



WHITEPAPER

Addressing Compliance with Microsoft® Exchange Server 2010

Overview

Microsoft Exchange Server 2010 can help organizations better meet compliance requirements for email including data retention, discovery, policy management and security. This paper provides an overview of compliance tools in Exchange 2010 and describes how they can help support common compliance scenarios. Note that Exchange 2010 is not designed to address all requirements of any specific regulation. Microsoft recommends that you work closely with your compliance subject matter experts, legal counsel, and auditors to confirm the complete set of businesses processes and technical controls suitable for your organization.

Introduction

With the bulk of business communications today being conducted electronically, email has come under increasing scrutiny by regulators.

Much of this scrutiny is aimed at regulated businesses such as those in financial services and healthcare. But messaging compliance actually extends much further to practically every size and type of organization. This includes messaging requirements related to legal e-Discovery, internal governance, industry standards, and other regulations.

Failure to manage these regulatory issues can result in severe consequences including financial, civil, and criminal penalties. Often even more damaging for companies are the indirect consequences of non-compliance including loss of reputation, diminished credit ratings, and even loss of market share to compliant competitors.

Despite the risks, many organizations fail to properly manage messaging compliance. For instance, only 35 percent of employers have an email retention policy in place according to a report by the American Management Association and the ePolicy Institute.¹ In the same survey, 43 percent of regulated employees report that they either do not adhere to regulatory requirements governing email retention or are unsure if they are in compliance.

Email represents a particularly daunting challenge for compliance. It is typically scattered across an organization in different databases and on devices both inside and outside the organization. For this reason, it can be difficult to apply consistent security, retention, and control policies.

Lack of centralization also poses a challenge for discovery, which often has to be done manually. This leads to added costs and complexity, especially when outside specialists are required. While there are numerous technologies available to automate compliance processes, they often involve additional user education and administrative support, adding to the complexity.

¹ "2007 Workplace Email and Instant Messaging Survey," American Management Association and The ePolicy Institute
*Requires Exchange Server 2010 Service Pack 1.

Compliance and Email

Following is a sampling of regulations across a wide range of industries that typically apply to email. While many regulations outline strict requirements for the handling of data, few make direct reference to specific types of data such as email. For this reason, it is important to carefully monitor the data transmitted and stored by your organization via email. If the data is regulated, your email systems may be subject to that regulation.

General

Electronic Discovery (e-Discovery)

E-Discovery refers to the preservation, retrieval, and review of electronically stored information (ESI), for litigation purposes. Unlike other regulatory scenarios, e-Discovery requirements affect virtually all companies subject to litigation. In the United States, e-Discovery is the subject of amendments to the Federal Rules of Civil Procedure (FRCP). Specifically, the FRCP Amendments require organizations to be able to retrieve in a timely manner all ESI (including email) that may be relevant to a case. This is not to say that all email data must be preserved at all times. The ruling provides "safe harbor" for companies that delete relevant data, as long as it is done based on "good faith" application and auditing of standard retention processes. Policies must be applied consistently before litigation is reasonably foreseeable in order to be eligible for "safe-harbor".

Sarbanes-Oxley Act (SOX)

This law, commonly referred to as SOX, was designed to bring greater accountability and transparency to the financial operations of all publicly traded companies. While SOX does not explicitly call out email, SOX mandates that public companies must control, protect, and retain financial data *and related files* that must be publicly disclosed. For example, SOX requires auditors to retain work papers and other information related to any audit report for a minimum of seven years. SOX also mandates that controls be put into place to prevent "unauthorized use" of or tampering with financial information both at rest and in transit and that these controls be documented for auditing purposes. Based on SOX, other countries have introduced similar legislation including Belgium, Canada, France, Japan, the Netherlands, and the United Kingdom.

The European Union (EU) Data Protection Directive

The EU Data Protection Directive (also known as Directive 95/46/EC) was designed to protect the privacy of personal data of EU citizens, including personal data contained in email. The directive extends to data that is passed outside the EU and also applies to foreign companies that have employees or customers in EU member states. Processing and collection of personal data can only be done with user consent. Once data is collected, the collecting organization must implement appropriate technical measures to prevent its destruction, loss, alteration, or unauthorized disclosure, storage, or access.

Financial Services

United States Securities and Exchange Commission (SEC) Rule 17a

The SEC originally enacted the Securities Exchange Act to protect investors from fraudulent or misleading claims by securities dealers. The Act required member firms to create and maintain transaction records which could be reviewed and audited. Rule 17a-4 of the Act was amended to provide procedures for storage of electronic records, including email and instant messages. The rule requires that archived messages must be stored for three years in duplicate in a non-rewriteable and non-erasable format. During the first two years of storage, all messages must be easily accessible to enable immediate SEC review if required.

National Association of Securities Dealers (NASD) Rule 3010

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 establish retention regulations similar to SEC Rule 17a-4.

Gramm-Leach-Bliley Act (GLBA)

GLBA requires financial institutions to safeguard clients' private information. This includes encrypting messages that contain confidential information when transmitted over an unprotected link, controlling access to sensitive customer data, and protecting email servers and network drives where confidential information may be stored. GLBA also requires specific protection from phishing, since this form of traffic may increase the risk of unauthorized access and use and of confidential data.

