The Significance of the Dodd-Frank Act

Larry Marks, CISA, CGEIT, CRISC, CFE, CISSP, PMP, is a member of ISACA's Governmental and Regulatory Agencies Regional Area 4 Subcommittee, and is also a member of the following US Technical Advisory Groups (TAGs): International Organization of Standardization (ISO)/ Technical Committee (TC) 236—Project Management Institute (PMI)—Program Management, ISO/ International Electrotechnical Commission (IEC)/Joint Technical Committee (JTC)/Working Group (WG) 6—Information Security, and ISO/TC 247—Fraud Countermeasures and Controls. He is also a member of the Association of Certified Fraud Examiners (ACFE) Editorial Advisory Review Committee and is vice chair of the ACFE Foundation Scholarship Committee.

In 2008, the global financial system was melting down. A result of the crisis was the US Dodd-Frank Act, which arose from numerous congressional hearings, commissions and other proposals. At more than 2,300 pages, the Act requires that new formal rules be adopted by 11 different regulatory agencies, all within a year and a half of its passage.[1] The new requirements are being phased in over time. No time frame for implementation of Dodd-Frank has been set. On 4 May 2011, the US House Agriculture Committee passed a bill to increase the statutory deadline by 18 months to give regulators the time and data they need to develop thoughtful guidelines without making substantive changes to the intent of the Dodd-Frank Act.

Myron S. Scholes, professor of finance, emeritus, in the Graduate School of Business at Stanford University (California, USA), indicates that infrastructure to support financial innovations, as suggested by economic theory, will, by and large, increase the chances that controls will be insufficient at times to prevent breakdowns in governance mechanisms.[2] It would be too expensive to build all of the information links, legal rules, risk management controls and so forth in advance of new product introductions.

The relevant questions that need to be asked are: How does the Dodd-Frank Act impact IT auditors? How does the Dodd-Frank Act impact global organizations?

PROVISIONS OF THE DODD-FRANK ACT THAT MAY IMPACT IT AUDITORS

A review of a brief summary of the Dodd-Frank Act (hereafter referred to as the Act) prepared by the US Senate[3] and the results of a recent research study prepared by more than 40 professors from New York University Stern School of Business (USA) found that the Act appears to impact IT auditors in the following areas:[4]

1. **Corporate governance**—The Act provides shareholders with a voice on corporate affairs with a nonbinding vote on executive compensation and golden parachutes.[5]
2. **Funeral plans**—The Act requires large, complex financial companies to periodically submit plans for their rapid and orderly shutdown should they go under. Companies will be hit with higher capital requirements and restrictions on growth and activity, as well as divestment, if they fail to submit acceptable plans. These plans will help regulators understand the structure of the companies they oversee and will serve as a road map for shutting down a company if it fails. Significant costs for failing to produce a credible plan create incentives for firms to rationalize structures or operations that cannot be unwound easily.[6] Auditors review the adequacy and completeness of disaster recovery and contingency plans prepared and executed by IT management. These plans are also evaluated by external regulatory authorities. The need for funeral plans will require IT auditors to review the company's shutdown procedures.
3. **Confusion as to governmental authorities**—The Act does not identify a central agency or authority that will be accountable for ensuring compliance. Instead, the responsibility is shared. As a result, the potential for conflicting and inconsistent requirements between agencies exists, which then complicates the evaluation of internal controls, processes and technologies. It becomes difficult because coordination with other agencies regarding their requirements and standards is a necessity.
4. **Financial stability oversight council**—The Act establishes an oversight group, called the Financial Stability Oversight Council. The council will be chaired by the Treasury secretary and will include the Federal Reserve Board, the Securities and Exchange Commission (SEC), the Commodity Futures Trading Commission (CFTC), the Office of the Comptroller of the Currency (OCC), the Federal Deposit Insurance Corporation (FDIC), the Federal Housing Finance Agency (FHFA), the National Credit Union Administration (NCUA), the new Consumer

Financial Protection Bureau, and an independent appointee with insurance expertise. The council is responsible for identifying and responding to emerging risks throughout the financial system. Also, the Office of Financial Research and member agencies of the council will collect and analyze data to identify and monitor emerging risks to the economy and make this information public in periodic reports and testimony to the US Congress each year.[7] A reasonable question to ask is whether the emerging risks to the economy will and should include risks to the IT infrastructure of enterprises, such as vulnerabilities and threats to their cybersecurity networks, social engineering, data leakage, lack of patch management procedures, and lack of ITIL Service Management processes. One can guess that the response to this query is negative, and that the risks included in the scope of the council's purview will be primarily financial.

5. **Fills regulatory gaps**—The Act requires hedge funds and private equity advisors to register with the SEC as investment advisers and provide information about their trades and portfolios necessary to assess systemic risk. These data will be shared with the systemic risk regulator, and the SEC will report to Congress annually on how it uses these data to protect investors and market integrity.[8] The question is whether the hedge funds will:
   - Update their procedures to ensure the accuracy and completeness of regulatory reporting of portfolio positions
   - Track and monitor the financial risk of their trading and principal positions, where appropriate
   - Reduce their IT risk, e.g., disaster recovery, to their infrastructure based on a tighter definition and latitude of system risk that they can incur
6. **Disclosure**—Requires nationally recognized statistical ratings organizations to disclose their methodologies, their use of third parties for due-diligence efforts and their ratings track records.[9] The question is whether and how this affects the status of the Statement on Auditing Standards (SAS) No. 70 standard issued by the American Institute of Certified Public Accountants (AICPA) and used by firms to ensure the quality of services offered by their clients and service bureaus.

