privileged.” Using a new feature within Outlook 2007, end users can also choose from company-defined categories

for the purpose of classifying messages for special handling; a built-in information bar defines each classification.

## Industry Compliance Scenarios for Exchange Server 2007

The following examples highlight how Exchange Server 2007 can help organizations comply comprehensively and cost-effectively with legislation and company policies affecting e-mail and messaging communications.

### **Financial Services – E-Mail Retention and Discovery**

Financial services firms face extremely strict regulatory requirements for controlling, preserving and accessing e-mail. With over 90 percent of compliance costs for securities companies being staff-related,<sup>§§</sup> reducing the complexity and effort required to comply is a key objective of financial services companies both large and small.

The new built-in capabilities of Microsoft Exchange Server 2007 address this challenge. For example, by using the new, easy-to-use transport rules within Exchange Server 2007, compliance officers and administrators can establish automatic journaling or archiving of every message that enters or exits the company, including the origin of the message, the recipients, who was copied, or who was blind-copied. Journaling can also be based on whether the sender/recipient is a member of a particular group, whether they are internal or external, and other criteria.

Administrators can also create managed folders that incorporate company retention policies. Users then classify content by dragging items into managed folders such as “Stock Trades,” “Analyst Reports,” or “Personal E-mail.” The per folder expiration policies are set by the e-mail administrator and ensure corporate retention policies are enforced and e-mail is deleted promptly upon expiration. Compliance officers can receive copies of e-mails based on company policy for specific classifications of e-mail correspondence. Compliance officers and administrators can monitor retention compliance through summary usage reports.

For audit and discovery purposes, the enhanced search features allow searching across multiple mailboxes. Search results are then copied to a separate mailbox – to a compliance officer or other manager, for instance. Specific mailboxes can also be placed on “hold” which stops automatic retention enforcement when litigation may be pending.

With Exchange Server 2007, financial services organizations can more readily and easily comply with current legislation, with built-in flexibility to change e-mail policies as mandates evolve.

---

<sup>§§</sup> “The Costs of Compliance in the U.S. Securities Industry,” Carlson, Stephen L. and Fernandez, Frank A., Securities Industry Association, February 2006

### **Brokerage – Ethical Wall Requirement**

Particularly applicable for the brokerage industry, the ability to establish and enforce an “ethical wall” for e-mail is a critical function for compliance with certain regulations. An ethical wall enforces separation between groups such as brokers and market research by not allowing any e-mail messages to be sent or received between members of certain departments.

Working together with the IT administrator, a compliance officer can establish an ethical wall policy within Exchange Server 2007 simply and quickly by using a transport rule that checks every e-mail to see whether communication between members of the separated groups is being attempted. If an attempt is made at communication between these groups, the server bounces the e-mail and sends a pre-configured message to the sender.

### **Healthcare – Secure Delivery & HIPAA Compliance**

Compliance with HIPAA, which mandates how private information must be protected to prevent unauthorized disclosure, has required healthcare providers and companies handling patient/employee-related health data to implement strictly enforced policies on data handling, including e-mail messages.

Exchange Server 2007 eases the compliance pain for healthcare-related companies by providing increased capabilities for enforcing data privacy in e-mail messages. From transport rules that apply handling instructions to encryption of e-mail content to audit trails of configuration changes, healthcare organizations can enforce company e-mail policies that prohibit unauthorized disclosure of private data.

For example, using the transport rules wizard in the Exchange Console Manager, an e-mail administrator can create a rule that searches the subject and content of every e-mail being sent for a pattern that reflects a social security number. If an e-mail is generated with content that includes a social security number and the sender attempts to send it to a recipient outside of the organization or one that is not defined as being authorized to receive confidential information, the e-mail is bounced. The sender then receives a pre-configured error message.

Healthcare companies can auto-encrypt e-mails containing confidential information that are being sent internally. This protects sensitive information in-transit without requiring any client software or end user training. Companies required to comply with HIPAA now have the ability to use the built-in capabilities within Exchange 2007 to more easily comply with the security requirements of the regulation.

### Corporate Policy Controls

In addition to compliance with legislation, organizations should have and enforce corporate e-mail policies based on best practices for risk mitigation.