Healthcare and Life Sciences

Health Insurance Portability and Accountability Act (HIPAA)

HIPAA requires that health care organizations adopt medical information security, privacy, and data standards to protect patient information. It extends to other organizations that may store or transmit patient data, such as health insurance companies. Health data must be isolated and inaccessible to unauthorized access, and the transmission of health information by email must be secured to ensure the confidentiality of data. While HIPAA does not specifically mention the retention of email, there is a required preservation period of up to six years for security and privacy policies, procedures, documentation of complaints, and other medical records. Email containing these types of data may be subject to the retention period.

Rule 21 CFR Part 11 (21 CFR 11)

Primarily focused on pharmaceutical and other U.S. Food and Drug Administration (FDA)-controlled industries, 21 CFR 11 defines requirements for electronic records, electronic signatures, non-repudiation, authenticity, and other controls. If the text in an email supports activities such as change control approvals or failure investigations, then the email messages have to be managed in a compliant way. This includes the use of secure electronic signatures as well as an audit trail of additions, deletions, and changes that is computer-generated, operator-independent, time-stamped, and secure.

*Requires Exchange Server 2010 Service Pack 1.

Compliance Requirements for Email

Organizations are subject to a myriad of regulations and policy mandates. However, most compliance scenarios are actually based on a common set of basic data management requirements. In terms of messaging compliance, these requirements typically include the following:

- **Retention & Discovery**

Organizations often need to retain email messages for an amount of time required by legislation. Many regulations also require timely access to these messages for discovery purposes. Searches prolonged through lengthy investigation of back-up tapes, for example, not only incur additional costs but can actually result in legal and regulatory penalties. Centralized archiving, retention, and search capabilities can help increase the efficiency of preservation and discovery processes.

- **Inspection & Control**

Most regulations require a set of controls to ensure the integrity of certain processes and types of data. For email compliance, this typically involves tools that can analyze messages for specific attributes such as personal data and apply appropriate routing or modification controls. Common scenarios include the ability to restrict messaging between specific senders, intercept sensitive messages for review or re-routing, or apply disclaimers or other modifications.



- **Security & Protection**

Security and protection of email traffic is required to ensure the privacy and confidentiality of customer and client data as well as sensitive corporate data such as financial records. This is typically achieved through various forms of encryption and rights management. Security settings at the device level are equally important, especially with the increasing use of mobile devices. Additionally, anti-spam and antivirus tools may be required to protect email from viruses that can affect the integrity of both systems and data. Anti-phishing protection can help maintain privacy.

[Exchange 2010 features advanced capabilities that can help automate and simplify fundamental compliance requirements.](#)

- **Reporting and Availability**

Underlying each fundamental requirement is the need for system and data availability. Highly available email systems are necessary to ensure the preservation and accessibility of email as

*Requires Exchange Server 2010 Service Pack 1.

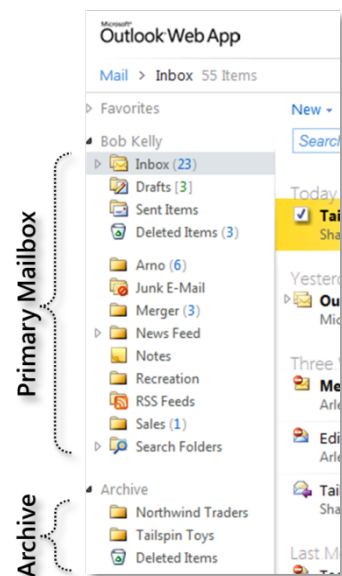
well as the consistent and thorough application of messaging control policies. Equally important is accurate reporting of compliance-related processes for monitoring and auditing purposes.

Some of these requirements will be more important than others depending on your specific compliance needs. HIPAA, for example, focuses largely on protection of patient data, while SOX emphasizes tight controls on financial reporting. In an ever-changing and expanding regulatory environment, it is prudent to address each basic requirement when developing your long term messaging compliance strategy.²

Supporting Compliance with Exchange 2010

Exchange 2010 supports the fundamental requirements of messaging compliance: preservation, discovery, control, protection, reporting, and availability. However, as with all messaging technology, it is important to note that no single technology can offer a turnkey 'compliance solution', as compliance requires procedural controls such as training and auditing that are beyond the scope of technology. That said, Exchange 2010 can help reduce the cost and complexity of a wide range of compliance challenges.

The out-of-the-box integration of Exchange compliance-related capabilities can provide even greater value and support complex compliance scenarios. Many of these features have been specifically designed to integrate with advanced partner solutions through scalable Web services interfaces. In this way, organizations can extend the compliance-related functionality of Exchange 2010 to address even the most specialized regulatory requirements.



