GlobalCerts™

MARKET OVERVIEW:

The Sarbanes-Oxley Act of 2002

Section 302: Corporate Responsibility for Financial Reports.
"...the signing officers (a) are responsible for establishing and maintaining internal controls ..... (b) have evaluated the effectiveness of the issuer's internal controls ...."

The Sarbanes-Oxley Act of 2002 ["the Act"] was established by Congress to restore investor confidence in the U.S. securities market, which had been damaged by business scandals and lapses in corporate governance. The Act and supporting regulations have rewritten the rules for accountability, disclosure and reporting. Good corporate governance and ethical business practices are no longer optional.

The Act deems corporate executives responsible for establishing, evaluating and monitoring the effectiveness of internal controls over financial reporting.

While there are many sections within the Sarbanes-Oxley Act, this paper focuses on sections 302 and 404, which address internal controls over financial reporting.

The reality of the Sarbanes-Oxley Act is that each public company needs to develop an individualized approach to reporting and compliance. Fortunately, the Information Systems Audit & Control Association (ISACA) founded in 1969 and the IT Governance Institute (ITGI) which was established in 1998 can help companies to comply with the Act. Major internal controls recommendations are directed mainly at the following:

1. **confidentiality** of the information transmitted
2. **non-repudiation** of the information and transactions
3. **authentication** of the users
4. **security policies and standards utilized by 3rd party (i.e. external audit)**

Section 404: Management Assessment of Internal Controls.

"...each annual report .....[must] contain an internal control report, which shall (a) state the responsibility of management for establishing and maintaining an adequate internal control structure and procedures ..... (b) contain an assessment of the effectiveness of the internal control structure and procedures....."

Email communication is increasingly affecting the way companies gather, manage and communicate financial information. Email is used to communicate financial information between dispersed corporate executives, outside auditors, lawyers and the Board of Directors. It is also used to communicate financial information with customers, as well as with a mobile sales force. Personal information including insurance applications, salary history, social security numbers, etc. is routinely communicated over the Internet to insurance companies, government organizations, law firms, recruiters, and other third parties. All of this information needs to be protected as well.

Most companies already required to comply with HIPAA, GLBA or EU privacy laws use secure email. Now that email is a part of the corporate infrastructure that, per sections 302 and 404 of the Sarbanes-Oxley Act of 2002, needs to be further controlled.

The GlobalCerts™ SecureMail Gateway™ can be used to help close a number of common gaps identified on the path to Sarbanes-Oxley sections 302 and 404 compliance. The SecureMail Gateway transparently adds "end-to-end" security to email applications like Microsoft Exchange, Novell Groupwise, Lotus Notes, and many others making it possible to mitigate risk and help comply with sections 302 and 404. It enables email messages to be encrypted and digitally signed ensuring confidentiality, privacy, integrity and improved non-repudiation. This ability to secure email messages can help organizations better control access to sensitive financial information.

Email has typically been sent “in-the-clear,” meaning that email headers, contents and attachments have been readily accessible to anyone with the ability to monitor network traffic. Traditionally, encryption has been sufficiently difficult to implement that many businesses chose to sacrifice security for ease of use. Now, however, new government regulations such as the Sarbanes-Oxley Act are putting even more pressure on IT managers to ensure that all records, including communications such as email, are secure and safe.

GlobalCerts meets the requirements of Sarbanes-Oxley sections 302 and 404 by:

- Automatically encrypting and decrypting email messages before they are transmitted across the Internet
- Ensuring privacy – ensures the message is sent encrypted
- Ensuring confidentiality – ensures only the intended recipient can decrypt the message
- Ensuring integrity – ensures the message has not been tampered with or changed in transit
- Facilitating disaster recovery
- Offering simple integrated logging and reporting features

The GlobalCerts SecureMail Gateway ("SMG") is an unobtrusive network appliance that works with your current email infrastructure and transparently allows for the encryption and decryption of email messages and attachments. Business communications are expedited and confidential without having to rely on the telephone or expensive physical document delivery methods.

The SMG is standards-based, is easily deployed and managed with little effort by your corporate IT department. Users keep their existing desktop email clients and their email addresses stay the same. The SMG also leverages Internet security standards such as S/MIME and browser-based SSL, rather than expensive VPNs or proprietary software plug-ins.

The SecureMail Gateway protects corporate email where it is most vulnerable – outside the corporate intranet. The solution has been designed to minimize the disruption of existing workflow and email infrastructure and protect email messages with strong, military grade encryption.

Simply put, GlobalCerts helps you to increase your internal controls. It is a simple, cost effective step to comply with the Sarbanes-Oxley Act of 2002.

100 South Street West
Charlottesville,Virginia 22902
434-245-5300
866-868-2747 (Toll Free)
www.globalcerts.net