Exchange Server 2007 includes extensive support for the capabilities required to enforce corporate e-mail policies. These built-in features include:

- Application of legal disclaimers to outbound messages
- Protection against intellectual property disclosure
- Preventing offensive language or content from being sent via e-mail
- Searching across mailboxes for legal discovery
- Automatic retention and expiration policies

Exchange Server 2007 enables companies to comprehensively implement and enforce e-mail rules to comply with corporate policies. Using transport rules, administrators can select conditions, actions, and exceptions that handle a wide range of capabilities from appending disclaimers to filtering content for offensive language.

For example, a transport rule can be created that checks the sender and/or recipient, automatically categorizes the e-mail as attorney/client privilege, and pre-pends a disclaimer with instructions to both sender and recipient. An administrator could also create a rule that prevents any message that is classified as company internal from being sent to an external recipient.

## Microsoft Exchange Hosted Services

Exchange Hosted Services for messaging security and management help organizations confidently satisfy compliance and business continuity requirements. Ideal for organizations constrained by resources or lacking in compliance expertise, Exchange Hosted Services are fully outsourced solutions that operate “in the cloud” without the need for additional on-site software or hardware.

Among other capabilities, Exchange Hosted Services offers solutions that address archival and encryption compliance requirements placed on organizations such as those in the financial services and healthcare industries. As retention requirements force greater amounts of records to be retained, services such as Exchange Hosted Archive, enable terabytes of storage without the cost of building and maintaining an on-premise infrastructure.

### **Financial Services – Hosted Archive Scenario**

One of the areas where smaller or medium-sized brokerages are hardest hit when it comes to compliance is the retention and destruction of e-mail and instant message communications. Exchange Hosted Archive helps brokerages and other companies rapidly comply with regulations such as SEC- 17A and NASD 3010.

Using Exchange Hosted Archive, as messages pass through the network, a copy of each is made and stored in a security-enhanced repository. Mail sent

within the organization is captured by the journaling function within Exchange Server 2007 (and previous versions of Exchange) and sent to the archive. Instant messages and other communications can be copied directly to the archive.

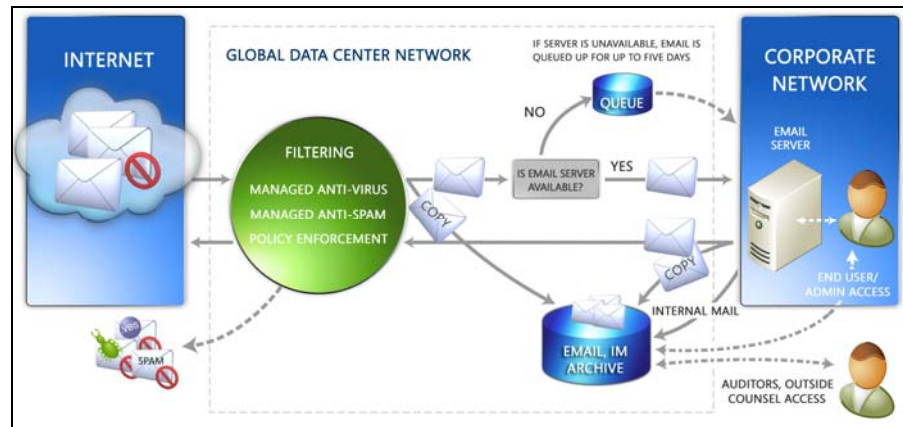


Figure 2. Exchange Hosted Archive intercepts messages “in stream,” which allows message filtering to be performed prior to archiving, improving the efficiency of archiving operations and eliminating unwanted content from the archive.

In addition to automatic retention and destruction of messages, Exchange Hosted Archive provides other key capabilities financial services companies need to ensure compliance with SEC and NASD rules:

- Non-tamperable archive (messages cannot be deleted before their scheduled time)
- Automatic archiving of messages, destruction of expired messages, and harvesting of messages for review
- Classification categories for reviewed messages, with escalation capability included
- Supervisor evidentiary report – evidence that reviews are happening on a regular basis including what’s scheduled to be done and what percentage of these tasks have been completed
- Temporarily halt destruction of messages during pending legal processes
- Audit Trail to report on all actions taken within the application
- Ad hoc search and retrieval of messages from the archive, with keyword and phrase matching

### Healthcare – Hosted Encryption Scenario

The ability to share patient health information with doctors, family members, family physicians, government agencies, and others via e-mail and message attachments is an important part of improving the speed and efficiency of healthcare organizations. However, these communications must meet HIPAA requirements for secure transmission of patient information. These

requirements have proved troublesome and expensive for many healthcare organizations, especially smaller ones, to implement.

