Security & Surveillance

United States: Network Security and Sarbanes-Oxley: Developing a Framework for Internal Controls

By Rosalind K. Allen and Lance D. Myers, Partners in the Washington D.C and New York offices, respectively, of Holland & Knight LLP. Contributions to this article were also made by Roosevelt S. Conyers. The authors may be contacted by e-mail at: lance.myers@hklaw.com and rosalind.allen@hklaw.com, or on tel. +1 888 688 8500.

On July 30, 2002, in response to numerous widely publicised corporate accounting scandals, such as Enron and Worldcom, among others, Congress enacted the Sarbanes-Oxley Act ("the Act") in order to restore public confidence in corporate governance. The Act drastically redesigns federal reporting obligations, and heightens accountability standards for corporate directors, officers, auditors, and legal counsel. Rules and standards for reporting on internal controls and procedures for financial reporting, pursuant to §404 and §302 of Sarbanes-Oxley, are still being implemented. However, companies need to establish reasonable guidelines and boundaries as a basis for identifying, designing and maintaining controls and procedures for financial reporting.

A critical aspect of maintaining proper internal controls for financial reporting is ensuring that the collection and maintenance of corporate data is protected against corruption and unauthorised access. Such a level of information security cannot be met unless comprehensively secure IT networks are in place. The Act requires corporate vigilance in adopting and executing a framework for securing, collecting, disseminating, and using corporate data.

In a related development, in February 2003, the President's Critical Infrastructure Protection Board released the "National Strategy to Secure Cyberspace" ("the National Strategy").[1] While the National Strategy does not propose regulation of corporate data security practices, it strongly advocates a voluntary approach that complements the "internal controls" mandated by the Act.

In April 2004, the Corporate Governance Task Force of the National Cyber Security Partnership issued a report entitled, "Information Security Governance – A Call to Action" ("the Report"). The Report concludes that strengthening national information security requires that this issue be treated as a matter of corporate governance that requires the attention of Boards and CEOs. In addition, the CEOs of publicly-traded corporations that lead the Governance Task Force provide guidance for generating and implementing an information security governance programme. The Report goes beyond the National Strategy in setting a standard for the duty of corporations to secure their data, and could inform compliance determinations under the Act.

This article provides an overview of key provisions of the Act regarding proper internal controls, outlines and discusses key considerations in developing a proper internal control framework, and identifies resources essential to meeting the Act's internal control mandate. In addition, this article identifies those aspects of the National Strategy and the Report that directly implicate the role of corporate governance in establishing and maintaining an information security programme. Interpretation and application of the Act is still in its nascent stage, therefore recommendations made by the National Strategy and the Report are relevant to evaluating the sufficiency of corporate information security practices.

The Regulatory Imperative for Proper Internal Controls for Financial Reporting

CEO and CFO Certification: Internal Controls for Financial Reporting; Disclosure Controls and Procedures

The SEC certification rule, "Final Rule: Certification of Disclosure in Companies' Quarterly and Annual Reports", requires CEOs and CFOs, as part of each quarterly and annual report, to certify that, among other things, they are responsible for, and have established and maintained, disclosure controls and procedures, and that they have:

- Designed the disclosure controls and procedures to ensure that material information relating to the company is made known to them.
- Evaluated their effectiveness within 90 days prior to the report's filing date.
- Presented conclusions about their effectiveness in the report.

Additionally, the CEO and CFO must certify that they have disclosed to the company's audit committee and external auditor any significant deficiencies and material weaknesses in internal controls for financial reporting.

The SEC, in its "Proposed Rule: Disclosure Required by Sections 404, 406 and 407 of the Sarbanes-Oxley Act of 2002", expressed its belief that "…a significant portion of internal controls and procedures for financial reporting are included in disclosure controls and procedures". Thus, while CEO and CFO certification of internal controls for financial reporting has not been expressly mandated by the SEC rules, to the extent that disclosure controls and procedures and internal controls for financial reporting overlap, those internal controls are the subject of certification.

