

# E-mail Compliance and Management

E-mail is one of the most rapidly growing sources of business content and has become a central business tool. While some organizations have recognized the increasing need to take seriously their responsibility to manage electronic communication technologies, it is clear that risk management issues and compliance failures persist, in large part due to a gap between the implementation of new technologies and organizations' management of them.

Traditionally, e-mail content resided on either an e-mail server or a user's desktop. This approach provides a number of challenges when organizations attempt to manage and protect the value of e-mail content. According to the Cohasset ARMA AIIM 2005 Electronic Records Management Survey, processes that were once acceptable for records management in the past are now inadequate due to the ever growing presence of electronic records and the associated challenges of technology and volume. Specifically, some of the issues include the adoption of electronic mail and other communications technologies which create new types of records, the complexity of electronic records and the business processes producing them, and the growth of records resulting from the ease with which electronic records can be created, distributed, and stored. With this expansion in the type, complexity and volume of business records, there is a need to refocus the processes by which electronic records are managed and archived.

There are a number of business drivers for archiving e-mail:

1. **Regulatory Compliance**

One of the most important, and perhaps the most familiar driver, is regulatory compliance. Federal and industry regulators understand the role e-mail plays in corporate life today. Consequently, almost every new regulation mandates that e-mail messages are to be saved for a certain amount of years and they must be quickly and easily retrieved when needed or when requested by regulators. The Sarbanes-Oxley Act requires organizations save every record that informs its audit process, e-mails included, for seven years. The Securities and Exchange Commission Rule 17a-4, which covers brokerages, is another example. The Health Insurance Portability and Accountability Act and Medicare both require health-care companies to save e-mails.

2. **Litigation**

A risk factor that is possibly a bigger driver of e-mail management is the threat of litigation. In recent years, due to the ever-increasing volume of litigation and the need for regulatory compliance, electronic records have assumed even greater value. Always important in determining the outcome of disputes, records have become pivotal in determining the destiny of organizations as well as the fate of business. Every company faces the possibility of litigation in the course of doing business. Increasingly, the litigators' first step in the discovery process is to request vast amounts of e-mail thus increasing the defendant's costs and increasing their willingness to settle. While the costs of discovery may be high, inability to produce e-mail or documents could produce disastrous results.



### 3. **Productivity**

Productivity is another issue driving the need for e-mail archiving. More and more the tendency of end users is to retain a significant amount of their e-mail. They believe that retaining all or most of their e-mail will add to their productivity. In point of fact, productivity decreases as e-mail accounts grow and mail servers are bogged down with the increased load. Additionally, the e-mail servers were designed to deliver communications not to serve as archival storage systems. E-mail systems are simply not the easiest or fastest way to retrieve archived e-mails. A system designed for archiving provides more cost effective storage, faster retrieval, better systems management, higher levels of security, which ultimately contribute to higher productivity

What to look for in an e-mail archiving solution:

#### 1. **Ease of Use**

Make e-mail archival as easy as possible. Users and administrators should be able to manually archive their e-mail in three seconds or less. The most elegant and technically advanced solution ever built will be ineffective if it is difficult to use.

#### 2. **Seamless integration**

A seamless integration between the e-mail application and the e-mail archival system is critical. Users must have the ability to store e-mails and their attachments directly into archival system from within their e-mail application. Users and administrators must be able to click one button and store e-mails quickly and easily.

#### 3. **Native File Format**

E-mails are must be stored in their original electronic, searchable format and must include attachments. Once the e-mail is stored it must be quickly and easily retrieved. This insures instant access to the information needed for discovery, litigation support and ongoing compliance. Each email and attachment should be "stamped" as authentic in its original format to assure bulletproof content authenticity for non-repudiation, auditing, or compliance.

#### 4. **Audit Functionality**

The archival solution must provide audit functionality so that all documents, including e-mails can be audited for any action taken by any user.

#### 5. **Storage**

Storage requirements will vary and are dependant on types of e-mails and documents archived as well as the retention schedules required. Therefore, it is critical that the archival system offers a scalable storage architecture. Additionally, the storage sub-system must provide RAID 5 (Redundant Array of Independent Disks). RAID 5 delivers a high level of fault tolerance to protect the archived documents and e-mails.

#### 6. **Data Backup**

Having a mechanism for the backup of the database and all files, including e-mails, is critically important. Two-tier storage (RAID paired with DVD-RAM) provides significant protection against lost data and documents and easily creates back-up disks for offsite archival storage.

#### 7. **Disaster Recovery**

The ability to rebuild the database from archived files in the event of a database failure is vital. In the event of database failure and loss, system data and digital documents can quickly be recovered using DVD RAM backup disks produced by the two tier storage architecture.



**8. Inbox management services - Alert Processing**

Having a mechanism whereby e-mails containing critical content are detected to insure proper notification within the enterprise management and legal ranks is another important factor when securing an e-mail archiving solution.

For more information on e-mail compliance or to see how PiF Technologies fulfills these requirements, please call 888-934-4443.