Preservation and Discovery

Exchange 2010 helps make it easier and more efficient to preserve and discover email through a wide range of integrated archiving capabilities.³

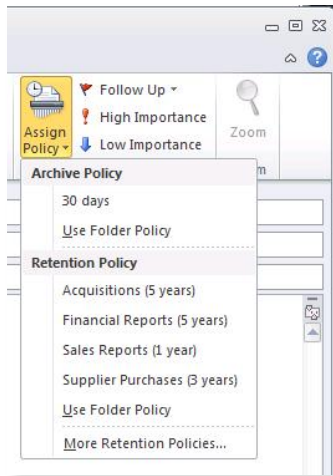
Personal Archive is a specialized mailbox associated with a user's primary mailbox. From a compliance standpoint, the Personal Archive is designed to address the discovery issues related to .PST files (also known as Microsoft Outlook® Data files) by making it easier to search and manage archives centrally within Exchange Server rather than separately on user's desktops. Email data from .PST files can be easily dragged and dropped into the Personal Archive.⁴ Email items from a user's primary mailbox can

² For details on general compliance planning strategy, consult the Microsoft IT Compliance Planning Guide, available at <http://technet.microsoft.com/en-us/library/dd206732.aspx>.

³ For more details, download the Exchange 2010 Archiving and Discovery whitepaper at: <http://go.microsoft.com/?linkid=9728428>

⁴ Administrators can also use the Import PST command.

also be automatically offloaded to the Personal Archive using retention policies. To help manage storage, Personal Archives can be moved to a database separate from primary mailboxes.*



Retention Tags enable the consistent application of retention and deletion schedules to email items, conversations, or folders in a mailbox. With retention tags, items in a user's primary mailbox can be automatically moved after a specified time to the Personal Archive or Deleted Items folder, or permanently deleted. Retention tags can be applied to default folders such as the Inbox and Sent Items to assign consistent retention actions across single or multiple mailboxes. Exchange 2010 administrators can also create personal tags to allow users to assign different expiration dates to specific items and folders in their mailbox. One or more tags can be grouped into a retention policy and customized for groups and individual users. This can be particularly useful for an organization with complex retention schedules. For example, instead of exposing the organization's entire set of tags to each user, an administrator might

choose to push out a customized policy set per department. Users can then easily add pre-configured personal tags as needed through the Exchange Control Panel.* The retention age of mailbox items is

Retention tags can be organized into policy sets for specific users and groups.

calculated from the date of delivery, not when a retention tag is applied. This means that users cannot extend a retention period beyond the longest personal tag available. For example, if the longest personal tag is 250 days

and an email item has reached that time period, a user cannot add another 250-day tag to extend retention. Using both retention tags and personal tags, organizations can apply various levels of control as required. For complete control, companies can apply retention tags only that users cannot override. For more user flexible control, a company might deploy sets of personal tags that enable certain users to extend a retention policy by set time periods. And in cases where a user may require full control of email retention, their mailbox could be set up with personal tags only (including tags with no expiration date) and no default policies.

Legal Hold enables immediate preservation of a user's deleted and edited mailbox items (such as email, appointments, and tasks) from both the primary mailbox and Personal Archive. When a user on Legal Hold edits an email item or deletes it from their Deleted Items Folder, these items are saved in their Recoverable Items folder (known as a dumpster in previous versions of Exchange). Users on Legal Hold cannot purge items from the Recoverable Items folder and all items in this folder are discoverable through multi-mailbox search. Legal Hold can be set on individual mailboxes or across the enterprise. Legal Hold also includes an option that automatically alerts users through Microsoft Outlook 2010 that a hold has been placed on their mailbox. Note: Legal Hold does not capture header information. For this reason, some compliance scenarios may also require journaling (see below).

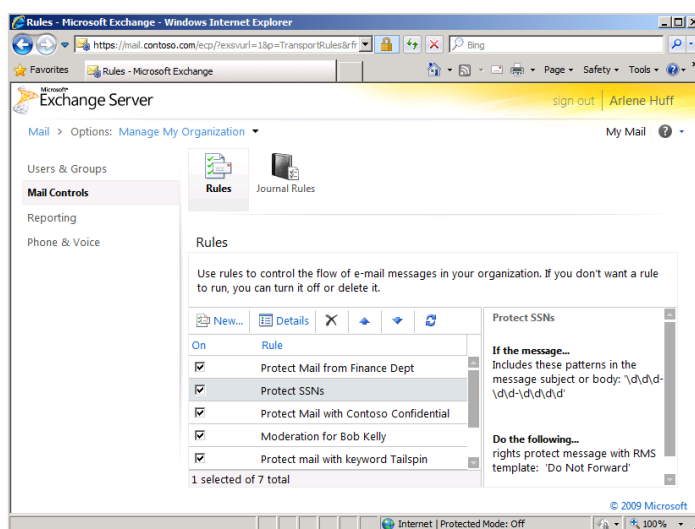
Single Item Recovery preserves edited and deleted items in the same way as Legal Hold. The difference is that, where legal hold preserves items indefinitely, single item recovery enables administrators to specify a holding period. For example, a single item recovery policy set to 90 days will preserve all edited and deleted items for that time period in the Recoverable Items Folder. Items older than 90 days will be deleted from the folder. Note: Items will also be deleted when the Recoverable Items Folder reaches a

*Requires Exchange Server 2010 Service Pack 1.

defined quota based on a first in, first out principle. To help manage this process and reduce the risk on unintended deletions, storage quotas can be customized for each Recoverable Items folder. The system will also provide alerts when volume approaches these quotas.

