A survey of corporate governance and overlapping regulations in banking

Kamala Raghavan
Received (in revised form): 17th April, 2007

Accounting and Taxation, Robert Morris University, Pittsburgh, PA, USA; Tel: +1 (412) 397-3970;
E-mail: raghavan@rmu.edu

Kamala Raghavan *was a senior executive at US major bank holding companies where she had responsibility for operations, compliance and systems. She had managed the operations functions and directed the banks' compliance with FDICIA, SOX, BSA/AML, Basel II and AMA until 2003. She is currently an assistant professor in Accounting and Taxation with research interests in banking, accounting, finance, internal control, and strategy.*

ABSTRACT

KEYWORDS: banking regulations, corporate governance, regulatory overlap

Banking managers, chief financial officers , and politicians are increasingly voicing their concerns about the 'excessive' burden imposed by compliance with Sarbanes–Oxley (SOX) Act, Bank Secrecy Act/Anti-Money Laundering (BSA/AML), and Interagency Supervisory guidance on operational risk advanced measurement approaches (AMA). The underpinnings of the banking regulations — FDICIA, SOX, AMA, and BSA/AML — are all, however, based on the organisation's internal control structure, and provide a solid framework for enterprise-wide management of operational risk and capital. The Intelligence Reform and Terrorism Prevention Act of 2004, ACH Guideline changes, Check 21, and increasing competition through technology-based products and services are part of the larger picture of evolving threats and increasing change in the industry that are challenging the banking managers to take a holistic approach to enterprise-wide risk management. In the current environment of corporate scandals and public distrust, the investor community will use the integrated compliance framework to differentiate between adopters and nonadopters of good corporate management practices. This paper highlights the regulatory overlaps and inherent leveraging opportunities in the compliance practices, and points out the competitive advantage to progressive banking institutions. It includes a personal view for implementing integrated enterprise-wide operational risk management leveraging on existing compliance practices, and outlines regulatory Guidelines for information technology controls and BSA/AML compliance. The paper explores how the compliance requirements are changing the emphasis of corporate governance and finance functions in banking institutions.

International Journal of Disclosure and Governance (2007) **4,** 181–194. doi:10.1057/palgrave.jdg.2050058

INTRODUCTION

The Board of Directors of banking institutions often find themselves unsure about dealing with overlapping and sometimes conflicting requirements imposed by FDICIA of 1991, Bank Secrecy Act/Patriot Act/Anti-Money Laundering (BSA/AML) of 2001, Sarbanes–Oxley (SOX) Act of 2002, and the Interagency supervisory guidance on operational risk advanced measurement approach (AMA) of 2003. Banking managers, chief financial officers (CFOs), and politicians are increasingly voicing their concerns about the 'excessive' cost and administrative burden imposed by compliance with these and other banking regulations. Congress and regulatory agencies are bombarded with lobbying efforts to reduce the requirements

of SOX. Some representative comments are listed below.

Complaints heard at the ABA National Conference for Community Bankers in February 2005 ranged from 'SOX 404 is a blank check for audit firms' to 'we are spending too much time on internal controls and not enough on banking, from my point of view, SOX 404 is coming close to pure burden for most banks'.[1] Responses to the survey conducted by the North Carolina Bankers Association in March 2005 showed that the bankers were disturbed about the duplicative nature of SOX evaluations with other regulations like FDICIA, and the percentage of net income going to SOX compliance instead of profit (range from 1.0 to 4.89 per cent).[2]

The signoffs and certifications to ensure accountability by corporate managers have, however, shown considerable success to bolster investor confidence since the inception of SOX. Institutional Shareholder Services' survey of corporate directors in 2005 titled 'Second anniversary: The impact of Sarbanes–Oxley' found that 60 per cent felt that SOX has been positive for their companies, and 70 per cent said that SOX led to improved board governance.[3] In CFO Research Services' survey of 180 finance executives in August 2005,[4] increased management confidence in the accuracy of the financial reports due to SOX requirements on documentation, monitoring, and enforcement of controls was cited as the primary benefit of the compliance effort. The survey respondents felt that the market reward of stock price premium for good governance and tight regulatory controls far outweighs the high costs for SOX implementation, and that companies (including highly decentralised ones) have been pushed by SOX to apply uniform standard for compliance across the entire organisation. CFO magazine survey of 213 finance executives in August 2006 also found that 70 per cent of the respondents felt that they had gained value from SOX compliance, and 65 per cent of the respondents felt that compliance with SOX has produced value in business process improvements.[5]

How do we reconcile the loud complaints from the corporate managers with the above survey results and remarks from regulators and corporate governance advocates about the need for continued regulatory oversight and value of the compliance actions? Who is right? Can these opposite views come together synergistically without increasing the costs annually? Can SOX, BSA/AML, and AMA compliance efforts leverage what banks have been already doing for FDICIA compliance? The answer to the first two questions is clearly a resounding 'yes' from the results of the surveys cited above. The comments from the directors and financial executives about the positive impact of SOX and other related regulations show that the regulatory oversight and compliance efforts are rewarded by investors in the form of higher stock price relative to nonadopter peers. The same surveys also showed that the compliance costs taper off, and stock prices remain high for adopters in later years — an ideal outcome for major implementation projects.

