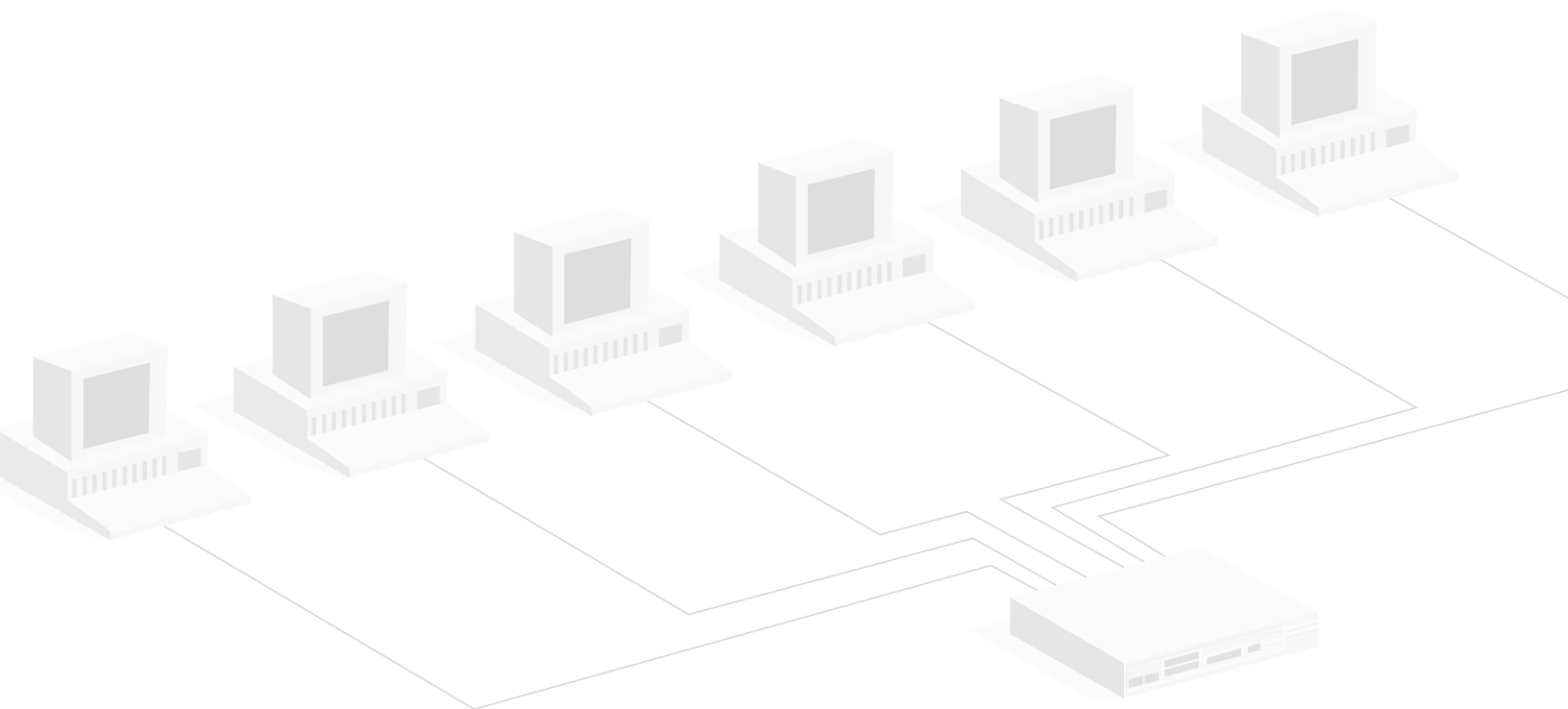


SOX and IT

How Observer can help IT Professionals comply with the data practices components of Sarbanes-Oxley



Executive Summary

U.S. Congress passed the Sarbanes-Oxley Act of 2002 (SOX) to stabilize U.S. markets in light of recent corporate scandals (Enron, WorldCom) that cost investors millions of dollars and deflated the U.S. economy. This Act reforms corporate governance particularly by adding integrity to internal processes that affect earnings and financial disclosures. Ultimately, these changes are supposed to regain consumers' trust in publicly traded companies and help them make appropriate investing decisions.

In general, SOX requires publicly traded companies to be more financially accountable. However, becoming more responsible extends beyond the accounting department—complying with SOX requires cooperation and support among many business units, including IT.