Management and External Auditor Obligations to Establish, Evaluate, and Report on Controls

Section 404 of the Act requires corporations to assess risks to their business processes that affect financial reporting. Specifically, with regard to internal controls for financial

  WDPR ISSN 1473-3579

reporting, the section requires each annual report of an issuer to contain an "internal control report" which shall:

- state the responsibility of management for establishing and maintaining adequate internal controls and procedures for financial reporting; and
- contain an assessment, as of the end of the issuer's fiscal year, of the effectiveness of the internal control structure and procedures of the issuer for financial reporting.

The external auditor is required, under the Section, to attest to, and report on, management's internal control assessment.

Accelerated filers (typically companies with aggregate market values of common equity held by non-affiliates of $75 million or more, and subject to the reporting requirements of the Exchange Act for at least one year) must comply with the new rules concerning disclosure of reports on internal controls in their annual reports for the fiscal years ending on or after June 15, 2004. Non-accelerated filers must initiate compliance with the disclosure requirements in annual reports for their first fiscal year ending on or after April 15, 2005. A company must begin compliance with the quarterly evaluation requirements for its first periodic report due after the first annual report that must include the management's report on internal control.

In light of the obligations being imposed by the Act on CEOs, CFOs, management, and a company's external auditors, the adoption and execution of proper internal controls for financial reporting by public companies should not be delayed. A critical aspect of proper internal controls for financial reporting is ensuring, collecting and maintaining corporate data, while protecting it against corruption and unauthorised access. Such a level of information retention and security cannot be met unless comprehensively secure IT networks are in place.

Information Retention and Security: Key Aspects of an Internal Control Framework

Challenges to IT Information Security and Retention

Cybersecurity is key to informed risk management. At a minimum, a corporation must have operational structures in place that reliably ensure access control and authentication. Securing and retaining corporate information is complicated by more formidable challenges to network security. First, executives and IT managers are facing more complex and frequent information threats, launched by hackers, with low and high levels of technical skill, and corporate insiders, who have access to corporate information as a result of an increased need for personnel administration of increased inflow of corporate information. Secondly, technology, through broadened corporate IT networks using mobile communication devices and extended off-site networks, has created new pathways through which hackers attempt to gain unauthorised access to corporate information. Also, operating system software codes are increasingly complex, and are constantly being revised, creating a vast IT landscape that requires constant and sophisticated efforts to secure. Planning for corporate cybersecurity must be proactive and continuous because new vulnerabilities are created or discovered regularly.

The National Strategy characterises cybersecurity as a collective effort, with each private entity responsible for securing those portions they own, operate, control and interact with. Because large scale operations are the most common targets of network intrusions, it is incumbent upon corporations to manage those risks responsibly. To reliably accomplish these goals, the National Strategy emphasises that corporate accountability for network security must involve the highest levels of management. The National Strategy recommends that the CEO and the board of directors should be directly responsible for security.

The Report acted on these general principles to,

> identify "… cyber security roles and responsibilities within corporate management structures and references and combines industry-accepted standards and best practices, metrics and toolsets that bring accountability to three key elements of corporate governance programs and information security systems: people, process and technology".[1]

The Report elaborates on the five recommendations of the Corporate Governance Taskforce:

- Organisations should use the Report's information security governance framework to fully integrate cybersecurity into their corporate governance process.
- Organisations should demonstrate their commitment to information security governance by stating on their websites that they will use the tools developed by the Corporate Governance Task Force to assess performance and report results to their board of directors.
- All Task Force members/contributors, as well as leading trade/membership associations, should commit to information security governance by voluntarily posting a statement on their respective websites, and by encouraging others to do the same.
- The Department of Homeland Security should endorse the Report's information security governance frameworks, the core principals, and encourage the private sector to make cybersecurity part of its corporate governance efforts.
- The Committee of Sponsoring Organizations of the Treadway Commission ("COSO") should revise the Internal Controls-Integrated Framework so that it explicitly addresses information security governance.

