

# IT Automation and Integrated Compliance

By Jim Hietala

*Challenges of assuring compliance when myriad third-party vendors are involved.*

Financial organizations are subject to numerous regulations and standards, including Gramm-Leach-Bliley (GLBA), Sarbanes-Oxley (SOX) and, in many cases, the Payment Card Industry Data Security Standard (PCIDSS). Industry regulators are challenging financial institutions regarding their risk-management practices and, specifically, their ability to understand and manage risks inherited from third-party service providers. Common problems in risk assessment and compliance management include the amount of manual effort typically required to carry out risk assessments and the lack of program effectiveness when done manually using spreadsheets and email.

In addition, many financial organizations are subject to multiple compliance regulations, including GLBA, SOX and PCIDSS. The sheer number of third-party vendors for many large banks presents a scaling issue for risk-assessment and compliance programs. The Financial Services Roundtable/BITS shared assessments initiative is developing standards for risk-assessment practices in the financial industry. In addition, a unified approach toward compliance with multiple regulations offers the possibility to both reduce costs and increase program effectiveness (see *Integrating Compliance for Efficiency* on page 33 in this issue).

## General Compliance Challenges

In a world where the amount of regulatory oversight has increased dramatically, developing and maintaining compliance presents some real challenges:

- The cost of compliance efforts has skyrocketed. In 2005, businesses spent an estimated \$15.5 billion on compliance-related activities.<sup>1</sup>
- In industries affected by multiple regulations, a schedule of overlapping and redundant activities is required to achieve and maintain compliance.
- There is a lack of a clear, unambiguous industry standard reference for mapping compliance regulations to security standards, such as ISO 17799 and NIST 800-53, and to the more detailed security controls implemented within an organization.
- Few information technology (IT) environments are static for long. While initially perceived by many to be a onetime event, compliance activities are now becoming a recurring task because of the constant change in the IT and business environment at most large organizations.
- Large corporations are spending far more on audits than planned. A recent study indicated that large firms spent an average of \$2.4 million more than they had planned on audits in 2004. It is fair to assume that the overruns were primarily caused by an expectation mismatch between the audit expectations and the way in which compliance was managed by the corporation. This is particularly true for SOX compliance.<sup>2</sup>

---

*Jim Hietala is Director of Product Marketing at ControlPath, Englewood, Colorado. Contact him at [jhietala@controlpath.com](mailto:jhietala@controlpath.com).*

## Regulatory Compliance Challenges in the Financial Industry

Financial organizations in particular face a complex regulatory environment. The overarching regulation affecting financial firms of all sorts is the GLBA.<sup>3</sup> At a high level, GLBA requires financial organizations to provide protection for their customers' nonpublic personal information, including account numbers, social security numbers and account balances. Enforcement of GLBA is left to various regulatory agencies depending on the type of financial organization. Regulatory agencies with oversight and enforcement responsibilities for GLBA include the following:

- Office of the Comptroller of the Currency (OCC) and Federal Deposit Insurance Corporation (FDIC), responsible for national banks
- Office of Thrift Supervision (OTS), responsible for savings and loans
- Federal Reserve System (FRS), responsible for FRS banks
- National Credit Union Administration (NCUA), responsible for credit unions
- Securities and Exchange Commission (SEC), responsible for brokerages and investment banks, mutual funds
- Federal Trade Commission (FTC), responsible for all other financial firms, including mortgage issuers and brokers

What are the sources of risk that financial organizations need to concern themselves with? Risks can be categorized in many ways, but a useful first distinction is to divide them into risks that affect internal business assets and risks that arise from outsourcing business processes. While it is convenient to discuss these as separate types of risks, they are frequently interrelated. For firms that do significant outsourcing, internal risk assessments often need to be matrixed to external service providers and outsourced business functions.