Based on industry experience, I submit that financial institutions' compliance practices for regulations such as FDICIA and the predecessor regulations to BSA/AML provide a strong foundation for building the enterprise-wide risk management, creating an advantage over their peers in other industries. Many large financial institutions have expanded the granularity of the FDICIA operational loss data and managers' self-assessments of internal control, augmented them with industry-wide external data to represent infrequent loss events, and used the database for SOX certifications and operational risk-based capital modelling for AMA. In a survey by American banker in May 2006,[6] banking managers said that the focus on operational risk management was helpful in ensuring accountability at all levels. Sixty-seven per cent of large banks and 56 per cent of the small banks cited operational efficiencies as the main benefit of operational risk management practices. Organisations like RBS, Greater Bay

Bancorp, Meridian Credit Union, and Sun Trust are working on ways to leverage compliance technology to improve management of products and customers, while Fiserv uses the centralised compliance platform to focus on the organisation's core competencies.[7,8] This paper highlights the regulatory overlaps and emphasises the integral nature of FDICIA, SOX, AMA, and BSA/AML compliance in overall customer relationship and internal control structure across business lines. It explores how the compliance requirements are changing the emphasis of corporate governance and finance functions in banking institutions.

BACKGROUND

FDICIA, SOX, AMA, and BSA/AML along with other related regulations form the pillars of the integrated enterprise risk management framework. FDICIA centered on *internal controls* related to banking operations, SOX concentrated primarily on *sound internal controls* related to financial reporting based on transactions, BSA/AML specified *due diligence procedures* for monitoring foreign correspondent and private banking customer accounts, and Inter-agency Supervisory Guidance on Operational Risk AMA (based on Basel II Guidelines) proposed assigning risk-based capital to businesses and products based on *internal controls*. All of the above regulations require that financial institutions have a comprehensive system of 'risk control self-assessment (RCSA)' and related documentation. The common thread in these regulations is internal control and compliance monitoring of transactions from *all* lines of business dealing with *all* customers, measuring and quantifying the inherent risks, and implementing risk mitigation measures. The underpinnings of the banking regulations — the elements of safety and soundness in FDICIA, the internal control and reporting requirements of SOX, the quantitative tools of AMA for assigning operational risk-based capital, and the due diligence and reporting of BSA/AML — are all based on the organisation's internal control structure, and provide a solid framework for enterprise-wide management of operational risk and capital. The FFIEC publication on uniform examination Guidelines for BSA/AML compliance issued in 2005,[9] and the joint note issued by Basel Committee, International Association of Insurance Supervisors (IAIS), and International Organisation of Securities Commissions (IOSCO) on initiatives to combat money laundering and financing of terrorism in 2003[10] indicate that examiners are taking a comprehensive, global, and systemic approach to regulatory compliance. In addition, Intelligence Reform and Terrorism Prevention Act of 2004, ACH Guideline changes, Check 21, and increasing competition through technology-based products and services are part of the larger picture of evolving threats and increasing change in the industry that are challenging the banking managers to take a holistic approach to enterprise-wide risk management. In the current environment of corporate scandals and public distrust, the investor community will use the integrated compliance framework to differentiate between adopters and nonadopters of good corporate management practices.

During the Y2K review of critical systems and infrastructures, financial institutions got a clear picture of the financial systems' technological dependence, interdependencies across market participants, inherent complexities of operations risk management, and the 'domino' effect of operational risk lapses at a major service provider or material counterparty on all institutions. The knowledge, however, gained during the effort Y2K was not used to identify, measure, quantify, and manage operations risks in later years. Leveraging on past FDICIA efforts would be a prudent business practice with big payoffs for banking managers. World-class financial institutions that review the regulatory overlap, prioritise the inherent risks, leverage past FDICIA efforts to build and streamline enterprise risk management activities will gain investor confidence and competitive advantage. Exhibit 1 graphically depicts the overlapping compliance requirements of FDICIA, SOX, AMA, and BSA/AML.