IT supports the corporation's drive to comply with SOX by securing and protecting financial data on the network. IT is also required to consistently document this effort. Without IT support, a corporation simply cannot comply with SOX and will endure retribution from the Securities and Exchange Commission, which regulates SOX.

Network Instruments' Observer can help support IT's role in SOX compliance by securing, monitoring, and documenting financial and other activity on the network.

The purpose of this document is to provide a brief overview of SOX, and how Network Instruments' Observer can help IT fulfill its responsibilities.

SOX Summary

Most of the IT department's responsibilities in the SOX Act fall under sections 302 and 404.

Section 302 requires the public company to affirm in each report that internal controls are adequate and they have not disclosed any knowingly false or misleading statements—presenting a fair representation of financial conditions. Both the public company's officers and public accounting firm must attest to the accuracy of the reporting. Any significant deficiencies found in the internal controls or fraud that involves management or employees must be reported.

Section 404 requires reports to identify management's responsibilities for establishing and maintaining adequate internal controls, and provide an assessment of the effectiveness of the internal controls and procedures affecting financial reporting. The public accounting firm must attest once again to the fairness and accuracy of the reporting.

Refer to the Appendix for the exact excerpt for sections 302 and 404 of the SOX Act.

Auditing Frameworks

There is a lot of room for interpretation of SOX—the Act does not specify a specific internal control framework or IT governance practice appropriate for compliance. In addition, the auditors who are required to attest to financial reports are typically not experts in IT technologies. To overcome these challenges, SOX references the COSO (Committee of Sponsoring Organizations of the Treadway Commission) framework. COSO provides an integrated framework to help businesses assess and enhance their internal control systems and align their IT governance practices with SOX.

There are five main components of the COSO framework that are relevant to SOX: Control Environment, Risk Assessment, Control Activities, Information and Communication, and Monitoring.

1) Internal Environment

The Internal Environment depicts the company's philosophy for risk management and sets the basis of integrity and ethics they oblige to uphold in the environment.

2) Risk Assessment

The purpose of Risk Assessment is to identify potential risks (security breaches, for example), the likelihood of those risks, and the consequent ramifications of those risks to determine how they should be managed.

3) Control Activities

This includes all the policies and operating procedures that are established to mitigate the risks identified in the Risk Assessment and ensure risk responses are handled appropriately. These activities should address the organization of and controls for information systems, as well as specific application guidelines to support accurate and timely processing of transactions.

4) Information and Communication

When creating the standard operating procedures, management must consider the flow of information within the company to ensure it effectively supports employees' activities. In addition, all relevant data needs to be identified, captured, and presented in a coherent format.

5) Monitoring

Internal controls need to be monitored on a continual basis to ensure the security and integrity of the information flowing throughout company and the validity of the corresponding reports. Modifications to internal controls should be made as necessary and recorded in the disclosure.

Observer's Role in SOX

Observer can be an essential tool for an IT administrator to have in place throughout the reporting period. The following technical brief outlines how Network Instruments' Observer can help comply with the data practices components of SOX.

Risk Management

Real-time monitoring for security breaches, plus the ability to measure server and application availability and performance should be part of any comprehensive risk management plan. Observer's Triggers and Alarms can log many common threats to performance and security, including viruses, illegal peer-to-peer activity, and broadcast storms.

The screenshot shows the Observer software interface. The 'Log Settings' tab is active, displaying a table of network events. A callout box with the text 'Alarms identify network threats' points to the table. The table has columns for 'Time', 'Device', 'Event Type', and 'Description'. The 'Event Type' column contains various alarm types such as 'Filter alarm (Peer-To-Peer Client) Liveness', 'Filter alarm (Peer-To-Peer Client) Liveness was disabled', 'Filter alarm (Char Clients) JMS, ICQ, Yahoo, MSN', 'Filter alarm (Char Clients) AIM, ICQ, Yahoo, MSN', 'Filter alarm (Virus) Beagle or / Beagle', 'Filter alarm (Virus) Beagle or / Beagle was disabled', 'Filter alarm (Dial Clients) AIM, ICQ, Yahoo, MSN', 'Filter alarm (Dial Clients) JMS, ICQ, Yahoo, MSN', 'Access Point Linkup (7.32.0) CNB - Wireless Unknown Access Points', and 'Alarm (Wireless Unknown Access Point) was disabled'.

