

Make better decisions, faster

March 2008



IBM Information Management software

**Integrated email archiving:
streamlining compliance and
discovery through content and
business process management**

Table of Contents

Executive summary. 2

Rising importance of email brings compliance, litigation and security risks 3

Challenges of email archiving 3

Core of effective email archiving: Extract, archive and retrieve . . . 4

Email archiving strategies: Point solutions evolve into ECM solutions 4

Integrated risk and records management: Streamlines compliance and discovery 5

Help ensure compliance and increase productivity 5

Reduce time, effort and expense of discovery 7

Improve employee efficiency and agency agility 7

IBM offers a comprehensive portfolio for integrated email archiving . . 8

Executive summary

Without a doubt, email has become a key communication tool for organizations worldwide. It is how we conduct business today. This rapid rise in email usage and the growing importance of email content has created unique archiving and management challenges for government organizations.

Like mailed correspondence or internal memos, email can be classified as official government communication and considered a public record that must be saved. For government IT and compliance departments, this means that email must be archived, accessible when needed and retained for future use to ensure legal compliance as well as to comply with security measures and government transparency requirements—measures that hold officials accountable for their actions and allow citizens open access to the activities of their government. Under these transparency measures, citizens can request copies of emails along with other records, and governments are obligated to produce them in a timely fashion.

Requests for legal discovery related to email messages are also increasing, particularly in light of recent scandals involving email, such as the National Security Archive lawsuit filed against the White House to recover more than five million missing emails allegedly deleted between 2003 and 2005. If organizations cannot produce email records sought by an investigator, they face potential fines and other legal repercussions.

The enormous volume of email and the mandate to retain and enable access to email content make it imperative for government agencies to implement an effective email archiving, discovery and compliance solution—one that can not only archive content, but also integrate records management with risk management. The ability to simply access email content is not sufficient. Archiving, united with retention policies, enables email content to be managed as a record and easily incorporated into government processes. Repeatable business processes that include email content can help organizations meet compliance mandates through automated retention practices, help reduce legal costs associated with discovery searches and improve employee productivity—all leading to agency agility.

Rising importance of email brings compliance, litigation and security risks

Most users take the benefits of email for granted: instant communication and collaboration, immediate access to critical information and the ability to mobilize people and resources rapidly. It is no wonder that email is quickly becoming the primary method of communication for conducting business. Analysts estimate that some 131 billion emails are sent daily, growing at nearly 50 percent compound annual growth rate to reach an expected 276 billion emails in 2009.¹

For government agencies, that growth is quickly evident in the integral role email plays in the decision-making process. Day-to-day interdepartmental interactions, informal discussions and employee communications can all occur via email rather than lengthy phone calls or in-person visits. Externally, email plays a key role in business relationships as public and private agencies and vendors negotiate contracts and provide services to government. Perhaps most importantly, email provides a new avenue of communication between government agencies and constituents. Because of its immediacy, email is well-suited to fielding complaints, official inquiries and general requests for information from the citizens served. However, processes and policies need to be applied to these communications to help ensure equitable treatment of constituents.

Challenges of email archiving

Freedom of Information legislation at both the national and regional levels requires public access to regulatory authorities' meetings, decisions and records. However, the increasing reliance on email to conduct everyday business often presents an overwhelming volume of messages that must be managed and stored—many including large file attachments that strain the design limitations of systems never intended to act as vast storehouses or support selective retrieval. To satisfy records management and risk management needs, today's governments need to archive email so that it can be easily accessed and available for use—on demand.

Because email data is unstructured, it is difficult to capture and discover the precise information needed to satisfy records requests or legal discovery. Over the last three years, the amount of unstructured email data fed into data warehouse and business intelligence processes grew by 47 percent.² This influx of unstructured data compromises the integrity of such processes by overwhelming systems and workers with its sheer volume, preventing agencies from taking advantage of the information contained within email as an asset.

For records management processes, an inability to quickly fulfill information requests can result in lost staff productivity. The burden of proof typically falls on the agency being asked for information. Consequently, in addition to their primary area of responsibility, many government agencies are now responsible for fulfilling public records requests and doing so in a timely manner—a daunting task for employees forced to wade through unwieldy backups to find the appropriate email correspondence. As much as 30 percent of employee time can be spent trying to find the right documents and information to fulfill requests for information. These costly, lengthy and difficult searches are not only inefficient, but they also distract staff from serving constituents and prevent government processes from moving forward in a timely manner. At one state agency, such a

request was reported to require two employees working full-time for nearly six weeks—a costly and inefficient process that kept those employees from performing their typical day-to-day activities.

Email has become a highly sought-after target for compliance regulators and opposing litigators, which introduces additional pressure for agencies to better manage their approach to email archiving. In compliance and legal evidence, time is of the essence—and errors cannot be tolerated. According to Gartner analysts, the cost for one email discovery could be as much as US\$150,000 to US\$250,000, and the typical cost per lawsuit can range from US\$1.2 million to US\$1.4 million.³ Time is often critical: Many discovery orders often need to be completed in as few as 72 hours. And keeping too many or too few emails—for too short or too long a time—can create huge liabilities.

