GBS

Legally compliant email management

- Strategies for processing, storing, securing, and integrating email with your most critical business applications and processes -

Expertise matters

Contents

1 Executive Summary

There is no debate that email is crucial to your business. And, every aspect of your business depends on a secure, efficient and responsive email system.

While network administrators can safeguard your email system from spam and viruses, additional email issues demand executive attention. First, a host of regulations such as the Sarbanes-Oxley Act require an audit trail of all email business records – with significant penalties for non-compliance. Secondly, you must proactively protect the confidentiality of vital business information. Thirdly, to maintain a competitive edge you need to drive efficiency into every level of your business. Email's wealth of intellectual and competitive capital is a significant corporate asset that can no longer be ignored.

Faced with these challenges, many businesses are implementing an email management strategy, which enables the safe and efficient integration of email into company-specific business processes. With email management, you can control and integrate email in the same manner in which other applications and processes are handled such as financial records, ERP and CRM systems, and manufacturing specifications.

Email management consists of integrated strategies and methods for processing, storing, and managing email, from creation to retention to disposal -- all in accordance with business processes and government regulations. The bonus, however, is email management's ability to improve your critical business processes, such as linking emails to appropriate corporate databases.

Email management must, however, be executed within a framework of bullet-proof email security and stringent hygiene. Therefore, your email management strategy must address the full range of current and emerging email threats. A solution that focuses on controlling just spam or viruses cannot deliver on the promise of email management. A point solution that simply archives will fall short as well. In fact, trying to coordinate multiple point solutions to achieve legally compliant email management will add expense and complexity that may negate benefits.

The email management mandate is clear. Businesses can no longer afford to transmit emails from mailbox to mailbox without rules and policies that support businesses processes. Businesses need integrated, multi-purpose email solutions that can be incrementally and easily implemented with an eye to the bottom line. With email management, your company can begin to tap the wealth of knowledge that is locked away, deal with the complexity of emerging statutes, knock out spam and viruses, and protect vital information. The result is a secure, organized and compliant email system that can be integrated with other business processes to drive decisions, limit risk and create a competitive edge.

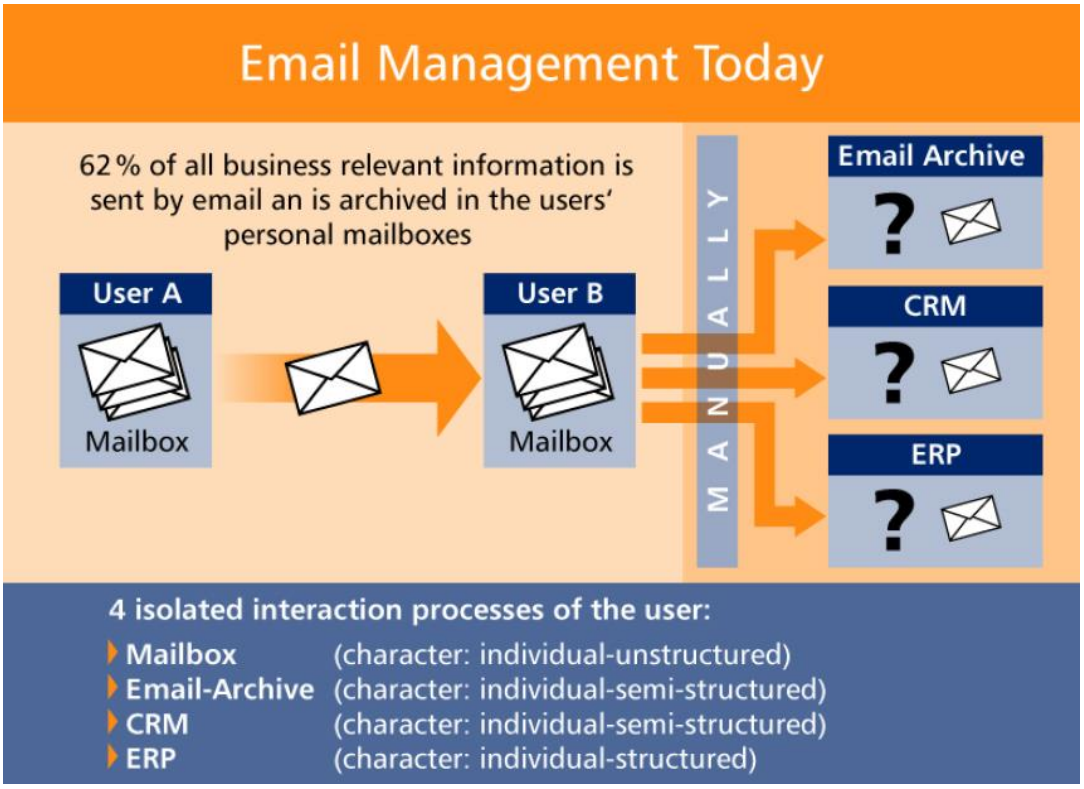

Illustration 1: Email management will eradicate the widely-used method of manual mailbox-to-mailbox email transmissions that do not support business processes.

