

A Framework for Governance, Risk Management and Compliance

By Tom Grubb and Tom Burke

Compliance and operational improvements are complementary and should happen in tandem.

Compared to other industries, banks do quite well in security governance and risk management. A November 2007 report by the Aberdeen Group, *Security Governance and Risk Management: The Rewards of Doing the Right Things, and Doing Things Right*, found that financial institutions are ahead of the pack in several important aspects of security governance and risk management. We believe that, therefore, banks and financial institutions also have a leg up when it comes to the broader topic of regulatory compliance.

It doesn't matter if we're talking about the relatively circumscribed realms of the Sarbanes Oxley Act of 2002 or if we're dealing with a much bigger picture. That big picture encompasses all the considerations that bankers must weigh as they endeavor to comply with literally hundreds of government regulations, industry standards and best business practices.

This article summarizes highlights of the Aberdeen report, shows how financial services firms stack up against the rest of the world in the security realm and describes how financial institutions can transfer those capabilities to succeed in governance, risk management and compliance (GRC).

Characteristics of the Best-Performing Companies in the Area of Security and Risk Management

The Aberdeen survey results show that the firms enjoying best-in-class performance shared several common characteristics, including the following:

- Seventy percent have established consistent security and compliance policies.
- Seventy percent have a responsible executive or team with primary ownership for security governance and risk management.
- Fifty-two percent have visibility into key information required to manage their security and compliance processes.
- Seventy-eight percent keep management accurately informed of information technology (IT)-dependent risks.
- Sixty-seven percent have implemented controls to monitor and verify that requirements of internal policies and external regulations are being satisfied.
- Sixty-seven percent have identified all information required for auditing and reporting.

Consistent with previous Aberdeen research, the leading driver of current investments in security governance and risk management was "compliance," taken in all of its dimensions—including compliance with government regulations, industry standards and best practices, industry regulations and internal policies.

Therefore, this report on information security has a high degree of applicability to the more comprehensive area of GRC. Banks are ahead of the curve in security governance; that gives them a leg up in the broader GRC arena.

Tom Grubb is Vice President of Polivec Inc., Mountain View, California. Contact him at tgrubb@polivec.com. Polivec was one of the sponsors of the Aberdeen research report.

Tom Burke is Vice President at Graber Associates, Burlington, Massachusetts. Contact him at tom@graberassociates.net.

In addition, the best-in-class organizations are the furthest along the continuum from initial achievement of compliance to the development of a sustainable, continuous compliance infrastructure through automation and streamlining of business processes to ensuring that their investments in security and compliance controls directly support their business objectives.

The Aberdeen survey found that financial services organizations are ahead of other industries in security governance and risk management (Exhibit 1).

Identifying External Forces

The Aberdeen study found that banks have more confidence than companies in other businesses in their ability to identify external forces that affect an organization's market position, competitiveness or business operations.

Banks are just slightly better than the average in identifying appropriate government regulations (67 percent to 65 percent) but are significantly ahead of

the pack (50 percent to 30 percent) when it comes to pinpointing industry regulations that must be heeded. This is not surprising, given that the banking regulatory burden is as onerous as that of any vertical segment.

Perhaps more important to our discussion of GRC aptitude among banks is the third example in this category: that banks are better than most at identifying the industry's best practices and standards (28 percent to 19 percent).

Establishing Consistent Policies and Procedures

Aberdeen's research indicates that 72 percent of banks have established and enforced consistent security policies and procedures, versus 63 percent of the companies surveyed.

Michael Mullins discusses this succinctly in an April 2007 article in *TECHREPUBLIC*: "Many organizations approach compliance from the wrong

Exhibit 1. Financial Services Companies Ahead in Security Governance and Risk Management

	Overall Average	Banks and Financial Services Firms
PRESSURES		
Government regulations	65%	67%
Industry regulations	30%	50%
Industry best practices and standards	19%	28%
STRATEGIC ACTIONS		
Establish and enforce consistent policies and procedures	65%	72%
CAPABILITIES		
Responsible executive or team with primary ownership	63%	71%
Visibility into key data required to manage processes	34%	39%
Management accurately informed of IT-dependent risks	50%	65%
Controls to monitor and verify that requirements of internal policies and external regulations are being met	41%	50%
ENABLING TECHNOLOGIES		
Risk management solutions or services	36%	38%
GRC solutions or services	13%	17%