Revelations of major corporate governance and accounting failures over the past few years have led to questions about the effectiveness of operational and financial reporting, compliance controls, and corporate governance practices. Compliance issues regarding bank lending practices, securities underwriting, mutual funds, stock options, and stock exchanges have caused serious investor concerns worldwide, and have led to companies scrambling to strengthen corporate governance practices and accounting disclosure standards, auditors to tighten the auditing standards, and regulators to impose tighter internal control requirements and stiffer penalties for officers. At the Bond Market Association's Legal and Compliance Conference in 2004, Fed Governor Susan Schmidt Bies cited several compliance problems in financial institutions, and internal control weaknesses causing them. Table 1 shows the lapses in internal control and highlights how enforcing requirements of SOX and BSA/AML based on effective FDICIA certifications on internal controls, and holding executives accountable for their fiduciary responsibilities could have prevented the issues.[11]

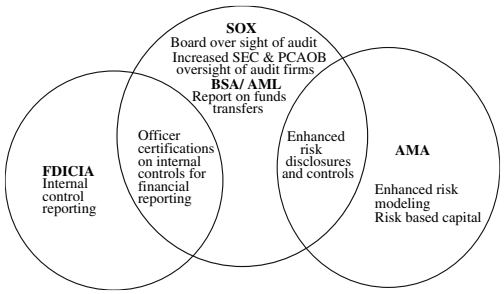

Exhibit 1: Synergies between FDICIA, SOX, BSA/AML, AMA

Recent studies have shown that reporting of material weaknesses in internal control have sizeable adverse impact on the firm's share prices and cut short the tenure of the CFO. Proxy adviser Glass, Lewis & Co analysed data from 899 companies during the period of January 2004 to April 2005 reporting material weaknesses or delaying their 10-K filings, and found that on average the firms lost 4 per cent of their share value. Dutch Consulting firm ARC Morgan in 2005 found that in 60 per cent of the companies disclosing material weaknesses, the CFO was replaced within three months.[12] Most companies reporting weaknesses under SOX have found information technology (IT) to be the prime source of the problem. CFO magazine's 2005 IT survey results showed that 94 per cent of the respondents cited IT control deficiencies

Table 1: Examples of compliance problems uncovered (2004)

Problems uncovered	*Internal control weaknesses*	*Regulation*
Criminals laundering funds through the banks.	Inadequate anti-money-laundering programmes, deficiencies in audit, and management oversight.	BSA/AML, SOX, FDICIA.
False information entered into the records; fraudulent funds transfers.	Failure to segregate duties: inadequate management oversight.	BSA/AML, FDICIA, SOX.
Trading programme with phony trades over a number of years resulting in significant losses.	Inadequate management oversight; compensation structures.	FDICIA, SOX, BSA/AML.
Improper transactions with special purpose entities (SPE).	Inadequate identification and management of risks; inadequate oversight by competent directors.	FDICIA, SOX, BSA/AML.
Complex financial transactions initiated by business-line managers.	Inadequate infrastructure and legal review; compensation structures.	BSA/AML, FDICIA.
Accounting irregularities and resulting financial statements.	Aggressive interpretation of accounting restatement rules; inadequate board oversight.	FDICIA, SOX, BSA/AML.

as contributor to SOX problems, and 49 per cent of the respondents felt that IT issues proved to be a larger part of the overall SOX compliance efforts than they had anticipated.[13] The survey results underscored the importance of IT controls to the overall strength of internal control framework of the firm.

Recognising the impact of IT controls on the overall corporate risk map, the Institute of Internal Auditors has issued an audit guide that focuses on IT controls as part of its Global Technology Audit Guides series to provide baseline knowledge and tools for implementing IT controls in 2005, and the Guide to Assessment of IT (GAIT) general Controls Scope based on Risk in 2007.[14,15] AICPA Annual Top Technology Initiatives Survey of 2007 also identified Information Security management as the # 1 technology initiative with the greatest effect over businesses in the upcoming year for the fifth consecutive year, and IT Governance as the # 6 initiative.[16] The following sections review the evolution and chronology of banking regulations, and role of IT controls in the overall regulatory compliance process. The appendices briefly outline a personal view for implementing enterprise risk management model leveraging on the existing internal control procedures, and other implementation approaches from regulatory publications.

THE NATURE OF BANKING REGULATIONS

The current set of banking regulations are the result of numerous legislative acts and regulatory documents developed over time, often without attention to coordination with earlier regulations. A number of influences have resulted in the current set of banking regulations that are often confusing and conflicting. While each regulation makes sense when examined individually, the total picture is often confusing because the regulations evolved over a long period, and are enforced by many separate government agencies.

Evolution of operations risk management

Operations risk management in financial institutions has evolved over time as FDICIA, SOX, BSA/AML, and AMA and other related regulations took effect. Table 2 shows the evolution of operations risk management over time.

Chronology of the banking regulations

Table 3 outlines the chronology of the regulations resulting from numerous legislative acts and regulatory documents developed over time, often without attention to coordination with earlier regulations. For example, BSA/AML requires banking organisations to develop, implement, and maintain effective AML programmes to address changing strategies of money launderers and terrorists trying to gain access to the US financial system. Enforcement actions in the recent years have, however, largely concentrated on violations on filing timely and accurate suspicious activity reports (SAR) and currency transaction reports (CTR), while ineffective internal control structures, insufficient testing and maintenance of BSA/AML monitoring systems and risk assessments, and inadequate training of personnel are critical issues with potentially higher risk.