2 Email - Your Most Important Business Application

Email is used in every level of business and personal interaction, enabling a flow of information that is the life blood of business. It may be the most important, universally used business application.

Safe, efficient and well-managed email requires a combination of good corporate policy and technology that can address a wide range of issues. If your company is focused on protecting your communication capability one threat at a time and meeting new regulations one rule at a time you are almost certainly adding expense and complexity to your IT environment. Individual point solutions have a place, but they may obscure the chance to take advantage of the underlying business value contained in email as it passes through your business processes.

Financial records have well-defined controls for accounting and compliance, which ensure accuracy, provide audit trails, and prevent unauthorized or untimely disclosure. Engineering and manufacturing information is part and parcel of your competitive advantage and protecting this advantage is routine document management policy. Managing email as an asset to protect its integrity, control costs, and extract maximum business value has moved to the same level of importance as other critical business applications. Recognizing the value of this information asset many corporations are adopting email management to control email in the same way they handle other important business assets.

3 Email management – Integrates Email into Business Processes

Successful email management demands an assortment of tools, policies, budgets, foresight and commitment. As email impacts every facet of your business, its management requires senior-executive support that drives long-term strategic planning and corporate policy. Email management is an integrated and holistic method, based on your specific business and government rules, for capturing, classifying, processing, storing, and retrieving email. The result is comprehensive control coupled with the email hygiene necessary for a secure and available system. The recommended email management approach provides a solid base for every element of mission-critical email including attachments, graphics and groupware discussions.

Email management is driven by the simple fact that email is so embedded in the fabric of your business that failing to manage it may place your company at risk. Email management is not just a defensive move to block spam or avoid government fines. And, it is much more than an Information Lifecycle Management system that optimizes data storage.

By integrating email into your business processes email management provides benefits that relate directly to cost savings, better organization and higher productivity in a dynamic business environment. Consider this: Content filtering and classification techniques are used to exam email for spam or viruses. Using these same capabilities on legitimate emails can generate important business benefits, such as:

- Linking similar information that may be under discussion in several departments to help identify trends and emerging markets.
- Filtering data from incoming email can speed delivery to your CRM and ERP applications to minimize human interaction, speed reaction times, and reduce errors.
- Using rule-based content recognition to prevent premature or inadvertent dissemination of sensitive internal information.

The goal is a secure, organized and compliant email application that can be integrated with other business processes to improve decision making, limit risk, and drive a competitive edge. An integrated email management solution offers significant advantages over point solutions and can be purchased and installed incrementally without interoperability problems. Let's look at how your company can meet the challenges of complex emerging regulations, block spam and viruses, protect vital information, and improve business processes – all at the same time.

Illustration 2: The email management is a continuum of email processes that advance business objectives.

The email lifecycle is a business continuum defined by seven closely-linked email processes:

- Pre-processing
- Firewall
- Content classification
- Compliance
- Archiving
- Retrieval
- Retention

Each phase has a number of important functions or components that work together to guarantee that businesses can process, store and retrieve an email throughout its entire life.

Each process is driven by company-, departmental-, group-, or user-specific policies and rules. Managing email at each phase of the cycle balances the need for tight security with the organizational requirements of your company and provides the internal control necessary to comply with today's regulations.

Typical email flow through the lifecycle management process.

1. **Pre-processing** ensures that incoming emails are decrypted and unpacked before filtering. Outgoing emails can be encrypted, packed, and signed, and with a disclaimer, depending on your organization's specific needs. These safeguards are implemented automatically freeing senders from tedious and frequently overlooked steps.

   Initial pre-processing delivers improved email organization and efficiency resulting in more uniform corporate standards and reduced liability. Parameter-driven electronic signatures and legal disclaimers improve the email consistency as well as the consistency of encryption standards to protect confidential information.

2. **Firewall** phase detects spam, viruses and other undesirable content based on pre-defined criteria. Viruses contained in emails and file attachments are identified and quarantined using manipulation-proof file pattern information. Ideally, a Firewall should permit the parallel use of up to 12 anti-virus engines. Spam is quickly identified and new spam techniques are recognized and acted on without intervention using a sophisticated content recognition capability.