While the National Strategy and the Report are voluntary standards holding no force of law, both documents are explicitly offering private industry the opportunity for self-regulation. There is, however, the implicit message that if the private sector ignores these recommendations, Congress may be compelled to impose security mandates.

Internal Control Objectives

Any internal control framework must begin with specific objectives in mind, thus avoiding the misdirection of costly security initiatives. Primary internal control objectives, in light of the Act, include the identification and management

of threats and IT vulnerabilities. Businesses must be able to prioritise informational assets, identify asset vulnerabilities, and delegate resources to assess and repel threats to these assets accordingly. Also, an internal control framework in the post-Act era, must produce timely security information so as to facilitate the accurate evaluation of internal controls by corporate officers, management, external auditors and legal counsel.

Strategic Considerations in Implementing an Internal Control Framework

An effective internal control framework is best implemented with certain strategic objectives. Primarily, corporate officers, management, external auditors and legal counsel, as well as IT staff responsible for maintaining information systems, must co-operate seamlessly. Since IT professionals rarely fully comprehend financial information, accounting professionals rarely fully understand a company's regulatory compliance obligations, and management rarely grasps the technical intricacies behind information security controls, it is necessary to implement an internal control framework that facilitates in-depth collaboration among these groups.

Additionally, an internal control framework must leverage the necessities of maximum informational security, timely access to corporate information, and comprehensive retention of corporate information with the goal of ensuring full, complete and accurate financial reporting.

Resources for Developing an Effective Internal Control Framework

Legal Counsel

There is an abundance of literature with general information and considerations addressing internal control and reporting requirements under the Act. However, to fully comprehend their obligations under the Act and subsequent SEC regulations, companies should consult with legal counsel.

External Auditors

Collaboration between legal counsel, external auditors, officers and management, and IT professionals is essential in developing and implementing an effective internal control framework. External auditors employ various models for internal control, the most accepted of which is the framework provided by the COSO. Many companies already possess an internal control framework based upon COSO principles. COSO identifies five components of internal control:

- Control environment – focuses on developing corporate discipline and structure as the foundation for an internal control system.
- Risk assessment – concentrates on identifying and managing risks to achieve internal control objectives.
- Control activities – involves the structuring and adoption of internal policies and procedures that ensure the execution of management's internal control objectives and risk-containment strategies.
- Information and communication – facilitates efficient delegation of internal control duties among staff by providing a framework for communicating specific internal control tasks to employees.
- Monitoring – concerns the overall maintenance of internal controls by management.

IT Specialists

IT initiatives within the internal control framework will focus upon acquisition and application of software conducive to meeting internal control objectives, and facilitation of management, legal counsel, external auditor, and staff duties by securing information and providing it to these individuals and groups in readily usable formats. Some issues that IT specialists will focus on are:

- Implementing a secure IT structure that restricts access to authorised individuals only. There are many software applications that are being developed to help IT specialists meet this security imperative. Some software applications purport to "encrypt" corporate information so as to prevent unauthorised access to, and interpretation of, that information. Other applications work to restrict IT applications so that they cannot be misused to perform unauthorised functions. Clearly, adoption of any or a combination of these applications will depend on specific security needs.
- Gathering and retaining information, and organising that information so as to facilitate timely financial reporting.
- Consulting with legal counsel and external auditors to ensure compatibility between the corporate IT network, the internal control auditing framework, and regulatory mandates.

Whichever internal control framework corporate officers and management choose, legal consultation and collaboration with IT and external auditing professionals is essential to ensuring that the framework complies with regulatory standards and meets the corporation's internal control objectives.

1 A draft of this document was released for comment on September 18, 2002. The final version was released in February 2003.

2 Press Release, National Cyber Security Partnership, *Corporate Governance Task Force of the National Cyber Security Partnership Releases Industry Framework,* released April 12, 2004.