

## COMPLIANCE INSIGHT: SARBANES-OXLEY ACT OF 2002

The Sarbanes-Oxley Act of 2002 was passed in an effort to bring about dramatic changes to corporate governance and oversight. There are many different dimensions to the act ranging from the role of directors to the internal controls companies must have in place. The consistent theme is around oversight and accountability to stockholders in a post-Enron world.

### THE ROLE OF MESSAGING

Sarbanes-Oxley compliance is a combination of processes and technology that will come together to ensure appropriate controls and oversight. In fact, AMR Research reports that Fortune 1000 companies have earmarked more than \$2.5 billion this year for investigation and initial compliance work.

Beyond financial and reporting systems, there is a pressing need to examine messaging systems as a potential source of risk and non-compliance. Often overlooked, e-mail is core to every major business process regardless of industry or company size. Everyday millions of e-mails are sent and received containing spreadsheets, documents, and text of business-related correspondence or even proprietary company information. Having no system in place to monitor and control messaging represents a gaping hole in Sarbanes-Oxley compliance.

### SARBANES-OXLEY & MESSAGING

The Sarbanes-Oxley Act of 2002 covers many topics and stipulates many regulations. Those below are important to understand when examining messaging and Sarbanes-Oxley compliance.

#### Section 302: Corporate Responsibility for Financial Reports

This is the requirement for both the CEO and CFO to “certify” financial statements and periodic reports based on their confidence that there are no untrue statements and that appropriate internal controls are in place.

Without the knowledge and understanding of what is taking place in the corporate e-mail system, it will be very difficult for these officers to have the confidence required for certification.

#### Section 303: Improper Influence on Conduct of Audits

This section prevents directors and officers from influencing, coercing, manipulating, or misleading accountants during the performance of an audit.

Providing a clear audit trail and record of all e-mail correspondence between directors/officers and independent auditors is an essential part of Sarbanes-Oxley compliance. This not only protects the company but provides proper oversight and visibility to the communications between auditors and directors/officers.

#### Section 401(a): Disclosures in Periodic Reports; Disclosures Required

There are many areas of disclosure covered in this section, but the one most pertinent to messaging concerns pro forma figures. Pro forma financial information provided in any public disclosure or press release must not be misleading and it must reconcile with the financial conditions and results of operations of the company.

Pro forma financial information can be communicated via e-mail or the attachments to an e-mail. Proper control and monitoring over the communication of pro forma financial information via the corporate e-mail system is a necessity.

#### Section 404: Management Assessment of Internal Controls

Each annual report must contain an “internal control report” that states the responsibility of management for establishing and maintaining appropriate controls and an assessment of the effectiveness of the internal control structure. Further, the auditor will attest to and report on the assessment made by management.

This statement to shareholders and the follow-on evaluation by the auditor requires a comprehensive program of internal control of which proper monitoring over corporate messaging systems is a crucial component.

#### Section 409: Real Time Issuer Disclosures

This section requires companies to disclose to the public on a “rapid and current basis” any information concerning material changes in financial condition or operations. This “real-time” view of anything that exposes operational or financial reporting anomalies as they occur is important for overall Sarbanes-Oxley compliance.

Combining both policies to control what occurs in messaging activity and real-time visibility to breaches or suspicious activities as they occur ensures companies will comply with rapid disclosure of information.

#### Section 501: Treatment of Securities Analysts by Registered Securities Associations

This conflict of interest rule applies to equity research professionals and their relationship with investment banking personnel. It requires “appropriate informational partitions” between research and investment banking such as an electronic information boundary controlling e-mail communications between the two groups.

The leading brokerage firms paid a record setting \$1.4 billion fine for conflict of interest activities between their research and investment banking departments. The “smoking gun” in many cases was e-mail correspondence. Implementing policies to control the communications between these two groups will ensure compliance with this section of Sarbanes-Oxley.

#### Section 802: Criminal Penalties for Altering Documents

This section mandates the “Accuracy of Records” and requires that all audit work papers be retained for a period of seven years. This applies to all audits or reviews completed after October 31, 2003.

Having a system in place to accurately separate and categorize e-mail correspondence related to audit and review activities is an essential components of a Sarbanes-Oxley compliance initiative and critical to Section 802 compliance.

#### Section 806: Protection for Employees of Publicly Traded Companies Who Provide Evidence of Fraud

This “Whistleblower” section is designed to prevent retaliation against employees who disclose fraudulent activities.

A company can provide complete anonymity by identifying messages sent to an ‘anonymous’ address & ensuring removal of sender identity as well as providing an alert to compliance/legal of the action.

## CONCLUSION

Every Sarbanes-Oxley compliance program must address messaging as a source of risk and potential non-compliance. Oversight and proper internal controls can be successfully achieved by deploying a policy-based system that provides operational visibility through reports and real-time interfaces.