Government agencies enforcing banking regulations

Another factor leading to confusing and conflicting regulations for financial institutions is the proliferation of different government agencies having responsibility for implementing the regulations, developing examination guidance, ensuring compliance, and administering sanctions as needed. Some of these international and national government agencies involved in FDICIA, SOX, BSA/AML, and related regulations are listed in Table 4.

As Table 4 indicates, a large number of national and international governmental and regulatory bodies are responsible for overlapping aspects of regulations, and financial institutions must satisfy all relevant bodies in attempting to comply with the regulations. The US Patriot Act/OFAC Guidelines outline

Table 2: Evolution of operations risk management

FDICIA	*SOX*	*AMA*	*BSA/AML*
Scope			
Financial institutions with assets of >$500 million. Excludes bank holding companies and nonbank subsidiaries.	All SEC registrants per Securities Exchange Act of 1934. Includes significant nonbank subsidiaries, but excludes IPOs and other offerings of stock.	Major banking institutions only.	All financial institutions.
Regulatory focus			
Safety and soundness, quality of internal controls.	Quality of internal controls relating to financial reporting and record keeping.	Regulatory capital aligned with the banks' risk management capabilities.	Quality of internal controls relating to regulatory reporting and record keeping.
Executive responsible			
Chief executive officer and line of business managers.	Chief financial officer.	Chief risk officer and operational risk manager.	Chief risk officer.
Baseline	*Awareness and measurement*	*Quantitative analysis*	
Internal controls and reliance on. • Internal audit. • People. • Processes.	Governance structure. Process assessments. Policy. Key Risk Indicators. Event data collection.	Internal and loss databases. Predictive analysis. Risk-based economic capital models. Economic capital.	Internal controls and reliance on. • Internal audit. • People. • Processes.
Responsibilities			
Line of business managers mitigate problems.	Senior management responsible for mitigating problems.	Firm-wide operational risk management function with Board of Directors' oversight.	Firm-wide operational risk control with Board of Directors' oversight.
Reporting	*Monitoring*	*Strategic management*	
Standard reporting. No requirement to report material weakness or deficiencies.	Goals for operations risk management. Consolidated reporting with requirement to report deficiencies and weaknesses.	Correlation between indicators and losses. Insurance linked with risk and capital; Compensation linked to risk-adjusted returns.	Special reporting guidelines.
Regulator			
FDIC	SEC, PCAOB, OCC, FRB	OCC, FRB, SEC	Treasury, OCC, FRB

Table 2: Continued

FDICIA	*SOX*	*AMA*	*BSA/AML*
Stakeholders			
Emphasis on safety and soundness to safeguard Government's interest in the bank.	Shareholders, retirees with 401(k) plans holding the bank's stock, creditors, and employees.	Safety and soundness to safeguard the Government's and shareholders' interest.	Emphasis on safeguarding public and Government's interest.
Report access			
Reports filed with regulators, accessible to public. No interim reports need to be filed.	Reports included in Annual Report on Form 10-K. Management is required to report changes in internal controls quarterly as part of Section 302 requirements.	Reports filed with regulators, accessible to public. Management is required to monitor, assess, and correct internal control deficiencies continuously, and assign operational risk-based capital.	Reports filed with regulators, accessible to public. Management is required to monitor, assess, and correct deficiencies continuously.

specific requirements generally known as the AML and customer identification programme (ALCIP) for enhanced internal control, customer identification, and periodic assessments and reporting (website: www.treas.gov/ofac). Similar legislation was passed by the European Union.[17] These regulations mandate that firms engaging in external financial transactions designate a specific compliance officer who will maintain US Treasury lists of blocked property and blocked transactions, report suspicious transactions, and ensure compliance and reporting consistent with the requirements of the AML laws and regulations. An annual internal review and external audit of the ALCIP policies and procedures must be conducted and reported to the appropriate government agency. The firms are required to respond within 120 hours to requests for information on accounts, monitor and block appropriate accounts, report any suspicious account activity, and collect, verify, and maintain identification information for customers under ALCIP. Clearly the banking institutions need knowledgeable management and compliance personnel to implement sophisticated monitoring and training systems to comply with these requirements, and train employees on the ALCIP requirements.

MANAGEMENT RESPONSIBILITIES AND CHALLENGES

The chief financial officer (CFO) usually has the responsibilities of Treasurer — strategic partner for assisting the profitability and growth of business units, and those of the Controller — internal and external financial reporting, regulatory and tax compliance, and accounting, audit, and other activities designed to ensure the accuracy and integrity of financial information. The finance-related provisions of the Patriot Act in 2001 and related money-laundering legislation in the EU, passage of the SOX in the US in 2002, and related legislation in the EU in 2002–2003 have further emphasised the controller role of the CFO. While SOX has greatly increased the responsibility of the CFO to ensure the integrity of the accounting data used to prepare financial reports with more extensive audit trails and controls, the Patriot Act requires the CFO to ensure better identification of customers and more extensive reporting on unusually large or suspicious transactions. In the post-SOX and BSA/AML era, CFO responsibilities regarding accounting integrity, identification of counterparties, and reporting transactions have greatly increased their reliance on computer information systems and data integrity.