Multi-Mailbox Search enables searching of mailbox items across the organization including email, attachments, calendar appointments, tasks, contacts, and Information Rights Management (IRM)-protected content⁵. Rich filtering capabilities include sender, receiver, message type, sent/received date, cc/bcc, and advanced regular expressions. Multi-mailbox search can work simultaneously across primary mailboxes, Personal Archives, and recovered items with an easy-to-use, Web-based console. To help streamline discovery processes, search results may be previewed* with keyword statistics before email messages located in the search are copied to the designated discovery mailbox, providing an estimate on the number of items in the result set. Search result de-duplication* can help reduce the amount of email that needs to be reviewed. Finally, added support for annotation of reviewed items helps make the e-Discovery workflow even more efficient and less costly.

Journaling can also be used for archiving by taking a copy of specified messages, voicemail, and faxes and sending them to a journal mailbox or SMTP address—for example, a hosted archiving service such as Exchange Hosted Archive⁶. Journal rules can be set at the database, organizational, per-user, and per-distribution list level and configured to target internal or external recipients. Journalled messages include not only the original message, but information about the sender, recipients (including distribution list expansion), copies, and blind copies. With the new journal report decryption feature, Exchange 2010 can be configured to save a clear-text copy of IRM-protected messages in the journal report for more efficient discovery. Note: journaling does not capture email items such as calendaring items and tasks unless they are sent or received through the hub transport server role.



Compliance tasks such as multi-mailbox search, legal hold as well as transport and journal rules can be delegated to authorized users through a simple, web-based control panel.

Inspection and Control

Exchange 2010 provides policy management tools that make it easier to control email traffic throughout the organization.

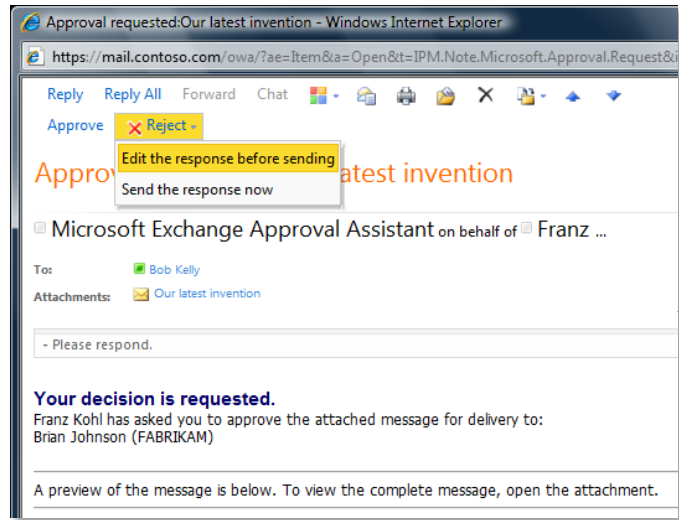
⁵See IRM Support below for technical requirements.

⁶ For companies where random sampling is required (such as with NASD rules in the financial services industry), messages can be journalled to an Exchange Hosted Archive which includes both automated sampling as well as Supervisory Evidentiary Review reporting to document and monitor compliance. Note that EHA is sold separately from Exchange Server.

*Requires Exchange Server 2010 Service Pack 1.

Transport Rules apply messaging policies to all email messages traveling inside and outside the organization. They are created similarly to Outlook rules using a set of conditions, actions and exceptions. Administrators and delegated users* can create transport rules based on a variety of email attributes including specific senders, recipients, distribution lists, keywords, and regular expressions (for common patterns such as those associated with credit card numbers or social security numbers). You can also create transport rules based on contents within a Microsoft Office attachment, a user's Active Directory® attributes (such as department, country, or manager), and multiple message types (including auto-replies and calendaring.). Exchange 2010 also features a wide variety of pre-defined actions including the ability to block, re-route and copy messages. New transport rule functionality particularly relevant to compliance scenarios includes:

- Transport Protection Rules:** when used with Active Directory Rights Management Services (AD RMS), transport protection rules enable an administrator to automatically apply Information Rights Management (IRM) protection to e-mail (including Office and XPS attachments) after a message is sent. This provides persistent protection to the file no matter where it is sent and prevents forwarding, copying, or printing depending on the set of AD RMS Policy Templates available from the AD RMS deployment.
- Dynamic Signatures:** automatically apply a signature to the bottom of an e-mail based on sender's Active Directory (AD) attributes. This feature can also be configured to apply rich, HTML signatures with specific fonts, company logos, and more.
- Moderation:** re-directs mail to a manager or trusted moderator for review. The reviewer can then approve or block the message and if blocked, provide an explanation back to sender. You can configure any type of recipient as a moderated recipient, and Exchange 2010 Hub Transport servers will ensure that all messages sent to those recipients go through an approval process.