Note: The responses from the study's industry average maturity class (the "middle 50%" of all respondents, based on reported performance) are compared to the responses from the banking and financial services industry segment. For example, 65% of the industry average identified "establish and enforce consistent policies and procedures" as a leading strategy, compared to 72% of banks who responded to the survey. Doing cross-tabs and comparisons between any given segment and the industry average allows for the most meaningful comparisons. Since many banks are in fact in the top 20% best-in-class category, but do not comprise the entire best-in-class category, comparing banks to the best-in-class might give the inaccurate impression that their performance was somehow suboptimal.

angle. They make the mistake of looking at the multitude of regulations and trying to decide: Are we compliant? But that's not the right question. What companies really need to be asking is: Are our policies compliant, and do we follow our policies? Stop chasing compliance by implementing new security technologies, security devices, and/or security controls; instead, address the issue where it belongs—in your security policies.”¹

Banks and financial institutions are used to setting consistent policies, which really amount to high-level direction. Policies impart general guidance and do not have to change very often if they don't mention specific rules and technologies. Procedures change when the environment evolves, but the policies remain the same.

Mullins gives the following example

Don't write an IT security auditing policy that states, “Retain all electronic logs that contain records of system or file access for a period of three years”—you don't need to be that specific. Your overall security policy should state, “Retain records of all authorized and unauthorized access to business resources, systems, and processes.” You've taken technology out of your policy and addressed compliance as an overall business process.

Putting Compliance into Action

Conventional wisdom holds that Enron had a comprehensive, well-written policy manual. Enough said. You have to back up policies with action, corporate commitment and enforcement. Here again, in a number of key aspects, banks compare favorably to companies in other industries.

CFO Should Take Charge of Compliance

In an August 2007 compliance survey to which 129 companies from a variety of industries responded, Polivec learned that the responsibility for compliance still rests in any number of places. The bulk

of the answers to a query on what department handles compliance were roughly evenly divided among executives, finance, human resources, legal and “other.”

Polivec believes that the CFO is the best one to take charge of compliance and that he or she should build a team that will do the actual work of directing and managing it. There must be an enterprise-wide perspective of compliance, because compliance affects every employee or worker to some extent.

Take a Big-Picture View, but Start Small

Organizations that are well on their way to compliance success have an enterprise-wide approach and are focused on streamlining of processes. Paradoxically, they approach compliance with a “crawl, walk, run” philosophy. That is, they solve one problem at a time, learn from it and apply their improved techniques to the next problem. For the first project, banks should pick a topic that touches the organization as broadly as possible but can be implemented without too much disruption to the business.

Regulations Must Map to Work Rules

Banks also beat the Aberdeen averages in their use and handling of information. They do a better job (39 percent to 34 percent) at gaining visibility into key data for management decisions. They also accurately inform management of IT-dependent risks (65 percent to 50 percent).

The visibility of key data for compliance should include linking or mapping the regulations and their requirements to the business and work rules where the actual work of compliance takes place. Most organizations that are moving toward compliance proficiency still have a way to go in this regard. Especially if they rely on spreadsheets, manual checklists and hard copy distribution of policy updates, organizations of all types are finding it difficult to keep their policies current and keep their employees fully informed about changes and updates. Automation is the answer here, and as we will see, it holds the most promise for bringing additional efficiencies.

As one general manager quoted by Aberdeen said, "These manual systems are *documenting* a lot of stuff. But can they really *drive* any effective behavior?"

Banks Must Verify That Requirements Are Met

In the Aberdeen survey, by a 50 percent to 41 percent margin, banks have controls in place to monitor and verify that policies and external regulations are being satisfied. They know the importance of checking up and verifying what is happening throughout their organizations when it comes to data security. This capability positions the banks well for the entire GRC function.

In a survey of compliance professionals taken by Polivec at the October 2007 annual conference of the Ethics and Compliance Officers' Association, more than half (51 percent) of respondents indicated that the most important key to job success is making sure that the company is actually following all applicable laws.

Following the laws means that employees throughout the organization are performing their duties correctly and that those duties are in compliance with the company's policies that, in turn, are developed in a manner that will lead to compliance with the laws. Before that happens, of course, employees need to understand what they are doing and why. There is a need to overcome what Peter Williams of Bloor Research describes as "a major disconnect between those tasked with defining the high-level policies and those down in the 'engine room' who have to implement them within their infrastructure."²

This will always be a concern, given that employee populations wax, wane and turn over with regularity and that rules and policies are always subject to change. Here again, automation of the continuing education of employees holds much promise.