Table 3: A brief chronology of regulations

1970: The Currency and Foreign Transactions Reporting Act commonly known as the '*Bank Secrecy Act*,' establishing requirements for record keeping and reporting by private individuals, banks, and other financial institutions.

1986: *The Money-Laundering Control Act* augmented the effectiveness of BSA. It directed banks to establish and maintain procedures reasonably designed to ensure and monitor compliance with the reporting and record keeping requirements of the BSA.

1991: *FDICIA* required banks to document, evaluate, and report on the effectiveness of their internal controls. Independent accountant must attest to management's assertions about internal controls.

1992: *Annunzio–Wylie Anti-Money-Laundering Act (AML)* strengthened US Treasury's role and the sanctions for BSA violations.

1994: *Money-Laundering Suppression Act (MLSA)* further strengthened the US Treasury's role in combating money laundering.

1996: *Suspicious Activity Report (SAR)* required filings by any US banking organization that detects a known or suspected criminal violation of federal law or transaction related to money-laundering activity.

2001: In response to the 9/11/01 terrorist attacks Congress passed the *Patriot Act*. It augmented the existing BSA framework by strengthening customer identification procedures; required financial institutions to have due diligence procedures, imposed enhanced due diligence procedures for foreign correspondent and private banking accounts; and improved information sharing between financial institutions and the US government.

2002: In response to the public outcry over the accounting scandals, the *Sarbanes Oxley Act (SOX)* was enacted. It required verification of adherence to enhanced financial reporting requirements, audit procedures, board composition etc; Develop process for documenting risks and controls relating to financial integrity; Buy or build supporting information technology; Monitor off-balance sheet transactions and use of SPE.

2003: The Inter-agency Operational risk Supervisory Guidance on Operational Risk Advanced Measurement Approaches (AMA) issued in 2003 is based on Basel II operational risk framework to assign risk-based capital to businesses/products based on internal controls. Banks are expected to: Implement systems and processes to capture and assess operational risks; Develop and refine AMA qualifying capital model for operational risks; Banks adopting the advanced measurement approaches (AMA) and internal ratings-based (IRB) approaches are required to conduct parallel calculations with current accord for 1 year prior to implementation.

The chief risk officer (CRO) is a relatively new role in most financial institutions, and the function is still evolving. AMA and BSA/AML requirements mandate the establishment of CRO function to oversee the integrated enterprise risk management structure including market, credit, operational, legal, and reputation risks. Risks faced by lines of businesses can arise from low probability *and* high loss events, high probability *and* high loss events, or from high probability *and* low loss events, and optimal procedures to manage each of these risk categories can differ greatly among banking institutions. The Patriot Act requires the CRO and CFO to ensure better identification of customers and more extensive reporting on unusually

Table 4: Agencies responsible for enforcing the banking regulations

Federal banking agencies (Board of Governors of the *Federal Reserve* System, Federal Deposit Insurance Corporation (*FDIC*), National Credit Union Administration (*NCUA*), Office of the Comptroller of the Currency (*OCC*), and Office of Thrift Supervision (*OTS*) are charged with chartering, insuring, regulating, and supervising banks. The agencies require each bank under their supervision to establish and maintain compliance programs for the regulations.

Financial Action Task Force (*FATF*), created in 1989 as a part of the US Treasury department, develops and enforces the Anti-money-Laundering regulations procedures and some additional requirements added by the US Patriot Act.

Financial Crimes Enforcement Network (FinCEN), a bureau of US Treasury is the delegated administrator of the BSA. It issues regulations and interpretive guidance, provides outreach to regulated industries, supports the examination functions performed by federal banking agencies, and pursues civil enforcement actions when warranted.

International agencies (various multilateral government bodies that support the fight against money laundering and terrorist financing).

Office of Foreign Assets Control (OFAC) administers and enforces economic and trade sanctions based on US foreign policy and national security goals against targeted foreign countries, terrorists, international narcotics traffickers, and those engaged in activities related to the proliferation of weapons of mass destruction. It has the authority to impose controls on transactions and freeze assets under US jurisdiction. OFAC sanctions are based on United Nations and other international mandates, are multilateral in scope, and involve close cooperation with allied governments. OFAC requirements are separate and distinct from the BSA, but because they share a common national security goal.

PCAOB: Public Companies Accounting Oversight Board (PCAOB) was established under the powers of SOX. PCAOB has the primary authority over accounting and financial reporting standards for public companies. It has oversight responsibilities on external auditors' performance and audit committee responsibilities.

US Treasury: Requires financial institutions (not only banks, savings associations, and credit unions, but also nonbank financial institutions, such as money services businesses, casinos, brokers/dealers in securities, and futures commission merchants) to establish AML programmes, file certain reports, and keep certain records of transactions.

large or suspicious transactions. The challenges created by terrorism and related regulations have greatly enhanced the role and importance of the CRO.

