



E-mail Lifecycle Management

**Strategies for Processing, Storing, Securing,
and Integrating E-mail with Your Most Critical
Business Applications and Processes**



Contents

1 Executive Summary – The ELM Mandate **2**

2 E-mail - Your Most Important Business Application..... **3**

3 ELM – Integrates E-mail into Business Processes **4**

4 ELM Drives Better Business **8**

5 ELM – Next-generation E-mail Management **9**

6 About GROUP Technologies AG **11**

1 Executive Summary – The ELM Mandate

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

While network administrators can safeguard your e-mail system from spam and viruses, additional e-mail issues demand executive attention. First, a host of regulations such as the Sarbanes-Oxley Act require an audit trail of all e-mail 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. E-mail's wealth of intellectual and competitive capital is a significant corporate asset that can no longer be ignored.

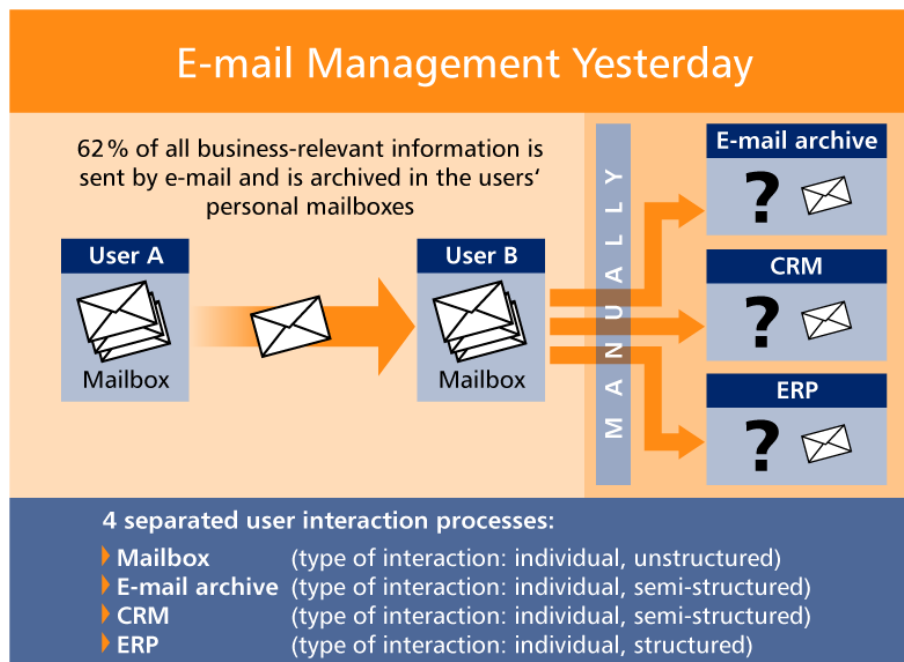
Faced with these challenges, many businesses are implementing an e-mail lifecycle management (ELM) strategy, which enables the safe and efficient integration of e-mail into company-specific business processes. With ELM, you can control and integrate e-mail in the same manner in which other applications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

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

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

The ELM mandate is clear. Businesses can no longer afford to transmit e-mails from mailbox to mailbox without rules and policies that support businesses processes. Businesses need integrated, multi-purpose e-mail solutions that can be incrementally and easily implemented with an eye to the bottom line. With ELM, 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 e-mail system that can be integrated with other business processes to drive decisions, limit risk and create a competitive edge.

Figure 1. ELM will eradicate the widely-used method of manual mailbox-to-mailbox e-mail transmissions that do not support business processes.



2 E-mail - Your Most Important Business Application

E-mail 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 e-mail 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 e-mail 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 e-mail 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 e-mail lifecycle management (ELM) to control e-mail in the same way they handle other important business assets.

3 ELM – Integrates E-mail into Business Processes

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

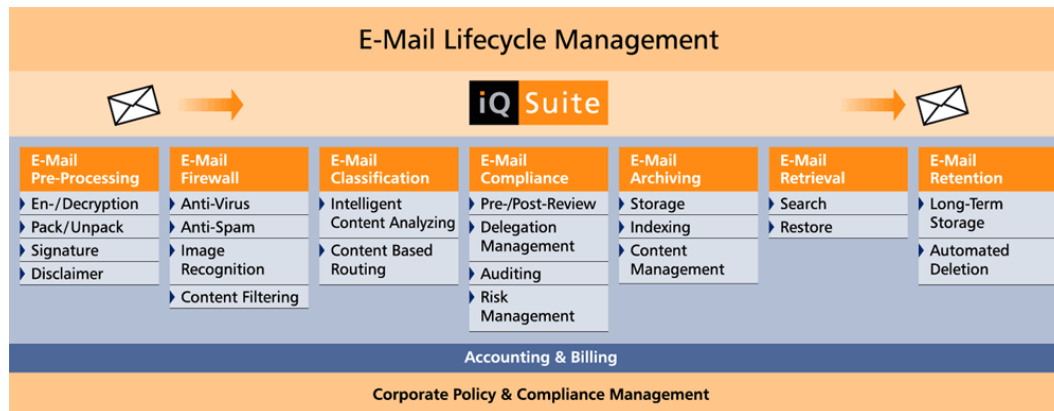
ELM is driven by the simple fact that e-mail is so embedded in the fabric of your business that failing to manage it may place your company at risk. ELM is not just a defensive move to block spam or avoid government fines. And, it is much more than an Information Lifecycle Management system that optimizes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