   Detailed logging of all processing provides a continuous view into the health of your email system. Legitimate business communication can now move to the next phase quickly and securely.

   Delivering legitimate email, devoid of spam, will help improve employee productivity and efficiency, protect your corporate brand, and increase customer satisfaction.

3. **Content classification** of email plays a decisive role in improving business processes. The content of incoming mail is analyzed, classified into categories, and forwarded to appropriate recipients. Automatic routing can dispatch email sent to a general email address such as support@company.com or directly to the department or person responsible for the product mentioned in the request. Content classification can also generate consistent keywords and context-based indexes for efficient archiving.

   Automated routing offers big improvements in organization and efficiency for both individuals and departments. For example, processing customer requests quickly based on content or classification can significantly improve response times and translate to much higher customer satisfaction.

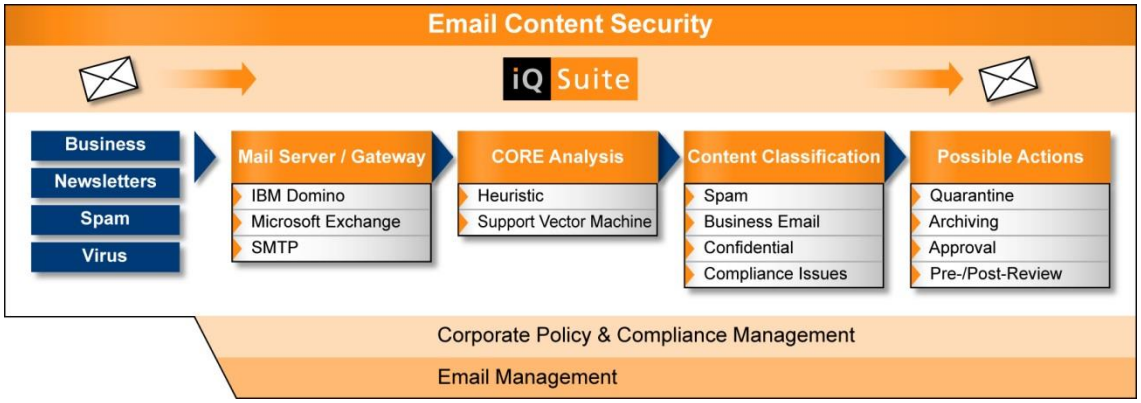

Illustration 3: Tightly-integrated security, classification, and routing tools are vital elements in successful email management.

4. **Compliance** ensures that email conforms to legal as well as company requirements. The content recognition capability is used to identify email that may violate company policies. For example, if your rules prohibit the dissemination of information such as a balance sheet or employee phone lists an email containing those items is placed into “Park” mode pending review. Even content such as “earnings per share” can be parked to be sure disclosure will not harm the company during quiet periods.

   From the Can-SPAM Act to the Sarbanes-Oxley Act to HIPAA and SEC rulings – businesses are faced with a flood of compliance issues. While they have distinct purposes and serve distinct constituencies, all these regulations have a common email thread: preserve email business records in an unaltered state, and have the ability to retrieve them on demand.

   Email management provides tools and techniques that prepare organizations for SOX readiness. For example, emails with content on pricing or discounts are identified and securely archived in a database before it they be altered – preserving both content and context. Once protected, the mail can be routed to the intended recipient, the compliance team, or a database related to the appropriate subject for further analysis. To limit both workload and risk, content recognition is used to select business-only email for transfer to a regulation-specific compliance system.

Internal controls also imply that email is protected from outside access to prevent tampering or disclosure. The systematic encryption of email can deny access to potential espionage and go a long way toward providing the control and the audit trail that must be certified.

Active risk management guarantees that your email communication is in compliance with all applicable laws, and using early-warning techniques to avoid possible violations can save costly discovery efforts. To meet audit requirements, the uniform application of rules and policies enhanced by technology must drive email communications. Adding content classification to speed management review and analysis will improve efficiency.

5. **Archiving** business-only email can be implemented as an entry-level solution or in conjunction with a third-party archiving system to fully comply with regulations. Rules and policies control the flow of email into the archives and determine its classification. Email is archived before it is delivered to maintain the original content and context together with index information from the email classification.