In April 2010, the AICPA published Statement on Standards for Attestation Engagements (SSAE) No. 16, to supersede the existing guidance (SAS 70) for performing an examination of a service organization's controls and processes, with an effective date of 15 June 2011. SSAE 16, *Reporting on Controls at a Service Organization*, updates the US service organization reporting standard so that it mirrors and complies with the new international service organization reporting standard, International Standard on Assurance Engagements (ISAE) 3402, *Assurance Reports on Controls at a Service Organization*.

A service auditor's report with an unqualified opinion offers several benefits, including:

- It differentiates the service organization from its peers by demonstrating the establishment of control objectives and effectively designed control activities.
- It can help a service organization build trust with its user organizations (i.e., customers).
- Without a current service auditor's report, a service organization may have to entertain multiple audit requests from its customers and their respective auditors. Multiple visits from user auditors can place a strain on the service organization's resources. A service auditor's report ensures that all user organizations and their auditors have access to the same information; in many cases, this will satisfy the user auditor's requirements.[10]

The differences noted by SSAE 16 are as follows:[11]

- The assertions in SSAE 16 are similar in nature to SAS 70 audit management representation letters. A separate management representation letter is also still required.
- For Type II reports, the service auditor's opinion on fair presentation of the system and suitability of design will be for the period covered by the report; under SAS 70, this is currently as of a point in time.

7. **Better disclosure**—Requires issuers to disclose more information about the underlying assets and to analyze their quality.[12] This requirement does not impact the degree and quality of information being released to the SEC at this time.

HOW THE DODD-FRANK ACT MAY IMPACT GLOBAL ORGANIZATIONS

Given the global nature of financial markets and competition among major banks, how organizations will be impacted internationally by the Dodd-Frank Act is not yet known. For example, the Dodd-Frank Act requires all firms to disclose the permissibility of hedging their stock and option positions. Further, some believe that international cooperation in regulation is needed to prevent financial firms from arbitraging the market for human capital through choice of jurisdiction. The international Group of Twenty (G-20) Finance Ministers and Central Bank Governors put in place a set of agreed-upon principles on compensation that address three layers of governance at significant financial institutions: managerial performance and risk incentives, corporate governance, and regulatory oversight. The international Financial Stability Board proposed to operate in tandem the:

- Creation of a board remuneration committee
- Endorsement of a limit on total variable compensation
- Review by regulatory supervisors of compensation policies to guard against institutional and systemic risk

The international impact of the Dodd-Frank Act is intertwined with efforts by the G-20 to control system and institutional risk.

CONCLUSIONS

At this time, the Dodd-Frank Act, along with other reforms issued by the US Congress and other regulatory agencies, attempts to address the systemic risk that impacted the US economy several years ago. The impact of this act on regulatory reporting infrastructure by firms will not be seen for at least several years. One chief information officer at a global fund manager told *Wall Street & Technology* that there is not enough information about Dodd-Frank for his firm to comment. "The legislation is long and complex at 2,307 pages, 16 titles and 540 sections. To back the provisions of the act, dozens of new boards, bureaus and offices must be created."[13] One can expect the following: raising budgets or financial companies trying to work around this regulation via spinoffs and the like.

ENDNOTES

[1] Acharya, Viral V.; Thomas F. Cooley; Matthew P. Richardson; Ingo Walter; *Regulating Wall Street, The Dodd-Frank Act and the New Architecture of Global Finance*, New York University Leonard N. Stern School of Business, Wiley Finance, USA, 2011

[2] Acharya, Viral V.; Thomas F. Cooley; Matthew P. Richardson; Ingo Walter; *Regulating Wall Street: The Dodd-Frank Act and the New Architecture of Global Finance*, Wiley, USA, 2010

[3] US Senate, *Brief Summary of the Dodd-Frank Wall Street Reform and Consumer Protection Act*, USA, 2010, *http://banking.senate.gov/public/_files/070110_Dodd_Frank_Wall_Street_Reform_comprehensive_summary_Final.pdf*

[4] *Op cit*, Acharya, Viral V.; Thomas F. Cooley; Matthew P. Richardson; Ingo Walter

[5] *Ibid*., page 2

[6] *Ibid*.

[7] *Ibid*., page 4

[8] *Ibid*., page 9

[9] *Ibid*., page 10

[10] *SSAE 16.com*, "Benefits to Service Organizations," *http://ssae16.com/SSAE16_service.html*

[11] Brenner, Bill, "SAS 70 Replacement: SSAE 16," *CSO*, 6 October 2010, *www.csoonline.com/article/622277/sas-70-replacement-ssae-16-*

[12] *Op cit*, US Senate, page 14

[13] MacSweeney, Greg; "Dodd-Frank's Impact on IT," *Wall Street & Technology*, 8 February 2011, *www.wallstreetandtech.com/regulatory-compliance/229200184*