Time	Device	Event Type	Description
02/24/2006 16:00:06	Local Observer / Network 1	Alarm	Filter alarm (Peer-To-Peer Client) Liveness matched 13 packets in 10 second interval. Last Packet IP: 207.218.141.112 -> 24.159.113.41, MAC: 00:0D:56:FB:48:59 -> 00:40...
02/24/2006 16:00:06	Local Observer / Network 1	Alarm	Filter alarm (Peer-To-Peer Client) Liveness was disabled
02/24/2006 16:00:46	Local Observer / Network 1	Alarm	Filter alarm (Char Clients) JMS, ICQ, Yahoo, MSN matched 1 packets in 10 second interval IP: 205.198.210.232 -> 207.218.141.112, MAC: 00:40:10:11:6C:CE -> 00:00:56...
02/24/2006 16:00:46	Local Observer / Network 1	Alarm	Filter alarm (Char Clients) JMS, ICQ, Yahoo, MSN was disabled
02/24/2006 16:03:26	Local Observer / Network 1	Alarm	Filter alarm (Virus) Beagle or / Beagle matched 3 packets in 10 second interval. Last Packet IP: 128.104.224.12 -> 128.104.224.16, MAC: 00:0D:56:FB:48:59 -> FF FF FF...
02/24/2006 16:03:26	Local Observer / Network 1	Alarm	Filter alarm (Virus) Beagle or / Beagle was disabled
02/24/2006 16:05:44	Local Observer / Network 1	Alarm	Filter alarm (Dial Clients) AIM, ICQ, Yahoo, MSN matched 1 packets in 10 second interval IP: 207.218.141.112 -> 205.198.248.133, MAC: 00:0D:56:FB:48:59 -> 00:40:10...
02/24/2006 16:05:44	Local Observer / Network 1	Alarm	Filter alarm (Dial Clients) AIM, ICQ, Yahoo, MSN was disabled
02/24/2006 16:15:24	Local Observer / Network 1	Alarm	Access Point Linkup (7.32.0) CNB - Wireless Unknown Access Points
02/24/2006 16:15:24	Local Observer / Network 1	Alarm	Alarm (Wireless Unknown Access Point) was disabled

Documentation

According to section 302 of the SOX Act, internal controls need to ensure that the information flowing within the company, and the devices involved in the processing, recording, and storage of financial information, is documented and appropriately isolated. Observer's network trending capabilities capture network activity over long periods of time, making it especially useful for validating the IT component of financial reports during the reporting period. Network trending reports allow the CIO to certify the integrity of financial data in the following ways:

- **Station Activity** time can reveal which systems participated on the network during the reporting period. For example, the functionality status of central servers and retail branches during the reporting period can be identified.

Systems that participated on network

Time systems participated on network

Date	Day	Start Time	End Time	Time Span (mins)	Status	First Seen	Last Seen
Sep 28 2004	Tue	09:30	09:40	00:10:00	●	09:30:04	09:39:48
Sep 28 2004	Tue	09:40	09:50	00:10:00	●	09:40:07	09:49:59
Sep 28 2004	Tue	09:50	10:00	00:09:51	●	09:50:17	09:59:59
Sep 28 2004	Tue	10:00	10:10	00:10:00	●	10:00:01	10:10:00
Sep 28 2004	Tue	10:10	10:20	00:10:00	●	10:10:13	10:19:56
Sep 28 2004	Tue	10:20	10:30	00:10:00	●	10:20:08	10:30:00
Sep 28 2004	Tue	10:30	10:40	00:10:00	●	10:30:00	10:39:59
Sep 28 2004	Tue	10:40	10:50	00:10:00	●	10:40:14	10:50:00
Sep 28 2004	Tue	10:50	10:51	00:01:02	●	10:50:00	10:51:02
Sep 28 2004	Tue	10:51	11:00	00:08:10	●	10:54:34	10:59:48
Sep 28 2004	Tue	11:00	11:10	00:10:01	●	11:00:02	11:09:58
Sep 29 2004	Wed	09:50	10:00	00:09:58	●	09:50:03	09:59:58

- Observer's **IP to IP Pairs** and **Internet Patrol** can show what “conversations” took place for key systems during the reporting period—both by identifying when the communication occurred and with which systems. This can, for example, prove that only authorized systems accessed servers storing confidential financial information.