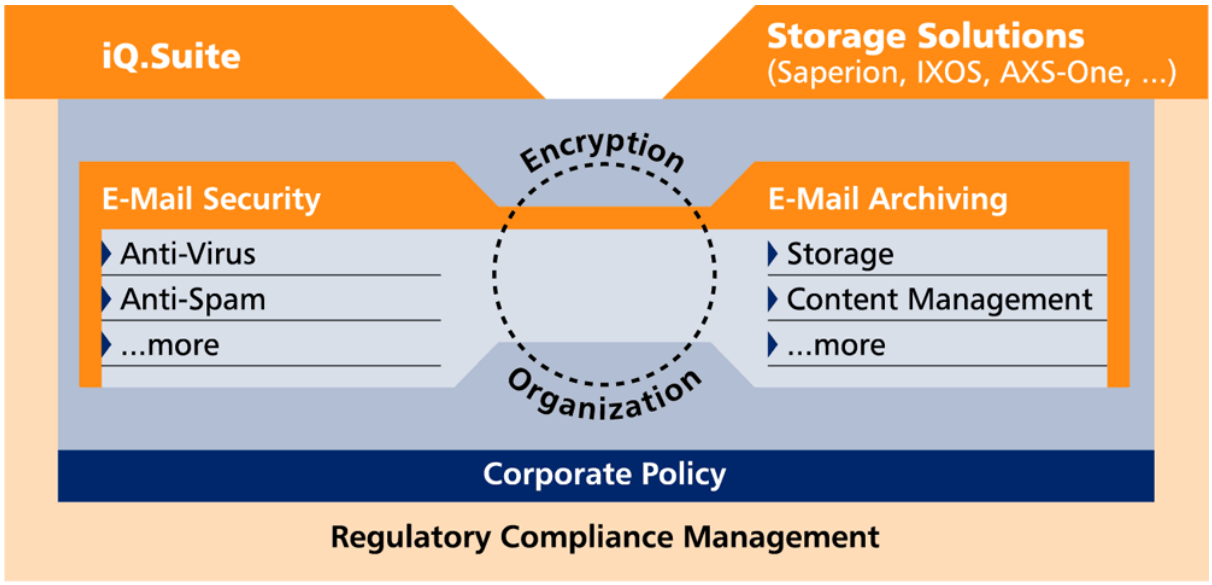

Illustration 4: Email archiving is no longer a 'nice to have' and a range of email retention, retrieval, and disposal requirements are addressed by email management.

6. Retrieval of email is part of the archiving process. Users can search for archived emails based upon index criteria, and email can be restored at a later date.

7. Retention capabilities, part of the retrieval process, are required for long-term email storage on third-party storage systems. Email held in long-term storage systems can be automatically deleted as appropriate.

   The risk of personal judgments and severe fines levied against the company make it imperative that you have an audit-proof archiving capability. Efficient content filtering provides the ability to prevent infractions by archiving all the required communication while eliminating the rest. Automatic and efficient archiving of email and internal email on groupware servers preserves business correspondence and records enabling you to quickly respond to regulatory demands.

4 Email Management Drives Better Business

Email management provides an organized and comprehensive set of capabilities to manage your most critical application. Compliance with internal and external policies and statutes is no longer optional and requires a proactive approach to succeed. The need to block spam, disable viruses and stem the burgeoning tide of email volume will be ongoing. Email management provides the platform and tools required to meet Email Lifecycle challenges while helping you control costs, build in solid controls, and optimize business processes.

Administrative overhead and the difficulties of integrating various solutions are minimized by considering the entire email environment from an integrated point of view. Messages are handled once instead of passing from system to system. Common protocol and reports add efficiency and simplicity to administration. Understanding the volume, flow and type of email traffic helps control the costs associated with providing storage, capacity and compliance. Employee abuse of the corporate email resource is quickly highlighted and cost center analysis provides real-time cost and budget data for future planning.

Legal compliance is assured by the reliable and uniform application of rules, content management and archiving capability. Organizations are protected against severe judgments and the need for cost-intensive discovery projects using active risk management in a secure environment.

Many business issues are driving the need for a secure and organized email resource tailored to your specific needs. By adopting a holistic approach to your email system you can begin to reap the email management benefits – a secure, organized, compliant and intelligent email solution that can be integrated with other business processes to enhance decision making, limit risk, and create a competitive edge.