By integrating e-mail into your business processes ELM 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 e-mail 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 e-mail 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 e-mail application that can be integrated with other business processes to improve decision making, limit risk, and drive a competitive edge. An integrated ELM 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.

Figure 2. The e-mail lifecycle management is a continuum of e-mail processes that advance business objectives.



The e-mail lifecycle is a business continuum defined by seven closely-linked e-mail 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 e-mail throughout its entire life.

Each process is driven by company-, departmental-, group-, or user-specific policies and rules. Managing e-mail 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 e-mail flow through the lifecycle management process.

1. **Pre-processing** ensures that incoming e-mails are decrypted and unpacked before filtering. Outgoing e-mails 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 e-mail organization and efficiency resulting in more uniform corporate standards and reduced liability. Parameter-driven electronic sig-*

natures and legal disclaimers improve the e-mail consistency as well as the consistency of encryption standards to protect confidential information.

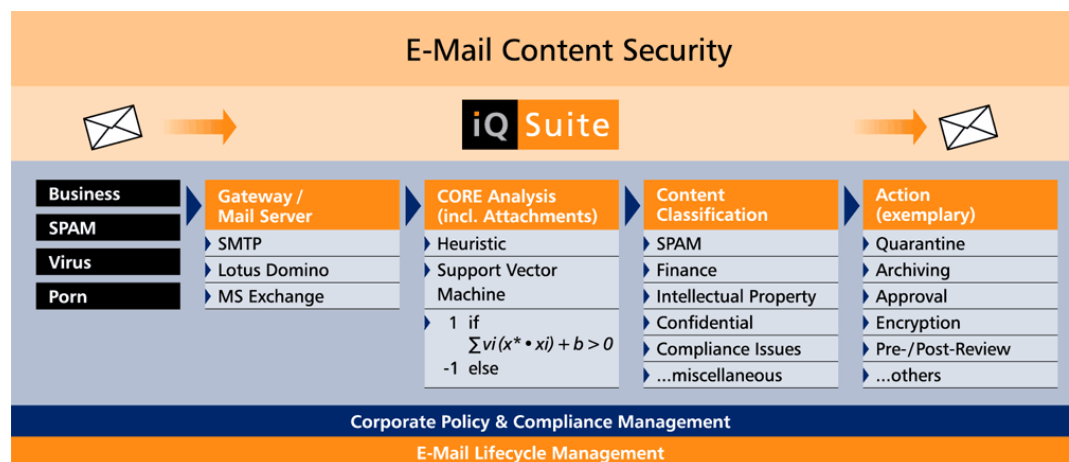
2. **Firewall** phase detects spam, viruses and other undesirable content based on pre-defined criteria. Viruses contained in e-mails and file attachments are identified and quarantined using manipulation-proof file pattern information. Ideally, a Firewall should permit the parallel use of up to 12 anti-virus 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 e-mail system. Legitimate business communication can now move to the next phase quickly and securely.

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

3. **Content Classification** of e-mail 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 e-mail sent to a general e-mail 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.

Figure 3. Tightly-integrated security, classification, and routing tools are vital elements in successful ELM.



4. **Compliance** ensures that e-mail conforms to legal as well as company requirements. The content recognition capability is used to identify e-mail 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 e-mail 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 e-mail thread: preserve e-mail business records in an unaltered state, and have the ability to retrieve them on demand.

