Sarbanes Oxley Act (SOX)
Cirius white paper

Introduction

The Sarbanes-Oxley Act, better known as SOX, was introduced in 2002 to bring greater accountability and transparency to the financial operations of public corporations. Namely, its provisions attempt to keep companies from cooking the books by demanding companies establish *internal controls* to accurately gather, process, and report financial information. With technology playing a crucial role in organizations' financial operations, the call to implement internal controls unavoidably extends to information systems used by finance, to assure the integrity of data within those systems. Email security becomes a crucial part of ensuring data integrity against loss, corruption or unauthorized disclosure.

In any business, email is a vital tool for communication and collaboration: A marketer emails promotions to customers, a sales rep emails sales orders to an accountant, an accountant emails accounting reports to a controller, and a CFO emails a financial report to investors. Email communication has become an important means of circulating financial information, yet it also remains vulnerable and exploitable. Email's many vulnerabilities—malware, phishing attacks, unauthorized access--create the risk of unauthorized disclosure, corruption, or loss of financial information, thereby thwarting SOX's goal of accurate financial reporting. Email communication policy becomes a crucial part of SOX's *internal controls* to safeguard information from unauthorized use, disclosure, corruption or loss.

This paper briefly details SOX's effect on email security and provides a framework for how organizations can best comply with SOX requirements by developing effective policy and implementing flexible email security solutions.

cirius

secure corporate messaging

Who is affected by SOX?

Sarbanes-Oxley currently applies to all US public companies, their global subsidiaries and any foreign company whose shares are traded on the US stock exchange. The act makes the chief executives and chief financial officers of companies personally responsible for the information that is included in their financial accounts and systems of internal financial control.

Why should my organization comply with SOX?

To ensure that companies meet rules, SOX places harsh penalties on organizations and individuals who manipulate and falsify financial reports as well as for gross negligence regarding financial compliance requirements. Violators face up to 20 years in prison and or $5 million in fines for failing to keep financial operations and reporting compliant. Additionally, the SEC can distribute civil damages to investors who were harmed by corporations as well as censure brokers, dealers and investment advisors involved in potential noncompliance. There is no doubt that ensuing criminal and civil litigation, punitive fines, and reputation damage of non-compliance will directly affect your company's bottom line.

What does SOX require for email compliance?

While SOX does not explicitly mention requirements for email security, two provisions: 302 and 404 include requirements directly relevant to email security and compliance policy. Section 302 mandates that organizations establish, maintain and regularly evaluate the effectiveness of *internal controls* placed within systems that support financial operations. Similarly, section 404 tasks company management to provide evidence that verifies the effectiveness internal controls in an annual report submitted to the SEC for consideration.

These broad provisions don't explicitly identify framework for how organizations should structure and evaluate these necessary *internal controls* for IT, much less email security. For guidance, the Information Systems Audit and Control Association has provided a widely-accepted framework that translates SOX requirements into more explicit control objectives. This framework for compliance, better known as the Control Objectives for Information and Related Technology (COBIT), in effect requires companies to implement policies and email solutions that:

1. Identify and protect financial information against unauthorized access, transmission or disclosure.
2. Authenticate individual message senders and intended recipients.
3. Secure the transmission of email communications containing financial information.
4. Secure message indexing, archiving, and retention.
5. Have the ability to audit and retrieve messages as needed by auditors and compliance officers.
6. Protect email servers and other systems that that store or process emails containing financial information.
7. Track and log of message traffic.

These are the main control objectives that affect email compliance. A full list of IT control objectives for SOX compliance can be found at the Web site of ISACA.

How Can My Organization Meet These Requirements?
Meeting control objectives for SOX compliance is twofold: developing effective policy and implementing email security technologies that enforce compliance policy.

Policy:
There's no out-of-the-box policy that works for every organization. An effective policy will be tailored to your company—the processes of reporting and circulating financial information, existing policies for acceptable email use should be considered. However, there are a few steps every organization can and should take to develop a policy for SOX compliance:

1. Identify where relevant financial information is within your company, how it is being circulated via email, and who can and should have access to email financial information. This will enable email solutions to later encrypt, archive, or even block transmission of email content based on users, user groups, keywords and other lexicons that identify your data as sensitive.
2. Identify what email messages need to be archived and backed up and how to do so in a way that facilitates compliance auditing and eDiscovery in the event of legal proceedings.
3. Implement technology solutions such as encryption, data leak prevention and archiving that can enforce compliance policy and provide necessary protections against unauthorized disclosure, corruption or loss of financial data.

4. Educate users on acceptable use policies for email. When users understand proper workplace email usage and the consequences of non-compliance, they will be less likely to let their guard down and make mistakes.

Email Technologies:
Implemented with a well-controlled policy, the following [technology] solutions can mitigate the risk of corruption, leakage, and loss of financial data through the email gateway as well as help address SOX technical security safeguard standards for adequate *internal controls*.

- **End-to-end encryption:** To meet regulation requirements that mandate messages containing relevant confidential data be secured, end-to-end encryption is often necessary to ensure that data remains confidential and secure between the message sender and the intended recipient, preventing unauthorized access or loss.
- **Data Leak Prevention (DLP):** A DLP solution for email is essential for SOX compliance, providing enhanced mail security through content filtering, authentication, and permissions rules that limit access and transmission of sensitive information sent within and outside the organization.
- **Archiving:** An effective email archiving system will enable organizations to meet control objectives for message retention and auditing by capturing, preserving and ensuring that ALL messages are available for eDiscovery and auditing purposes.

When encrypted and backed-up, archiving provides additional protections for information against loss and unauthorized exposure. It is important to ensure that all encrypted messages can archived decrypted complete with all metadata to ensure message authenticity.

Don’t sacrifice functionality for compliance

While it is important to implement an email solution that conforms to the control objectives laid out by COBIT, often technologies created to ensure regulatory compliance inhibit email functionality and workflow, frustrating users. According to a 2011 study by the Ponemon Institute, over half of email encryption users were frustrated with their encryption solutions being inflexible and difficult to use. Email security should complement existing solutions rather than complicate them. So when considering a solution for secure email, it’s important that it conforms to SOX requirements without compromising the functionality and workflow of existing email that your business depends on. This means implementing a solution that allows easy and scalable deployment, simplifies management complexity, and works with your existing email infrastructure to enable user-productivity and email functionality.

Cirius is a cloud solution for email encryption, secure file transfer and DLP that helps address GLBA technical security safeguard standards, and lets you use your email just the way it is.

Cirius:

- Simplifies the complexity of secure communication and collaboration, preserving workflow by integrating seamlessly with any email platform including MS Outlook, MS Office 365, Gmail and Zimbra (for both sender and recipients regardless of their network configuration).
- Conforms to SOX technical requirements for secure transmission of NPI.
- Safeguards confidential emails and files from unauthorized disclosure or loss through powerful DLP tracking features and permissions tools; additionally allowing recall of messages and attachments even if the content has already been read.
- Automates and securely delivers messages and file attachments decrypted to any email archive database or third party application through a secure API.
- Enables anytime, anywhere secure communication and collaboration by allowing users to send, track and receive secure email and attachments on any mobile device including iPhone, iPad, Android, BlackBerry and Windows Phone.

Cirius offers financial services providers the most flexible solution to help address SOX technical security safeguard standards for email and file transfer.

About Cirius

The makers of Cirius believe that email security should complement your email, not complicate it. Our cloud-based solutions for secure file transfer and email encryption work seamlessly with any email to enable secure communication and collaboration anytime, anywhere.