The chief information (technology) officer (*CIO/CTO*) has the responsibility to ensure adequate internal control in operational systems, guard against unintended possible assistance to money-laundering activities or unintended transactions with inadequately identified counterparties. Studies have shown that breaches in computer security in the firm are likely to be punished by investors with a loss in the firm's market value.[18] The CIO faces strategic challenges in focusing on the design of secure and integrated systems to comply with regulations without adversely affecting the firm's product strategies or competitive position. In addition, the CIO has to address tactical challenges such as the hiring, retention, training and deployment of personnel, and adequate disaster recovery and contingency plans.

SOX and BSA/AML requirements have also greatly increased the role and responsibility of the *Board of Directors and Audit Committee*. They require the directors to sign off that they understand the regulatory requirements, and that they plan to oversee management compliance with the regulations. They mandate that the audit committee of the board be responsible for the oversight of the audit and risk management functions of the organisation. The US Department of Homeland Security requires that organisations comply with the Emergency Preparedness and Business Continuity Standard endorsed by the American National Standards Institute (ANSI), and decrees that audit committees and Boards of Directors will face additional liabilities if they ignored this standard. Clearly boards of directors face significant new responsibilities and liabilities, challenging them to look for innovative, holistic, and cost-efficient approaches to enterprise-wide risk management. Since IT controls have significant impact on the overall management of the organisation's internal control and enterprise risk, financial institutions can use IT governance steps by Norton[19] as a model: (1) Organisations need to map critical IT investments to the business strategy, and define priorities for the business units; (2) Board of Directors and management have understanding of the impact of IT on the organisation's operations, and be responsible for IT governance; and (3) Board of Directors and management address information security in the context of the enterprise's priorities, strategies and product requirements, and not solely as a technology issue. Appendix A provides a personal view of the implementation steps for enterprise risk model based on industry experience, and appendices B[20] and C[21] provide brief outline of Charles Schwab's framework for IT governance[22] and high-level overview of the implementation to BSA/AML compliance. Financial institutions can adopt the suggested approaches based on individual competencies and needs.

CONCLUSIONS

Banking managers have the responsibility to manage all aspects of regulatory compliance including the provision of adequate technical and human resources, and providing unambiguous and strategic directives to ensure a robust, integrated risk management platform. In recent surveys, the managers have expressed increased confidence in the accuracy of the financial reports due to SOX, and agreed that the market reward of stock price premium for good governance and tight regulatory controls far outweighs the high costs for SOX implementation. Both the costs for the compliance efforts and the payoffs from standardising and benchmarking of operational risk are substantial due to the complexity involved. Early indications from sophisticated financial institutions that have begun capturing quantitative information about operational risks, measuring and modelling trends and distributions of incidents, and allocating capital based on the risks show that they will enjoy competitive advantage due to lower capital allocation.[23] Since investors have also shown that they expect and reward best-in-class SOX compliance in companies in higher stock prices, managers as agents of the shareholders have an obligation to identify the synergies and leveraging opportunities between FDICIA, SOX, AMA, and BSA/AML compliance, and improve corporate governance. Financial institutions must develop an integrated enterprise risk management framework with a comprehensive assessment of the risks across services, geography, customers, and lines of business, the institution's strengths in personnel and technology, and corporate culture. World-class financial institutions that review the regulatory overlap, prioritise the inherent risks, and streamline enterprise risk management activities will gain investor confidence and move ahead of competition.

Audit committees, Board of Directors, and managers of financial institutions face major challenges in integrating enhanced enterprise-wide risk management, higher levels of IT security, and efficient allocation of resources to

meet the enhanced compliance requirements. They have to ensure that the new corporate strategies to comply with increased regulations also result in better management of customer relationships and enhanced long-term shareholder value. These challenges have both short- and long-term implications. While the implementation of a holistic, robust enterprise-wide risk management system can be expensive and time consuming in the short run, it will pay long-term dividends in competitive advantage and higher shareholder value.