Devices that participated on network

Time devices were active on network

Station 1	Station 2	Packets Total	Bytes Total	Packets 1 < 2	Bytes 1 < 2	Packets 2 < 1	Bytes 2 < 1	Time Span
MEDEA	AT&T	2	216	0	0	2	216	AM 2 4 6 8 10 12 2 4 6
netinst.netinst.com	AT&T	72	6088	40	32	3008	208	
netinst.netinst.com	AT&T	676	48916	335	335	24455	24455	
netinst.netinst.com	AT&T	18	2673	8	8	684	248	
netinst.netinst.com	AT&T	543	479727	454	489	179165	50311	
netinst.netinst.com	AT&T	662	426418	286	315	101979	32440	
netinst.netinst.com	AT&T	2	138	0	0	138	138	
netinst.netinst.com	AT&T	1066	11066	1030	1038	28769	11264	
netinst.netinst.com	AT&T	385	50067	0	385	0	50067	
netinst.netinst.com	AT&T	260	25136	140	120	18160	15840	

- Observer can collect **trending** data across all supported topologies (802.11 a/b/g, gigabit, Ethernet, WAN). Therefore, if the financial system depends on WAN links, deploying a Network Instruments WAN hardware probe to collect trending data can help prove that key WAN circuits were monitored and functional during the reporting period.

Types of trending data

Length of trending

Trending	Status	Start time	End time	Interval (mins)	Stations/Pairs	Packets	Bytes
Application Analysis	16%	10:48:24	10:49:00	1	0	0	0
IP	85%	10:40:00	10:50:00	10	0	1246	179142
Network	16%	10:48:24	10:49:00	1	16	105	10612
VLAN	16%	10:48:24	10:49:00	1	13	36	4048

Secure Log-in

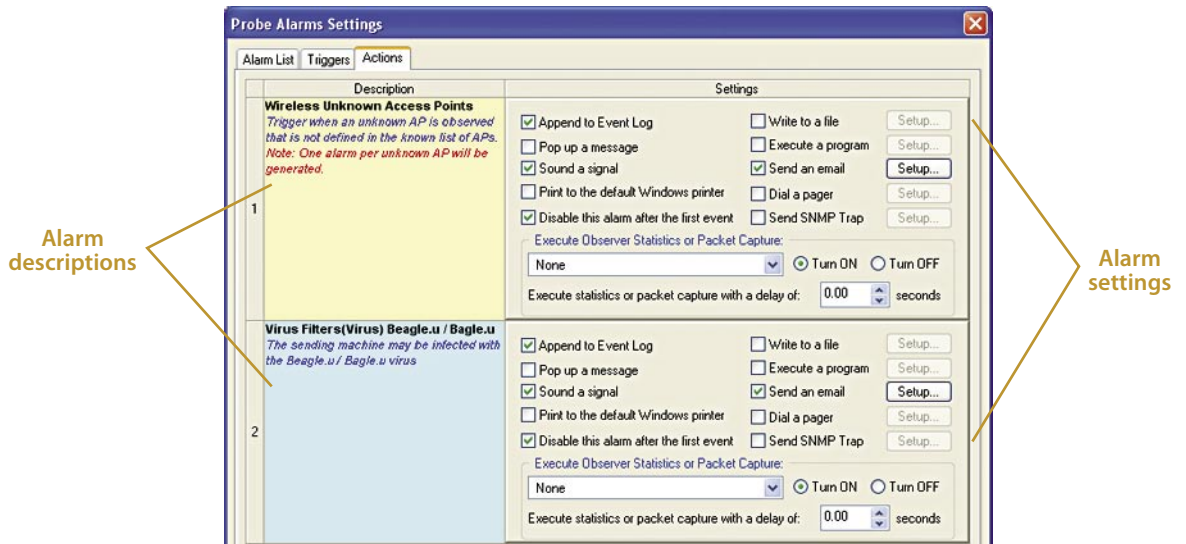
Network Instruments Management Server (NIMS) helps protect the integrity of financial data by retaining a list of user-names, passwords, and permission levels for multiple probes on the network. This ensures only designated administrators are managing specific activity. The NIMS also detects and documents all successful and unsuccessful login attempts to the management devices.