Role Based Access Control (RBAC) allows Exchange 2010 administrators to grant users such as records managers, compliance officers, and litigators the specific rights needed to perform compliance-related activities.

The moderated transport feature enables pre-review of all messages before delivery by designated moderators

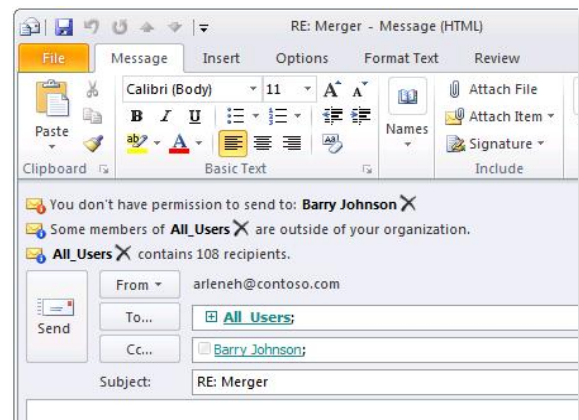
These activities may include multi-mailbox searches, creation of transport rules, retention policies and personal archives,* and access to administrator and mailbox auditing* (see Reporting, below). These rights can be controlled at a granular level. For example, administrators can restrict which mailboxes can be searched (which may be relevant to users covered by regional privacy regulations) and can also restrict the criteria that can be accessed to create transport rules.

Message Classifications can be applied automatically using transport rules or manually by users in Outlook 2010 or Outlook Web App. When a message is *classified*, the message contains specific

*Requires Exchange Server 2010 Service Pack 1.

metadata that describes the intended use or audience of the message (such as attorney-client privileged).

Exchange 2010 can also enforce message classification requirements when a message enters the transport pipeline. For example, transport rules can be used to identify messages with the attorney-client privileged message classification and check whether the message meets the organization's list of attorney-client privilege requirements (such as whether the message was encrypted or sent externally). If the message does not meet the requirements, it may be returned to the sender, IRM-encrypted, or subjected to other compliance actions.



MailTips alert senders about certain conditions that may result in policy violations or unintended delivery. For example, MailTips will display an alert if a message is about to be sent to a large audience or if the recipient is external, restricted, or moderated. Administrators can create customized MailTips based on specific recipients. The MailTips feature is available in both Outlook Web App and Outlook 2010.

MailTips alert users about potential risks and policy violations.

Protection

Exchange 2010 protects email data with powerful tools and support for encryption and email hygiene capabilities.

Intra-Organizational Encryption automatically encrypts sessions used to transmit messages within an organization. Transport Layer Security (TLS) encryption is used for server-to-server SMTP traffic and Secure Socket Layer (SSL) is used for HTTP client access traffic (Outlook Anywhere, Outlook Web App, Exchange ActiveSync®, and Exchange Web Services); RPC server-to-server traffic is also encrypted, and Outlook RPC traffic encryption can be required as well (RPC encryption strength is based on the operating system and Security Support Provider Interface).⁷

Inter-Organizational Encryption uses Transport Layer Security (TLS) to encrypt sessions for outbound mail. With Opportunistic TLS, Exchange 2010 will automatically encrypt the outbound session. In addition, inbound e-mail sent to Exchange Server 2007 from the internet will be encrypted if the sending server supports TLS (Exchange Server 2007 automatically installs SSL certificates). Exchange 2010 also supports mutual TLS authentication, where each server verifies the identity of the other server by validating a certificate provided by the other server. In this scenario, a Domain Secured icon is displayed in Outlook and Outlook Web App to verify that the message was received from an external domain over

⁷ For Outlook clients connecting via TCP and not via HTTPS, Exchange 2010 supports encryption of RPC traffic by default.
*Requires Exchange Server 2010 Service Pack 1.

a verified connection. This Domain Security functionality can provide a relatively low-cost alternative to S/MIME or other message-level security solutions.

Message Encryption can control how sensitive data is accessed and distributed. To protect messages, Exchange 2010 features extended support for both IRM and Secure Multipurpose Internet Mail Extensions (S/MIME).

- **IRM Support**⁸ enables users and organizations to control forwarding, copying, and printing of files in a way that persists no matter where protected files are sent internally or externally. Exchange 2010 includes features that make it easier to manage, apply, and work with IRM protection. To help ensure compliance with security policies, IRM protection can be applied automatically with transport rules based on keywords, recipients, or other criteria. (See Transport Protection Rules above.) With Outlook Protection Rules in Outlook 2010, IRM protection can be applied automatically at the client before delivery. Administrators can give users the option to disable Outlook Protection Rules if, for example, it is applied to non-sensitive messages. Protection can be applied to voicemail by policy or directly by a user to prevent forwarding. Exchange 2010 can also decrypt IRM-protected messages, enabling indexing and discovery as well as the application of transport rule policies, anti-virus/anti-spam filtering, and other critical system processes. For users, Exchange 2010 enables IRM-protected messages to be read and composed in Outlook Web App. For added convenience, protected files can also be viewed as WebReady documents* without having to install or start the associated application (such as Microsoft Office Word, Microsoft Office PowerPoint®, and Adobe Acrobat).