Additional risk may appear in the form of user-created local email folders outside the purview of the IT systems responsible for maintaining compliance. Email stored in this manner cannot be put on “hold” during a pending audit or lawsuit and IT cannot manage its life cycle or delete it as appropriate. IT may need to scour countless backup tapes or search every user’s private archive to find relevant email—an extremely invasive, costly and error-prone process.

Core of effective email archiving: Extract, archive and retrieve

Extracting sent and received emails along with associated attachments from a messaging system is the first step toward effective and efficient record management and discovery. The most complete record possible will include captured metadata such as date, from, to, cc, bcc and subject, as well as keywords and phrases within the body of the email or attachment.

Once extracted, email and attachments should be offloaded to a robust and scalable content repository to help ensure that all archived email remains easily accessible. The integration of email archiving and content management helps agencies consistently apply a single set of records management policies to all content.

With archived emails residing in a central repository, recovering email to fulfill record requests or legal discovery becomes a simple matter of executing a search against the repository. Searches can be performed against any standard email metadata. Advanced capabilities such as Boolean logic, fuzzy search and wildcards provide significant flexibility and control over the search process.

Email archiving strategies: Point solutions evolve into ECM solutions

Email archiving strategies are developing along two parallel paths—email archive point solutions and more comprehensive Enterprise Content Management (ECM)–based solutions. Both strategies have certain capabilities in common: the ability to archive email and various other types of content, support for legal discovery and the ability to perform email supervision for compliance purposes.

Point solutions—typically deployed by agencies as a quick answer to rapidly increasing storage demands placed on email systems—offer simple archiving and retention capabilities. Although these point solutions are relatively easy to deploy and maintain, they can create a repository silo of data.

Many organizations that have deployed email archive point solutions now seek to develop a more inclusive content management strategy. This integrated content archiving moves beyond email to include instant messages, spreadsheets and other types of organizational content in a single repository. By uniting information previously locked in information silos, agencies can achieve greater organizational insight and empower people to make higher quality, better informed and faster decisions by having instant access to the right information at the right time.

ECM-based solutions are designed to use a single infrastructure to manage all types of electronic content, making them the natural platform for integrated content archiving. Since ECM-based solutions feature full record management capabilities, email and other archived content can be fully integrated into an organization's processes. For example, an email sent to a customer service mailbox begins a customer service workflow process. An ECM-based archiving solution allows email to be linked to that process, ensuring that the case file or line of business system contains a full record of relevant communication about the job. By integrating this record management capability with risk management processes, ECM-based solutions manage archived data with automated retention, hold and destruction policies based on complex context rules.

Integrated risk and records management: Streamlines compliance and discovery

Once an email is archived as a record, the record can also be managed and integrated with risk management policies. By incorporating email into the structured business processes, government agencies now have the capability to better meet compliance requirements, reduce legal discovery costs, improve employee productivity and increase organizational agility.

Help ensure compliance and increase productivity

In concert with records management capabilities, an integrated email archiving solution can help government organizations meet compliance requirements with centralized and certified records management and content management.

With the capability to declare and classify email and attachments as official records, a single set of records management policies can be consistently applied across all record types. These types of policies enable agencies to better monitor, manage, retain and dispose of email records to meet compliance requirements. By archiving email as records—consistent with documents, spreadsheets, presentations, forms data, invoices, statements and other media types—agencies can use uniform retention practices across the organization to help reduce the risk of non-compliance. Figure 1 shows the importance of retention policies for email.

Email Retention Options

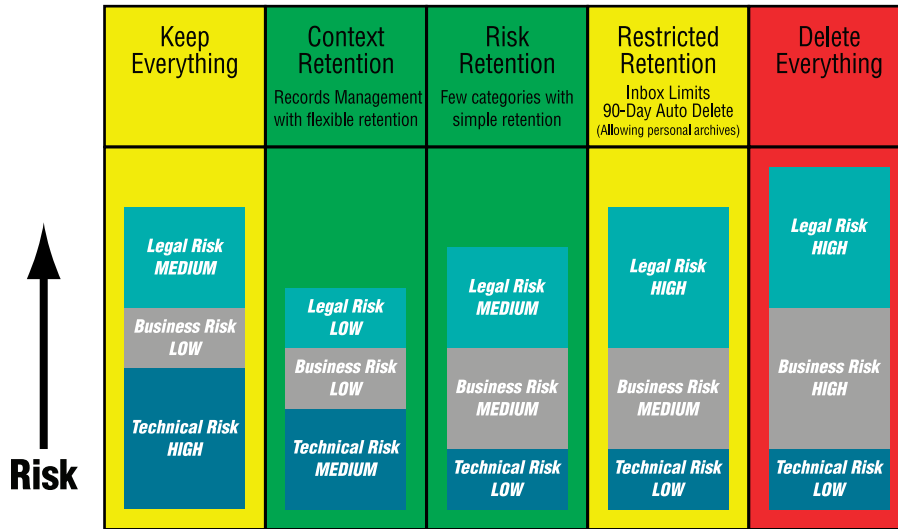


Figure 1: Risk associated with email retention policies

This integrated approach to email archiving helps government agencies control email records from creation to destruction. Administrators can prevent records from being edited or deleted, and actions such as viewing and printing are logged for audit and reporting purposes.