Network administrators

Permission levels set for administrators

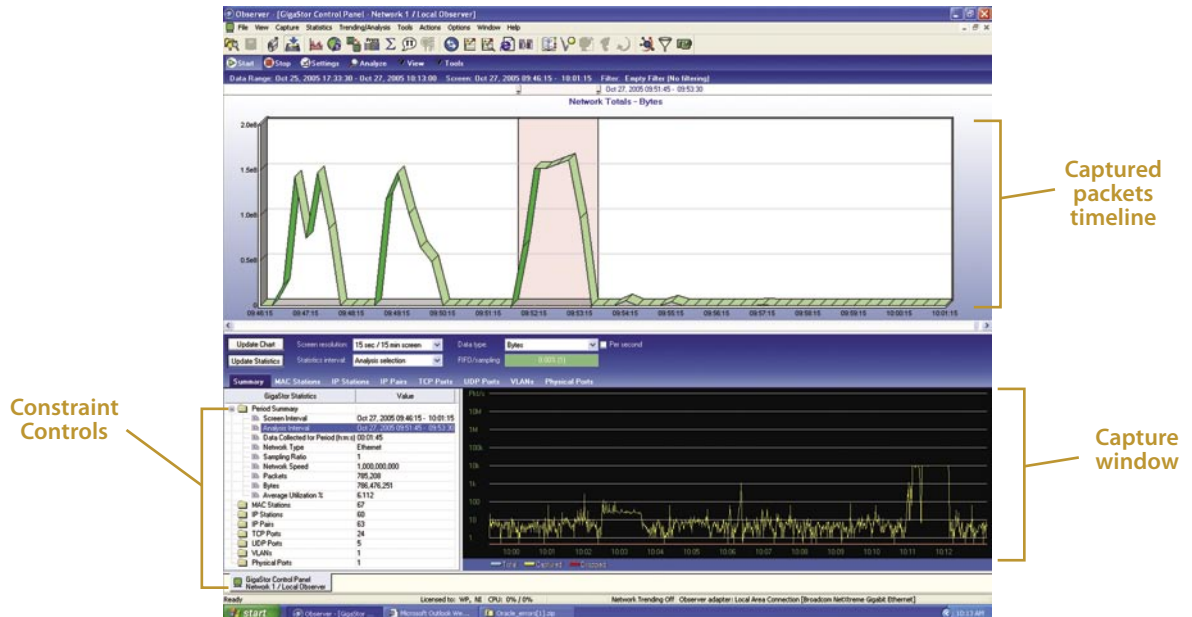
Warning System

Observer's **Triggers and Alarms** can also identify suspicious activity and automatically alert an administrator. For immediate response to problems such as a security breach, Triggers and Alarms can be configured to run a packet capture when problem activity is triggered—eliminating the need to manually track it down. This effort to immediately address problems can be documented, and is looked favorably upon by auditors.



Historical Analysis

Suspicious activity is not always immediately evident. With its simple time-based navigation utility and extensive storage capacity, the **GigaStor** makes it possible to sort through days, weeks, even months worth of network data down to the nanosecond. Therefore, an incident that occurred weeks ago can be quickly investigated and documented. The GigaStor can also reconstruct the stored data, providing hard evidence such as e-mails, web pages (including images), instant messages, and VoIP conversations.



Cost/Benefit Analysis

Adjusting internal control standards and IT governance processes to comply with SOX will naturally induce expenses, but these expenses can quickly escalate if not managed wisely. Utilize Observer to help manage and report on financial communications and network conditions—all while keeping expenses at a minimum. No other network monitoring tool or management device can provide this much functionality and security in one solution, and at such a reasonable price.

Conclusion

IT has been designated as a key role player in SOX compliance. Although it may take considerable effort to coordinate management philosophies and implement an organized and acceptable set of standards, SOX compliance can ultimately enhance business functions—not just please the SEC. Relying on Observer to help support the company’s mission to comply with SOX will make meeting those standards much easier and more reasonable than any other tools.

Observer helps IT professionals comply with the data practices components of Sarbanes–Oxley in the following ways:

SOX Role	Observer Feature	Description
Risk Management	Triggers and Alarms	Identifies many common threats.
Documentation	Station Activity	Reveals which systems participated on the network during the reporting period.
	IP to IP Pairs Internet Patrol	Show conversations that took place between key systems.
	Historical Analysis	Stores days, even weeks’ worth of network data, providing hard evidence of network communications including web pages, e-mails, phone conversations, and instant messages.
Security	Secure Log-in	Retains a list of permission levels on network probes to protect the integrity of financial data.
	Triggers and Alarms	Immediately alert IT of suspicious activity.