“With the combination of the Edge Transport server role in Exchange Server 2010 and Microsoft Forefront Protection for Exchange Server, bfu has seen a 90 percent reduction in the amount of spam messages

⁸ Requires AD RMS infrastructure available in Windows Server 2008 SP2 or higher. Exchange 2010 requires AD RMS SuperUsers permissions to decrypt IRM encrypted content.

*Requires Exchange Server 2010 Service Pack 1.

- **S/MIME Support** enables users to send digitally signed and encrypted email to one another from Outlook, Outlook Web App⁹ and a variety of devices. Signed messages allow the recipient to verify that the message came from the person that the message claims to be from. Encrypted messages allow the sender to ensure that only the intended recipients can read messages that are sent to them. While it's true that the message is unreadable to anyone who might intercept it while in transit, it is also true that even the Exchange administrator cannot read these messages. To help ensure policy compliance, transport rules can be created that identify S/MIME-signed and S/MIME-encrypted messages and apply an action (such as block, re-route, etc.) Note: unlike IRM-protected messages, S/MIME-encrypted messages cannot be searched through Exchange 2010. Also, S/MIME protection is not persistent; once a recipient opens an S/MIME-encrypted message, it can be forwarded to other recipients with the original protection removed.

that reach employee mailboxes.” - The Swiss Council for Accident Prevention

Anti-Spam Filtering is enabled in Exchange 2010 by a built-in, multi-layered anti-spam system. Filtering agents can be installed on the Edge and Transport server and include Connection, Sender/Recipient and Content filtering as well as anti-phishing capabilities. Administrators can customize each agent and also use real-time block lists. For premium protection, the Enterprise Client Access License includes Microsoft Forefront® Protection 2010 for Exchange as well as Forefront Online Protection 2010 for Exchange. Forefront provides continuous content filter and IP reputation updates.

Anti-Virus Support enables integration of leading antivirus solutions with the Edge, Transport, and Mailbox server roles. This includes the multi-engine malware protection in Forefront Protection 2010 for Exchange and Forefront Online Protection 2010 for Exchange.

Mobile Security using Exchange ActiveSync is supported by many of the security features noted above as well as over 50 management policies to better control mobile devices and data.¹⁰ For example, a minimum password length can be enforced on devices of users most likely to work with sensitive data. ActiveSync can be disabled per user. Certain types of devices can be restricted, such as those with inadequate encryption features. And with remote device wipe, policies can be set to delete all data from a mobile phone the next time it connects to the Exchange server. This can be useful when a mobile phone is lost, stolen, or otherwise compromised

Reporting

Exchange 2010 helps streamline compliance audits with better tracking of user activity and policy creation and deployment.

Administrator Audit Logging tracks every action taken by an Exchange 2010 administrator or delegated user with management privileges, such as a compliance officer. Audit logging can be used to track the

⁹ S/MIME requires that users sign in to Outlook Web App using Microsoft Internet Explorer 7 or Internet Explorer 8.

¹⁰ Applies to Exchange ActiveSync devices. Not all devices will support the same security policies.

*Requires Exchange Server 2010 Service Pack 1.

creation and application of retention policies, as well as mailbox journaling, multi-mailbox search, and transport journaling activity. Statistical reports enable managers and compliance officers to identify users that are not following email policies.

Mailbox Access Auditing lets you log successful user access to folders and messages either in their own mailbox or another user's mailbox. You can also track both folder and item-level activity, including changes, deletions and sent messages as well as when the actions occurred and who performed them.*

Delivery Reports provide users with detailed message reports including time and date of delivery, reasons for non-delivery, and policies applied to a message. Organizations can also select tracking which indicates whether a message was marked as read. Administrators can get even greater detail such as logs of every stage of a message's journey from originator to recipient across multiple servers. Delivery reports can be accessed easily online and are automatically indexed for quick retrieval.

Availability

High availability, disaster recovery, and backup capabilities support your compliance infrastructure and simplify management.

Mailbox Resiliency capabilities come built in to Exchange 2010, reducing the complexity of operating a highly available Exchange environment. The solution can be used to manage both on-site and off-site data replication and mailbox servers. Fast failover times (as little as 30 seconds) and the ability to switch between database copies when failures occur can dramatically improve an organization's uptime. Up to 16 replicated database copies can be deployed incrementally to meet the specific availability needs of your organization. These advances can reduce reliance on back-up tapes and lower related discovery costs. They can also make Redundant Array of Inexpensive Disks (RAID)-less disk configurations feasible for Exchange deployments - which has the potential to dramatically decrease storage costs.

*Requires Exchange Server 2010 Service Pack 1.

Addressing Compliance Challenges with Exchange 2010

In this section, we describe how the compliance features of Exchange 2010 can be used to support real-world compliance scenarios. We will use a fictitious company, Contoso, to outline the scenarios. But obviously, the capabilities and processes required to address these scenarios vary greatly by company size and geography. Also, auditor opinions might differ on the sufficiency of a specific control or feature within your organization. Use these scenarios as a baseline and work with your legal counsel and other managers to determine specific requirements.