Case Study: Banco Santander International

Banco Santander International recognized its numerous regulatory and reporting compliance requirements and developed a set of best practices for compliance. Based in Miami, Santander is a client of

Polivec, Inc., a GRC solution provider that was one of the sponsors of the Aberdeen research report.

Santander had been using a paper-based system attempting to keep track of its success in complying with directives of the Federal Financial Institutions Examinations Council (FFIEC), the Patriot Act, the Bank Secrecy Act and others. Using spreadsheets and folders to track its 500 employees' performance had become too cumbersome. The bank first zeroed in on FFIEC compliance, its most time-consuming regulatory activity. It employed an automated, Web-based system to centralize all the bank's *policy* documents and then distributed electronic copies of current policies to the employees who were required to adhere to them.

Once the bank's senior managers were satisfied that all FFIEC-related tasks were being performed and were able to report that performance to auditors and regulators, the bank automated the tracking of compliance with additional banking regulations, with the bank's own procedures for operations and information security and with laws and internal procedures in the human resources area.

But Santander set out not merely to substitute an electronic tracking system for a paper-based one. The bank sought to change behavior. Santander's CIO, Gus Abalo, remarked, "Banking is ... always about improving efficiency to be ahead of the competition. Regulatory compliance is an important part of the overall expenses of the bank, and the fastest growing one To achieve efficiencies you have to change the way people work."

Before Banco Santander could automate its compliance function, "We needed to make our policies visible to the entire organization," said Santander's Bill Josepha, chief information security officer.

Abalo explained further, "By bringing transparency to the entire process of compliance we can effectively mitigate the risks posed by failing to comply with policies and regulations. In essence, we made our policies come alive."³

Adopting Technology to Advance GRC Efficacy

The Aberdeen survey notes that banks are just about at the industry average in the adoption of a technology platform geared to GRC. When asked

about GRC solutions or services, 17 percent of banks responded affirmatively versus the average of 13 percent. As for risk management solutions or services, it was banks 38 percent, average 36 percent.

Polivec's August 2007 survey of 129 companies found that, to date, many approaches to managing compliance have been tried, with varying degrees of effectiveness. "Point solutions" and ad hoc, manual methods still predominate, effectively keeping the compliance function in organizational silos that hamper a coordinated compliance strategy. Manual systems (55 percent), folders (57 percent) and spreadsheets (61 percent) all outrank technology and software solutions (45 percent), as does "not sure" at 57 percent. So the executives surveyed here also displayed a considerable lack of knowledge of what is being done, if anything.

Next Steps for Financial Institutions

Banks' capabilities in security and risk management position them to stop treating compliance in a reactive, ad hoc manner and start asserting control of it through establishing "a sustainable 'continuous' compliance infrastructure through automation and streamlining of business processes."⁴

What the banks can do to maintain and lengthen their lead is clear. Per Aberdeen, "The emerging opportunity here is to leverage the automation of controls and the centralized collection, normalization, and correlation of security and compliance information to establish a consistent, unified view of risk and compliance information across the organization."

Derek Brink, Aberdeen's vice president and research director for IT security and the author of the study, notes that "Addressing and sustaining compliance in today's environment calls for a committed program, not a series of one-time events."

Endnotes

- ¹ Michael Mullins, CCNA MCP, *Take Technology Out of Your Security Policies to Maintain Compliance*, TECHREPUBLIC, Apr. 12, 2007.
- ² Peter Williams, Senior Analyst, Bloor Research, *The Case for Converging Governance, Risk and Compliance*, IT Director.com, Aug. 29, 2007.
- ³ Polivec, Inc., *Banco Santander International Case Study*, www.polivec.com/index.php/resources/, July 2007.
- ⁴ Aberdeen Group, *Security Governance and Risk Management: The Rewards of Doing the Right Things, and Doing Things Right*, Nov. 2007, available at www.aberdeen.com/summary/report/benchmark/4446-RA-security-risk-mgmt.asp.

This article is reprinted with the publisher's permission from **Bank Accounting & Finance**, a bimonthly journal published by CCH, a Wolters Kluwer business. Copying or distribution without the publisher's permission is prohibited.

To subscribe to **Bank Accounting & Finance** or other CCH Journals please call 800-449-8114 or visit www.CCHGroup.com.

All views expressed in the articles and columns are those of the author and not necessarily those of CCH or any other person.