Corporate Headquarters Network Instruments, LLC • 10701 Red Circle Drive • Minnetonka, MN 55343 • USA
toll free (800) 526-7919 • telephone (952) 358-3800 • fax (952) 358-3801 • www.networkinstruments.com

European Headquarters Network Instruments • 7 Old Yard • Rectory Lane • Brasted, Westerham • Kent TN16 1JP • United Kingdom
telephone +44 (0) 1959 569880 • fax +44 (0) 1959 569881 • www.networkinstruments.co.uk

France Office Network Instruments • 1 rue du 19 janvier • 92380 Garches • Paris • France
telephone +33 (0) 1 47 10 95 21 • fax +33 (0) 1 47 10 95 19 • www.networkinstruments.fr

Germany Office Network Instruments • Allacherstrasse 189 • 80997 München
telephone +49 (89) 159 842-48 • fax +49 (89) 159 842-49 • www.networkinstruments.de

Sec. 302 CORPORATE RESPONSIBILITY FOR FINANCIAL REPORTS

REGULATIONS REQUIRED.—The Commission shall, by rule, require for each company filing periodic reports under section 13(a) or 15(d) of the Securities Exchange Act of 1934 (15 U.S.C. 78m, 78o(d)), that the principal executive officer or officers and the principal financial officer or officers, or persons performing similar functions, certify in each annual or quarterly report filed or submitted under either such section of such Act that—

- 1) The signing officer has reviewed the report;
- 2) Based on the officer's knowledge, the report does not contain any untrue statement of a material fact or omit to state a material fact necessary in order to make the statements made, in light of the circumstances under which such statements were made, not misleading;
- 3) Based on such officer's knowledge, the financial statements, and other financial information included in the report, fairly present in all material respects the financial condition and results of operations of the issuer as of, and for, the periods presented in the report;
- 4) The signing officers—
 - a. Are responsible for establishing and maintaining internal controls;
 - b. Have designed such internal controls to ensure that material information relating to the issuer and its consolidated subsidiaries is made known to such officers by others within those entities, particularly during the period in which the periodic reports are being prepared;
 - c. Have evaluated the effectiveness of the issuer's internal controls as of a date within 90 days prior to the report; and
 - d. Have presented in the report their conclusions about the effectiveness of their internal controls based on their evaluation as of that date;
- 5) The signing officers have disclosed to the issuer's auditors and the audit committee of the board of directors (or persons fulfilling the equivalent function) —
 - a. All significant deficiencies in the design or operation of internal controls which could adversely affect the issuer's ability to record, process, summarize, and report financial data and have identified for the issuer's auditors any material weaknesses in internal controls; and
 - b. Any fraud, whether or not material, that involves management or other employees who have a significant role in the issuer's internal controls; and
- 6) The signing officers have indicated in the report whether or not there were significant changes in internal controls subsequent to the date of their evaluation, including any corrective actions with regard to significant deficiencies and material weaknesses.
 - b. FOREIGN REINCORPORATIONS HAVE NO EFFECT.— Nothing in this section 302 shall be interpreted or applied in any way to allow any issuer to lessen the legal force of the statement required under this section 302, by an issuer having reincorporated or having engaged in any other transaction that resulted in the transfer of the corporate domicile or offices of the issuer from inside the United States to outside of the United States.
 - c. DEADLINE.—The rules required by subsection (a) shall be effective not later than 30 days after the date of enactment of this Act.

Sec. 404 MANAGEMENT ASSESSMENT OF INTERNAL CONTROLS

a. RULES REQUIRED.— The Commission shall prescribe rules requiring each annual report required by section 13(a) or 15(d) of the Securities Exchange Act of 1934 (15 U.S.C. 78m or 78o(d)) to contain an internal control report, which shall—

- 1) state the responsibility of management for establishing and maintaining an adequate internal control structure and procedures for financial reporting; and
- 2) contain an assessment, as of the end of the most recent fiscal year of the issuer, of the effectiveness of the internal control structure and procedures of the issuer for financial reporting.

b. INTERNAL CONTROL EVALUATION AND REPORTING.—With respect to the internal control assessment required by subsection a., each registered public accounting firm that prepares or issues the audit report for the issuer shall attest to, and report on, the assessment made by the management of the issuer. An attestation made under this subsection shall be made in accordance with standards for attestation engagements issued or adopted by the Board. Any such attestation shall not be the subject of a separate engagement.