Long Term Email Preservation

Contoso is required to store email items in an unaltered state for various time periods. For mailboxes with content that may need to be held indefinitely, Contoso's IT manager enables a Legal Hold policy. This ensures the preservation of all email items, including calendar items and tasks—as well as edited and deleted versions of these items. The company also has users with content that needs be preserved for a specific period of up to nine years. For these mailboxes, the IT manager enables a Single Item Recovery policy with the appropriate deleted item retention window. Once an edited or deleted item has reached the nine-year window, it is then automatically and permanently deleted from the system.¹¹ As the volume of email items grows over time, Contoso deploys a retention policy that automatically moves item to users' Personal Archives which it can store on a separate database. Contoso leverages the many storage enhancements in Exchange 2010, giving it the option of storing the Exchange mailbox and archive databases on cost-effective storage choices such as Serial Advanced Technology Attachment (SATA) hard disk drives and RAID-less configurations—without sacrificing system availability - to reduce both capital and operational costs.¹²

Supervision

Contoso is also required to monitor email for both internal HR policies and regulatory requirements. The company uses transport rules and journaling depending on the type of monitoring required. Transport rules have been configured to monitor messages for offensive keywords and phrases covered by HR policy. Messages that contain restricted content are copied to a mailbox or sent for review by a manager or other designated user. Journaling rules are also be used to maintain copies of messages for review and are configured per user. However, journaling has the advantage of including a journal report with each message which lists additional information such as BCC field or distribution list membership.

¹¹ With Single Item Recovery, items will also be deleted if the recoverable items folder reaches a specific quota. To ensure items are not deleted unintentionally, administrators can set specific storage quotas per mailbox and enable notification via an event log alert when the folder approaches that quota. The quota can then be adjusted accordingly.

¹² For more details, download the Exchange 2010 Large Mailbox Vision whitepaper at: <http://go.microsoft.com/?linkid=9727796>

*Requires Exchange Server 2010 Service Pack 1.

Contoso also uses journaling to send copies to Exchange Hosted Archive to conduct random sampling as required under NASD rules.¹³

E-Discovery

Contoso has just been informed that they will be facing legal action and needs to begin eDiscovery proceedings on several employees. The company's IT manager has already done things to streamline the process. First, and well before the e-Discovery request, the manager disabled PST files in Outlook and instructed users to drag and drop existing PST files into their Personal Archives. Second, the IT manager has assigned a management role to members of the legal department, enabling them to directly execute a variety of eDiscovery processes in Exchange without having to work through the IT department.

Using the Exchange Control Panel, the lawyer covering the eDiscovery process quickly places the mailboxes of the employees under investigation on Legal Hold. This ensures all items in both the primary mailbox and archive of each user are discoverable, including any items that are edited or deleted after the hold has been executed. He

then begins a multi-mailbox search starting with one or two keywords. A multi-mailbox search preview provides an estimate of the number of items that will be returned by this query. Due to the large number of estimated items, he adds more specific keywords and regular expressions to the query to return fewer items. A copy of these items will then be placed in a discovery mailbox. To further refine the results, the lawyer also selects the de-duplication option which will remove duplicate copies of items sent to the discovery mailbox (without affecting the original items). As the lawyer reviews the results, he finds some items that are relevant to the case and some that are privileged. He marks them respectively using the annotation feature, which associates a note to the message without actually changing the content.

Once the initial investigation is complete, results can be easily accessed by a third-party, specialized e-Discovery application through Exchange Web Services for further investigation and processing, saving the time and bandwidth required to actually export results as a PST folder. As the lawyer completes his e-Discovery process, he suspects that some email relevant to the case may have been deleted prior to the Legal Hold. However, this is allowed under e-Discovery legislation as long as these messages were expired through regular expiration policies. Fortunately, she can easily access administrative logging reports that help verify these policies for litigation purposes. In this way, Contoso can better manage email volume while remaining compliant to e-Discovery procedure.

Voicemail Retention

Contoso leverages Unified Messaging in Exchange 2010 so users can manage their voicemail in the same inbox as the rest of their email items. However, for compliance purposes, the company wants to apply a

"We used to spend one or two days looking for information we needed for legal requirements. Now, with multi-mailbox search in Exchange Server 2010, we can find what we need in an hour or less. That's a 90 percent improvement in discovery time for Binaria." - Julio Sandoval, Head of Middleware, Binaria

¹³ Exchange Hosted Archive includes both automated sampling as well as Supervisory Evidentiary Review reporting to document and monitor compliance. EHA is sold separately.

*Requires Exchange Server 2010 Service Pack 1.