References and Notes

1 Cocheo, S. (2005) 'SOX 404 soaks some, leaves others grateful for respite', *ABA Banking Journal*, **97**(April), 63–66.
2 Batts, N. (2005) '404 means huge costs for questionable gains', *American Banker*, **170**(82, 29 April), 1–12.
3 Harrington, C. (2005) 'The value proposition', *Journal of Accountancy*, **200**(3), 77–81.
4 CFO Research Services (2005) 'Compliance and Technology: A Special Report on Process Improvement and Automation in the Age of Sarbanes–Oxley', CFO Publishing Corp, Boston, MA.
5 Durfee, D. (2005) 'By the numbers: The 411 on 404', *CFO*, **19**(September), 28.
6 Garver, R. (2006) 'Operational risk: Who is making progress', *American Banker*, **171**(5 May), 912.
7 Adams, J. (2007) 'Leveraging compliance: Following the rules can really pay off', *Bank Technology News*, **20**(1 February), 30–32.
8 Krell, E. (2006) 'The risk-intelligent company', *Business Finance*, **12**(October), 39–42.
9 Federal Financial Institutions Examination Council (FFIEC) (2005). *Bank Secrecy Act/Anti Money Laundering Examination Manual*, US Govt. Printing Office, Washington, DC.
10 Basel Committee on Banking Supervision (2003). *Initiatives by the BCBS, IAIS and IOSCO to Combat Money Laundering and the Financing of Terrorism*, BCBS, London.
11 Bies, S. S. (2004) 'Vital speeches of the day', *Current Issues In Corporate Governance*, **70**(14, 1 May), 424–429.
12 Durfee, D. and Ronald, F. (2006) 'The future of reporting, reader survey: Progress report', *CFO*, **20**(September), 52–53.
13 Anonymous (2005) 'Survey says….Sarbox & IT: How bad can things get?', *CFO-IT* (Summer), 56.
14 Institute of Internal Auditors (2005). *Global Technology Audit Guide: IT Controls*, IIA, Altamonte Springs, FL.
15 Institute of Internal Auditors (2007). *Guide to the Assessment of IT (GAIT) General Controls Scope Based on Risk*, IIA, Altamonte Springs, FL.
16 American Institute of Certified Public Accountants (2007). *Annual Top Technology Initiatives Survey*, AICPA, New York.
17 Buck, T. (2005) 'New money laundering legislation puts extra onus on EU professions', *Financial Times* (27 May), 4.
18 Rapoport, M. (2005) 'Companies pay a price for security breaches', *Wall Street Journal* (15 June), C3.
19 Norton, D. (2002) 'The alignment enigma', *CIO Insight*, **15**(Special Issue), 12–14.
20 Federal Financial Institutions Examination Council (FFIEC) (2003) 'Interagency statement: Supervisory guidance on operational risk: Advanced measurement approaches for regulatory capital', *Federal Register*, **68**(149, 4 August).
21 Aggarwal, R. and Raghavan, K. (2006) 'Management and board challenges complying with bank secrecy act and money laundering regulations', in Benton, E. Gup (ed.) *Money Laundering, Financing Terrorism and Suspicious Activity*, Nova Science Publishers, New York.
22 Damianides, M. (2004) 'Sarbanes Oxley and IT governance: New guidance on IT control and compliance', *EDPACS*, **31**(10), 1–14.
23 Ernst and Young (2004) 'Audit committees and the war on terror', *Board Matters Quarterly*, **2** (December), 7–8.
24 Bank for International Settlements (2004). *Basel II: International Convergence of Capital Measurement and Capital Standards: A Revised Framework*, BIS, London.
25 Office of Comptroller of the Currency (1999). *Infrastructure Threats from Cyber Terrorists*, US Govt. Printing Office, Washington, DC.

Appendix A

PERSONAL VIEW FOR IMPLEMENTING OPERATIONS RISK MODEL

The Basel II Sound Practices,[24] SOX requirements, and the Supervisory Guidance on AMA Guidelines have been major drivers of improvement in governance and operational risk management in banks worldwide. They provide the tools to enhance and protect shareholder interests by analysing the institution's risk profile quantitatively, and allocating risk-based capital. These new internal control and governance measures are slowly getting integrated into the activities of the banking institutions while holding the executives accountable for compliance. An implementation model for operations risk management model is given below based on my personal view and industry experience:

- Ensure a strong commitment from executive management to process improvement in the form of financial and organisational resources. Establishing a central oversight body, clear communication channels across organisational units about the responsibilities and accountability of individual managers, commitment to remediation and enforcement of control procedures, and a corporate culture of continuous process improvement are essential success factors to this effort.
- Assemble a central task force of personnel resources with expertise in operations risk management process including the identification and measurement of operational risks, and developing a robust model to allocate risk-based capital to the lines of businesses/products.
- Identify the corporate strengths and weaknesses, competing priorities, core competencies, and expected deliverables. Apply project management techniques to establish realistic project timeline and budget, and obtain necessary capital project approvals.
- Obtain approval from the executive management and Board of Directors on the proposed project plan. Establish project milestones and frequency of reports.
- Establishing clear communication about the project deliverables and expected benefits to the organisation, and management incentive systems structured to promote compliance will ensure buy-in from the business unit managers.
- Form a task force consisting of representatives from across the organisation with deep understanding of the core competencies, operational procedures, controls, and quantitative disciplines to guide the implementation process. The task force can morph into a standing committee with responsibilities for oversight and review in the post-implementation phase.
- Using the existing FDICIA compliance database, collect operational loss data and exposures, and scenarios and self-assessments from the lines of business management to build an internal database. Review the granularity of loss and risk data based on the type of business.
- Develop definitions and specifications for industry-wide key risk drivers and key risk indicators (KRI) for each risk type. The Guidelines for SOX and FDICIA compliance can be used as the basic framework.
- Participate in industry-wide task forces and organisations to gain access to external data. To adequately represent the rare loss events that occur infrequently within any organisation, industry-wide external data needs to be added to the database. Review and resolve issues on reliability of data, consistency in classifications and data capture bias between institutions.
- The model should consider 'goodness-of-fit' tests to the data. If data are limited, employ techniques such as 'bootstrapping' to create multiple distributions for analysis. Use statistical techniques such as Monte Carlo simulation, Bayesian modelling, causal modelling, and actuarial approach

for risk quantification based on available resources.