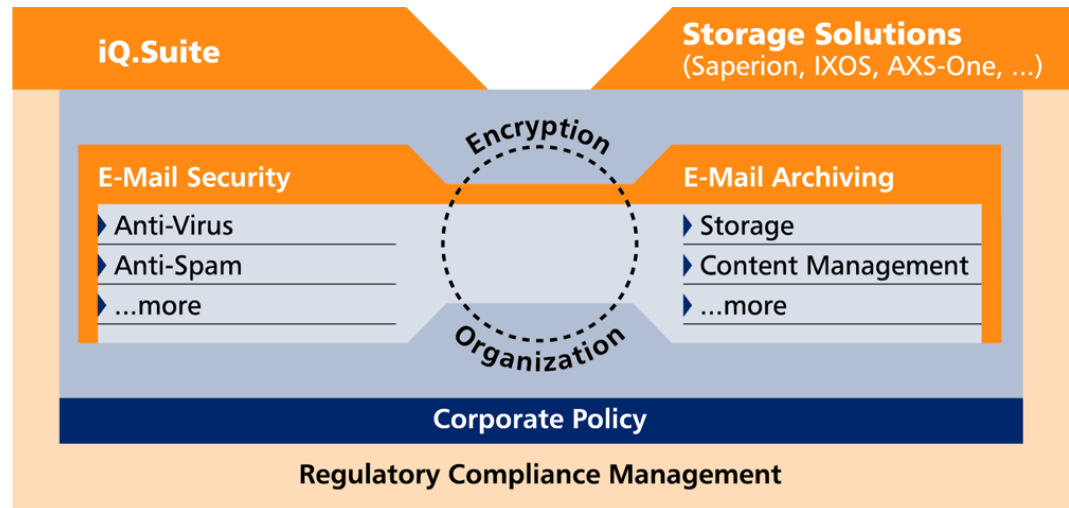
ELM provides tools and techniques that prepare organizations for SOX readiness. For example, e-mails with content on pricing or discounts are identified and securely archived in a database before they be altered – preserving both content and context. Once protected, the mail can be routed to the intended 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 e-mail for transfer to a regulation-specific compliance system.

Internal controls also imply that e-mail is protected from outside access to prevent tampering or disclosure. The systematic encryption of e-mail 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 e-mail 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 e-mail communications. Adding content classification to speed management review and analysis will improve efficiency.

5. **Archiving** business-only e-mail 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 e-mail into the archives and determine its classification. E-mail is archived before it is delivered to maintain the original content and context together with index information from the e-mail classification.

Figure 4. E-mail archiving is no longer a 'nice to have' and a range of e-mail retention, retrieval, and disposal requirements are addressed by ELM.



6. **Retrieval** of e-mail is part of the archiving process. Users can search for archived e-mails based upon index criteria, and e-mail can be restored at a later date.
7. **Retention** capabilities, part of the retrieval process, are required for long-term e-mail storage on third-party storage systems. E-mail 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 e-mail and internal e-mail on groupware servers preserves business correspondence and records enabling you to quickly respond to regulatory demands.

4 ELM Drives Better Business

ELM 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 e-mail volume will be ongoing. ELM provides the platform and tools required to meet E-mail 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 e-mail environment from an integrated point of view. Messages are handled once

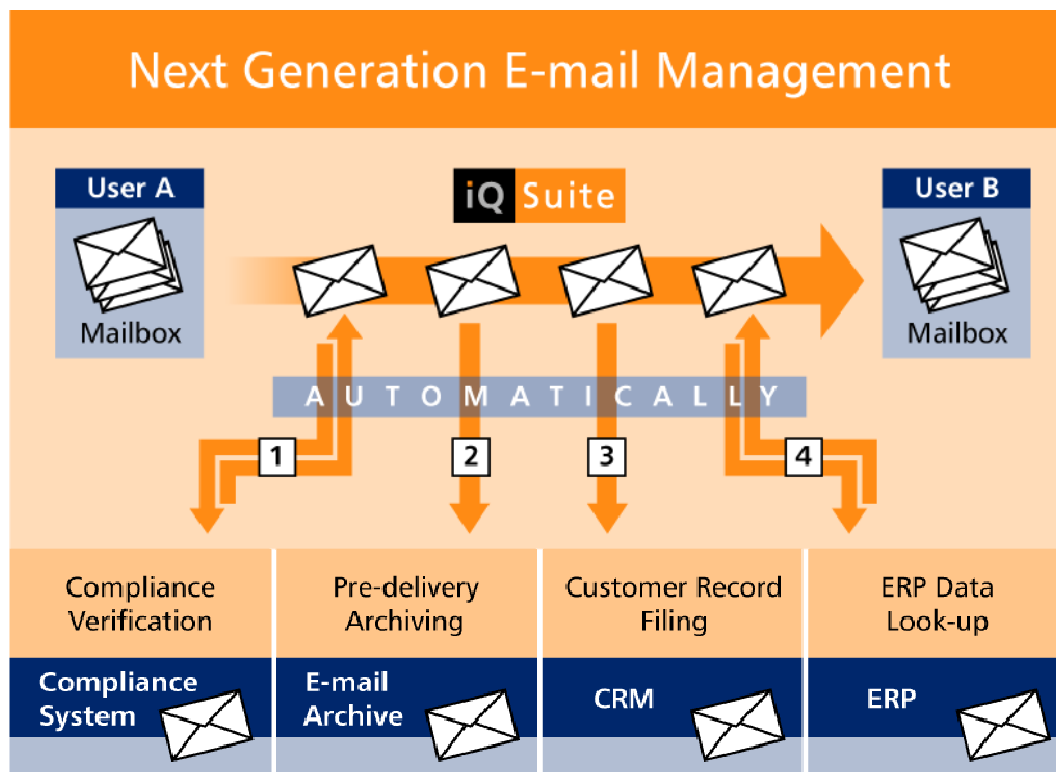
instead of passing from system to system. Common protocol and reports add efficiency and simplicity to administration. Understanding the volume, flow and type of e-mail traffic helps control the costs associated with providing storage, capacity and compliance. Employee abuse of the corporate e-mail resource 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 e-mail resource tailored to your specific needs. By adopting a holistic approach to your e-mail system you can begin to reap the ELM benefits – a secure, organized, compliant and intelligent e-mail solution that can be integrated with other business processes to enhance decision making, limit risk, and create a competitive edge.