With Exchange Hosted Encryption, healthcare providers are ensured of secure transmission through encryption of e-mail messages. The service enables users to send and receive encrypted e-mail directly from their desktops as easily as regular e-mail. Using a simple process, users can encrypt and deliver any business communication without complex hardware and software to purchase, configure, and maintain.

By using a commonly used identifier—such as an e-mail address—as the encryption key, this solution provides a simple yet highly secure method to encrypt business communication, thereby helping to ensure compliance with HIPAA security rules. No additional steps or clicks are required on the user's part to ensure secure communication because the user is recognized by his or her e-mail address or user login.

The Exchange Hosted Encryption managed service is a cost-effective solution for healthcare companies lacking on-site technical expertise or with limited resources.

## Selecting the Right Compliance Solution

In determining the appropriate e-mail compliance solution for a company, organizations must balance a number of factors, including the diverse desires and needs of all the potential constituents: end users, legal department, human resources, IT operations, and compliance managers. With the internal and external factors clearly understood, companies can then evaluate e-mail compliance solutions to match capabilities to requirements and company philosophy.

Key criteria organizations should consider when evaluating e-mail compliance solutions, include:

- Provides key capabilities to address the compliance requirements of message retention, controlled access, and information and process integrity. Many solutions address one or more of these functions, but not all of them
- Reduces the complexity of e-mail compliance with easy-to-use policy management built in to the solution
- Enables organizations to flexibly implement only the policies and rules required by regulations relevant to their industry and geography
- Provides enterprise-class performance and reliability
- Integrates tightly and seamlessly with the enterprise messaging solution to minimize complexity and cost of ownership
- Provides freedom of choice for implementation between fully-hosted and in-house compliance solutions

Microsoft offers customers a range of compliance solutions from Exchange Hosted Services to on-premise Exchange Server 2007. According to Gartner Group's Rich Mogull, "Implementing a compliance architecture with an enterprise's current technology can help reduce the cost of regulatory compliance."<sup>\*\*\*</sup>

Exchange Server 2007 meets all of the criteria for a comprehensive e-mail compliance solution. Its built-in compliance features, as well as architecture changes, enable organizations to address the key e-mail challenges of message retention, controlled data access, and information and process integrity in an integrated, flexible way across the entire enterprise. It provides a robust, easy-to-use toolkit for customizing policies specifically to meet an organization's unique compliance and corporate challenges.

Erica Rugullies, Forrester Research analyst, commented, "Businesses have been clamoring for the leading e-mail providers, like Microsoft, to enhance the capabilities of mail servers. [With the new services,] Exchange customers

---

<sup>\*\*\*</sup> "Email Compliance Quick Reference Guide, Strategies for Regulatory Compliance and Legal Risk Management," Overyly, Michael R.

won't have to seek out a third-party product for archiving and e-mail management."<sup>†††</sup>

---

<sup>†††</sup> "Microsoft Revamps Hosted-Messaging Services," Erica Rugullies, Forrester Research, March 30, 2006, NewsFactor.com

## Summary

Establishing, enforcing and proving e-mail compliance is a key requirement for companies across all industries, but especially in the heavily-regulated industries of financial services and healthcare.

Microsoft Exchange Server 2007 offers new, built-in compliance features designed to help organizations cost-effectively comply with regulations. Starting with the new policy engine, this latest version offers compliance-ready capabilities such as enhanced journaling, multiple mailbox search, message categorization, automatic retention and expiration of messages, and audit trails. Companies can create and enforce the policies they need for their particular industry and business requirements.

For organizations without the internal IT infrastructure or desire to customize a solution, Microsoft also offers turn-key, hosted solutions – Microsoft Exchange Hosted Services – that address specific areas of compliance such as encryption and archiving. Exchange Hosted Services complement on-premise or hosted Exchange e-mail servers.

Microsoft's compliance capabilities within the e-mail server enable companies to lower the cost and reduce the complexity of implementing controls. Ease of compliance provides a compelling case for upgrading to Exchange Server 2007.



---

### Legalese (style = Legalese)

This is a preliminary document and may be changed substantially prior to final commercial release of the software described herein.

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 OR IMPLIED, 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.

© 2005 Microsoft Corporation. All rights reserved.

Microsoft, are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries.  
All other trademarks are property of their respective owners.