- Design and implement effective management compensation systems based on the line of business' level of risk and compliance with operational risk management policies.
- Establish a standing committee with responsibilities for oversight of the database and the enterprise risk model to ensure that they are updated for changes in products, customers, and lines of business. The committee will consist of representatives from business units across the organisation that can be considered 'subject experts'.
- Establish a corporate executive-level position with responsibility for review and oversight of enterprise risk management, authority to mandate remediation for control lapses. This executive is responsible to provide reports and information related to the corporate governance responsibilities of the Board of Directors and the Audit committee.
- The project task force can morph into a standing committee with responsibilities for oversight and review in the post-implementation periods.

Appendix B

CONTROL FRAMEWORK FOR IT GOVERNANCE

The IT Governance Institute developed the Control Objectives for Information and Related Technology (COMT) when COSO framework was first introduced. Over the years, CoBIT (Control Objectives for Information and Related Technology) Management Guidelines were developed, and CoBIT is recognised globally as the IT governance and control framework. It is accepted by organisations worldwide, and provides necessary information for management to provide reasonable assurance of the IT control structure and information integrity for Section 404 of SOX. Charles Schwab Co. use of CoBIT framework for IT governance can serve as a model for other financial institutions: map CoBIT domains and control objectives to the FFIEC IS Examination Handbook Guidelines for financial institutions; map the audit universe to CoBIT control objectives; map audit strategy, objectives, and scope to CoBIT control objectives; develop and administer CoBIT control assessment questionnaires to evaluate the effectiveness of existing controls, and detail the risk mitigation plans for areas with control deficiencies; evaluate the effectiveness of existing controls for each area and document the results using COBIT maturity Guidelines; analyse, document, and validate results; and present results in an audit report issued to senior management and appropriate committee of the Board of Directors.

The technology infrastructure has been identified as one of the most vulnerable areas in banking institutions. The steps outlined by Office of Comptroller of the Currency in March 1999[25] to combat infra-structure threats from cyber-terrorists can serve as a model in implementation of the operations risk management model: install a strong intrusion detection system that is resistant to outside attacks. The system should be reviewed periodically; develop definitions and specifications for industry-wide key risk drivers and KRI for each risk type (the Guidelines for SOX and FDICIA compliance can be used as the basic framework for this effort); implement disaster recovery plans that are regularly tested and updated; maintain adequate expertise to administer, secure, and monitor network security; plan network design and architecture in terms of connectivity, key components, and firewalls; implement physical security programme to control access to computing and information resources; turn audit trails on; encrypt files and transmissions; incorporate logical access controls to information resources; conduct regular background checks of employees in sensitive positions; report significant unauthorised access attempts; communicate with peers about best practices; collect operational loss data and exposures, and

management scenarios and self-assessments from the lines of business, to build an internal database; commit enough financial resources to operations risk management process including the identification and measurement of operational risks, and developing a robust model to allocate risk-based capital to the lines of businesses/products; design and implement effective management compensation systems based on the level of risk management in the business.

Appendix C

IMPLEMENTATION APPROACH TO BSA/AML COMPLIANCE MODEL

The BSA/AML examination manual provides a detailed discussion of the requirements for compliance in specific areas such as correspondent banking, electronic banking, funds transfers, brokered deposits, ATM's, private banking, trust, investment management, and others. Appendix J in the manual identifies 'Quantity of Risk Matrix', and areas identified as 'high risk' (trust, investment, electronic banking, secured lending, brokered deposits, etc). It provides a roadmap for institutions to focus their own efforts and resources by comparing the internal risk assessments to regulators' perceptions of 'high-risk' businesses and activities, and take any remedial action as needed in the BSA/AML compliance structure. A high-level overview for developing a comprehensive BSA/AML compliance structure is given below.

- Perform due diligence based on customers and activities, and assign scores based on the risk profiles, similar to credit scores. Identify high-risk business activities, money service businesses, validate names against 'terrorist-related' lists from the government databases.
- Develop, test, and continuously enhance internal control systems tailored to the risk profiles of specific banking activities. In addition to the annual audit, have the system tested by independent experts on a periodic basis.
- Establish continuous monitoring of control systems charged with reviewing and reporting of money-laundering activities. Develop/purchase software to identify customer activity patterns, to be able to detect anomalies. Develop/contract forensic examination capabilities.