Further enhancing security, emails are captured at the appropriate point to preserve the original form and ensure authenticity. The central repository can reduce the perceived need by individuals to retain private email archives on their computers, while security and access controls protect information integrity and user privacy.

The integrated approach to content archiving can also help to significantly reduce the impact of compliance measures on employee productivity. With an automatic process for defining and classifying records, end users do not need to learn new applications or make complex decisions about what constitutes a record and which retention rules to apply. This approach also enables users to perform only one search across a centralized repository instead of many individual silos, helping organizations reduce the cost and effort required to respond to record requests and regulatory audits.

Reduce time, effort and expense of discovery

Beyond easing compliance efforts, integrated content archiving helps agencies respond faster when required to produce email records for a regulatory audit or a lawsuit—with less effort and cost, and with increased accuracy.

Staff can quickly extract knowledge and data buried in email using a thorough index of email content that facilitates the relevancy and precision of discovery searches. Flexible, advanced search queries can be performed across single or multiple mailboxes to identify all email messages that may pertain to a case—without IT loading and searching email backup tapes. Search results can be saved, refined and exported to make relevant data easily reviewable by third parties.

An integrated email archiving solution also enables government agencies to preserve and provide access to the information found in email records pertinent to a specific discovery. By placing email on hold, messages are exempt from the typical archiving or deletion schedule. These locked-down records are verified as authentic to satisfy regulatory and legal requirements.

The application of classification and retention protocols that are repeatable allows discovery costs and timelines to become more predictable. Automatic classification can help save time and increase productivity. With better information, staff can negotiate the discovery process quickly, allowing more time for legal reviews and preparation while lowering the costs associated with lengthy discovery searches.

Improve employee efficiency and agency agility

By integrating the email archiving solution with a content management system based on open standards, government organizations can accelerate and automate business processes. Email involved in day-to-day activities can be incorporated into automated departmental workflow processes and associated with case management systems, the lifeblood of government agencies. With the required background and attachments in hand as the job is assigned, staff productivity increases and manual errors inherent in passing paper files around an office are eliminated. Interdepartmental knowledge captured in emails is retained in an easily searchable fashion as well, enhancing the training process and reducing the impact of lost skills as employees retire or leave the organization.

Perhaps most importantly, an integrated email archiving solution transforms unstructured email content into a highly valuable information resource. The metadata generated from email records can be incorporated into analytics systems to identify trends, expose risks and analyze long-term data, increasing an agency's ability to adapt.



IBM offers a comprehensive portfolio for integrated email archiving

Because agencies at the local, state and federal levels are in different phases of adopting email archiving processes, IBM offers a flexible and integrated solution that helps government agencies address their challenges in record management and regulatory compliance, lowering legal discovery costs and becoming more agile as an agency.

The IBM email archiving, discovery and compliance portfolio includes multiple solutions—from traditional point solutions for mailbox management to ECM-based solutions that act as a platform for integrated content archiving. IBM email archiving solutions help reduce the risk of noncompliance by moving email from the most common messaging systems, including Microsoft® Exchange, Novell GroupWise and IBM® Lotus Notes® and Domino® environments, to a secure, central repository—all based on the automated retention policies right for your organization. And no matter how large your email archive becomes, IBM search and discovery solutions are designed to conduct accurate, fast and flexible searches and legal holds, helping to reduce the time and costs related to record inquiries and legal discovery. These solutions support full-text indexing and search on attributes, message body and attachments and can use more than 600 IBM and non-IBM storage devices for unparalleled flexibility.

By integrating these capabilities with record management solutions from IBM, your organization can leverage critical information across diverse applications and repeatable business processes to increase agility and better serve your constituents.

For more information

For more information about the IBM email archiving, discovery and compliance portfolio, contact your IBM representative or visit ibm.com/software/ecm

© Copyright IBM Corporation 2008

IBM Corporation
3565 Harbor Boulevard
Costa Mesa, CA 92626-1420
USA

Printed in the USA

03-08

All Rights Reserved.

IBM, the IBM logo, Domino and Lotus Notes are trademarks or registered trademarks of International Business Machines Corporation in the United States, other countries or both.

Microsoft is a trademark of Microsoft Corporation in the United States, other countries or both.

Other company, product and service names may be trademarks or service marks of others.

References in this publication to IBM products or services do not imply that IBM intends to make them available in all countries in which IBM operates. All statements regarding IBM's future direction and intent are subject to change or withdrawal without notice, and represent goals and objectives only.

For more information, visit
ibm.com/software/data/ecm.

[1] The Radicati Group, Inc. "Market Numbers Quarterly Update." April 2005.

[2] Stephen Swoyer. "Unstructured Data: Attacking a Myth," TDWI Research. September 2007.

[3] Gartner. Need source from IMD11858-USEN-00.