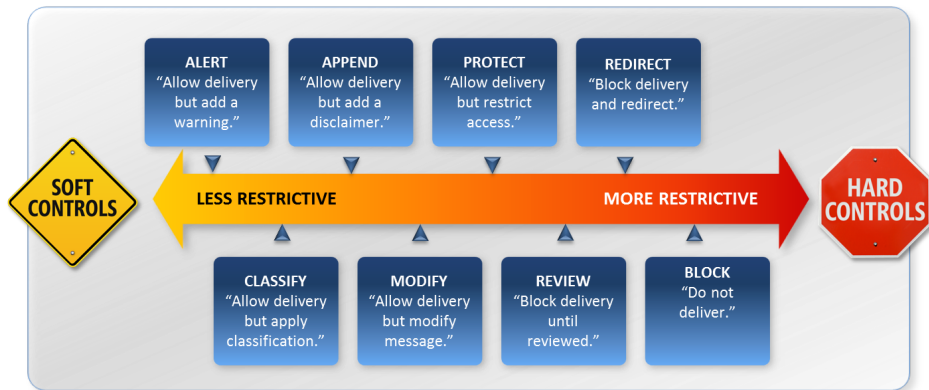
separate retention policy to all voicemail items. The company can achieve this in two ways: First, it can enable a separate managed content setting for voicemail (as well as other specific email items). For example, Contoso can create a 90-day default Inbox policy, with a 30-day default policy for voicemail. Contoso may also want to enable a different back-up policy for voicemail. In this case, it has the option of storing its voicemail in a separate Exchange environment altogether. This gives users two mailboxes, one for voicemail and one for all other email items. By synchronizing the two environments, users can access both mailboxes using the same password.

Data Loss Prevention (DLP)

It has not been a good month for Contoso. Along with legal battles, the company has also discovered that

several product announcements have leaked publically prior to official

disclosure. Their IT manager is immediately tasked with implementing a data loss prevention strategy. However, his team has been reluctant to deploy automated controls on email traffic, fearing false positives. With the wide range of control features in Exchange 2010, the team has been able to effectively address this issue. For example, they activated a MailTip which alerts users that they have included external recipients, either explicitly or within a distribution list. While this MailTip will be applied to all email, it does not actually restrict delivery. Its purpose is to remind users about potential data risks. For more sensitive messages, the IT manager creates transport rules that scan for specific data, such as the name of an unreleased product or serial number. These messages will either be IRM-protected or sent for review before delivery. For highly confidential information, such as unreleased product names and features, separate rules are created to block, redirect or modify the message.



Administrators can automatically apply a wide range of protection and control policies, depending on the sensitivity of the data in the email.

Privacy and Protection

Contoso is subject to privacy regulations, which requires protection of personal data both inside and outside the network. In particular, Contoso is concerned with data it shares with partners. It needs to protect the confidentiality of that regulated data while still allowing the partner to index it for search purposes. For this scenario, Contoso uses the new IRM support features in Exchange 2010. The rule searches messages (including Microsoft Office attachments) for keywords and regular expressions requiring protection such as patient ID numbers. If an email is generated with sensitive content, IRM protection is applied automatically through Active Directory Rights Management Services. To enable partners to access this protected mail in Outlook Web App, Contoso creates a trust between its RMS server and the partner's Exchange 2010 server.¹⁴ In this way, the partner's Exchange 2010 server can also decrypt the message to enable indexing and search as well as journaling (where a decrypted copy is

¹⁴ The Microsoft Federated Gateway (MFG) is used to federate the sending organization's RMS server and the partner's Exchange 2010 server. Software required for RMS federation to MFG is available with Windows Server 2008 R2 SP1.

*Requires Exchange Server 2010 Service Pack 1.

included with the original message.) The message is then re-encrypted and delivered to recipient, who can access based on the permissions specified by the sender.

Summary

Establishing email compliance is a key requirement for companies of all sizes across industries and geographies.

Exchange 2010 offers new, built-in features designed to help reduce the cost and complexity of regulatory and internal compliance. These features address the core elements common across compliance scenarios including preservation, discovery, control and protection of email. Equally important are the advanced availability and monitoring capabilities that help ensure the integrity of your compliance processes.

“By using the native archiving, retention, and compliance features in Exchange Server 2010, we can save several hours each week for the administrator who used to manage this process.” - Peter Caspersen, Systems Analyst, EDC

Together, these features can help address a wide range of compliance scenarios, from local regulatory requirements to internal governance. An extensible architecture and broad partner network help ensure that you have the tools and resources necessary to meet specific compliance requirements.

Additionally, these features can be applied easily to your entire messaging infrastructure, including non-regulated data. In this way, the compliance features in Exchange 2010 can help:

- Reduce the risk of sensitive data being lost or leaked outside the organization.
- Make it easier to search and access email data for research, review, and other business purposes.
- Monitor email to better address HR policies and other internal mandates.
- Increase user productivity by automating compliance processes.
- Reduce storage costs and increase performance through archiving.

And because Exchange 2010 leverages a familiar messaging infrastructure, you can reduce the burden of compliance for users and administrators alike.

For more information, visit microsoft.com/exchange.

document.

MICROSOFT MAKES NO WARRANTIES, EXPRESS, IMPLIED OR STATUTORY, AS TO THE INFORMATION IN THIS DOCUMENT

*Requires Exchange Server 2010 Service Pack 1.