5 ELM – Next-generation E-mail Management

Figure 5. Next-generation e-mail lifecycle management requires sophisticated mailbox-to-mailbox content filtering and classification techniques.



ELM is next-generation e-mail management that is quickly gaining traction with forward-thinking companies. GROUP Technologies, a worldwide pioneer in ELM, has focused on developing a comprehensive set of e-mail management and content security solutions since its inception in 1992. Delivering the industry's first antivirus product to the complete e-mail lifecycle management suite available today, GROUP Technologies consistently provides the stability and scalability necessary to handle massive volumes of e-mail coupled with the expertise to innovate. Companies all over the world rely on GROUP Technologies 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 ELM solution is delivered in the company's flagship product -- iQ.Suite. Developed specifically for e-mail security, organization and management, iQ.Suite is comprised of applications that can be used standalone as point solutions or integrated for a comprehensive ELM solution. Designed for Lotus Domino, Microsoft Exchange, and SMTP platforms, iQ.Suite can be seamlessly integrated into an IT strategy for optimum, scalability, stability, and functionality.

6 About GROUP Technologies AG

GROUP Technologies AG is a world leader in E-mail Lifecycle Management. The company's fully integrated iQ.Suite products ensure efficient security and effective organization of e-mail, from encryption, virus protection, and spam filters to e-mail classification and secure archiving.

The iQ.Suite is modular, fully scalable, and offers a high degree of investment security. The modules are completely server-based, can be centrally administered at a low cost, and are available for Lotus Domino, Microsoft Exchange and SMTP platforms.

With the iQ.Suite, companies can reduce costs, optimize the performance of their e-mail environment, and increase productivity. GROUP's clients include many well-known companies such as Deutsche Bank, Ernst & Young, Honda, Heineken, and Miele. More than six million users and 2,000 companies worldwide protect and organize their systems with GROUP Technologies products.

GROUP Technologies AG is headquartered in Karlsruhe. It maintains a subsidiary in the USA, and distributes its products internationally, both directly and through partner companies.

www.group-technologies.com

For more information, call toll-free in the US and Canada: 877-GROUP-55;
e mail: info.us@group-technologies.com;

GROUP Technologies | 321 Fortune Boulevard | Milford, MA 01757, USA |

Phone: +1 508-473-3332

© 2005 GROUP Technologies AG

The product descriptions are general and descriptive in nature. They can be interpreted neither as a promise of specific properties nor as a declaration of guarantee or warranty. The specifications and design of our products can be changed at any times without prior notice, especially to keep pace with technical developments.

The information contained in this documentation deals with issues as assessed by GROUP Technologies AG at the time of publication. As GROUP Technologies AG is bound to react to changing market requirements, this document by no means represents an obligation by GROUP Technologies AG and GROUP cannot guarantee the correctness of the information presented in this document after its publication.

This documentation is intended for information purposes only. GROUP Technologies AG hereby excludes any warranty, express or implied, for this document. GROUP Technologies AG is unable to guarantee, either explicitly or tacitly, the quality, execution, standardization or suitability for a specific purpose.

All product or company names in this document may be protected brand names of their respective owners.

Headquarters

GROUP Technologies AG

Ottostrasse 4

76227 Karlsruhe / Germany

Phone +49(0)721-4901-0

Fax +49(0)721-4901-199

info.de@group-technologies.com

www.group-technologies.com



North American Headquarters

GROUP Technologies

321 Fortune Blvd.

Milford, MA 01757/USA

Phone +1 508-473-3332

Phone 877-476-8755 (US and Canada)

Fax +1 508-473-9940

info.us@group-technologies.com

www.group-technologies.com