5 Next-generation Email Management

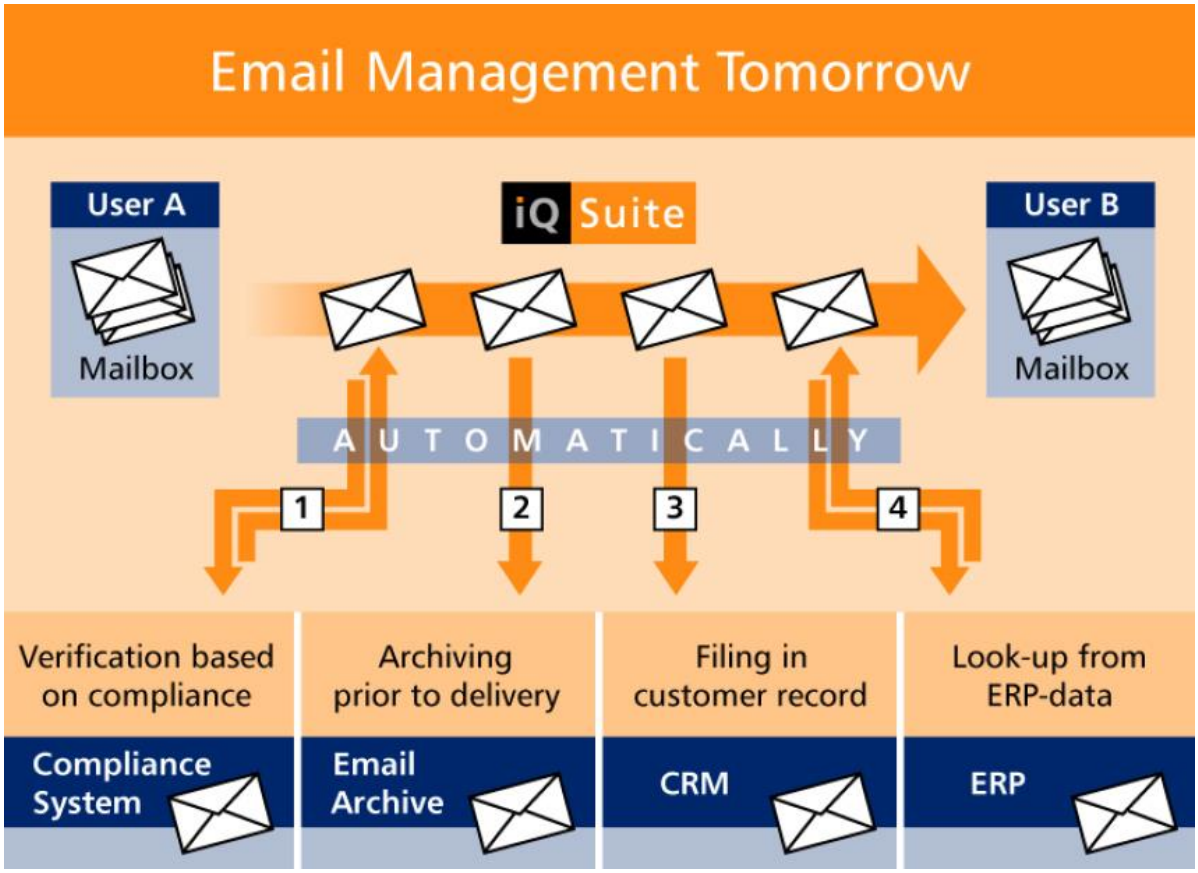

Illustration 5: Next-generation email lifecycle management requires sophisticated mailbox-to-mailbox content filtering and classification techniques.

Email management is next-generation email processing that is quickly gaining traction with forward-thinking companies. GBS Software, a worldwide pioneer in email management, has focused on developing a comprehensive set of email management and content security solutions since its inception in 1992. Delivering the industry's first antivirus product to the complete email lifecycle management suite available today, GBS Software consistently provides the stability and scalability necessary to handle massive volumes of email coupled with the expertise to innovate. Companies all over the world rely on GBS Software to provide the modular tools and controls that help manage, monitor and protect intellectual assets and ensure compliance with the wide range of emerging regulations.

GROUP's email management solution is delivered in the company's flagship product -- iQ.Suite. Developed specifically for email security, organization and management, iQ.Suite is comprised of applications that can be used standalone as point solutions or integrated for a comprehensive email management solution. Designed for IBM Domino, Microsoft Exchange, and SMTP platforms, iQ.Suite can be seamlessly integrated into an IT strategy for optimum, scalability, stability, and functionality.

About GBS

GROUP Business Software is a leading vendor of solutions and services in the fields of messaging security and workflow for the IBM and Microsoft collaboration platforms. Over 5,000 customers and more than 4 million users worldwide trust in GBS expertise. The company operates in Europe, North America and Asia.

Further information at www.gbs.com