Because GLBA is high level and not prescriptive, the Federal Financial Institutions Examination Council (FFIEC, comprised of several of the regulating agencies noted above) created the Interagency Guidelines,<sup>4</sup> very specific requirements around IT security and risk assessments. These

guidelines include numerous specific standards to be implemented in support of safeguarding customer information. They give guidance to financial institutions regarding the use of physical security controls, encryption, logical access controls, malicious code and malware, personnel security, business continuity and disaster recovery and many other aspects of information security.<sup>5</sup>

The guidelines specifically require that financial institutions do the following:

- Exercise due diligence in selecting service providers.
- Require service providers by contract to implement appropriate measures designed to meet the objectives of the guidelines.
- Monitor service providers to confirm that they have satisfied their requirements, including auditing the providers, obtaining summaries of test results and other evaluations.

The FFIEC has published further guidance in an update to the IT Examination Booklet (June 2004) dealing specifically with outsourcing technology services.<sup>6</sup> This addendum places responsibility for managing outsourcing risks with the financial institution's board and senior management. The addendum specifies how financial institutions are to perform risk assessments:

- Financial institutions must gather data regarding the information and technology assets of the organization, threats to those assets, vulnerabilities, existing security controls and processes and the current security standards and requirements.
- Financial institutions must analyze the probability and impact associated with the known threats and vulnerabilities to its assets.
- Financial institutions must prioritize the risks present due to threats and vulnerabilities to determine the appropriate level of training, controls, and testing necessary for effective mitigation.

The guidance also directs financial institutions to evaluate the adequacy of their providers' internal and security controls and to conduct regular, comprehensive audits of the service provider relationships. In addition, "financial institutions have a legal responsibility to ensure that service providers take appropriate measures designed to meet the objectives of the information secu-

rity guidelines, and comply with GLBA sections 501 (b).” This guidance extends the mandatory security measures proscribed by GLBA and the Interagency Guidelines to the service providers and makes the financial institution legally responsible for ensuring that these security controls are in place.

As regards service providers to financial institutions, other regulatory guidance as to the requirements to assess risks from these relationships is found in the Bank Service Company Act, 12 USC §§1861–67(c).<sup>7</sup> This act also extends the regulators’ oversight of financial institutions to include their third-party service providers.

Regulators in the financial community are increasingly insisting that financial institutions can outsource the function but not the risk. In other words, the financial institution has the obligation to assess and understand the risks that it inherits from third-party service providers and to effectively manage these risks. Regulators look at various kinds of risks that arise from third-party service providers, including the following:

- **Strategic risk**—the risk to earnings or capital arising from adverse business decisions or improper implementation of the decisions.
- **Reputation risk**—the risk to earnings or capital from negative public opinion. Adverse consequences in this category can arise from poor customer service provided by the third party, which reflects negatively on the financial institution. Reputation can also be negatively affected in the event of a security breach that is experienced by the third-party service provider and that affects the financial institution’s customers.
- **Compliance risk**—this is the risk to earnings or capital that occurs from violations of laws, rules or regulations.
- **Transaction risk**—this is the risk to capital or earnings arising from problems in service or product delivery.
- **Credit risk**—these risks are associated with a service provider’s failure to meet the terms of its contract with the financial institution or to otherwise perform as agreed.
- **Other risks**—country risk (economic, social and political risk) may be a concern when dealing with outsourcers in foreign countries.

Regulators expect the management team of the financial institution to understand, manage and mitigate these risks.

Many financial institutions are also involved with credit cards, either as issuers of cards or as merchants processing card transactions. The payment card industry has promulgated its own standard (PCIDSS<sup>®</sup>) for data security, again aimed at providing protection for consumer data. While not a government regulation, PCIDSS compliance is mandatory for all credit card merchants and processors. The payment card standard is highly specific about oversight and assessment—depending on the size of the firm, quarterly network scans and annual assessments by a qualified data security consultant are required. The payment card industry also has fines and other penalties for noncompliance, including the potential loss of a merchant or processor’s ability to process card transactions.

The challenge of managing risk and ensuring compliance with multiple regulations is considerable (see *Integrating Risk, Compliance and Control for Efficiency ... and Effectiveness* on page 33 in this issue). Consider a financial institution that is an issuer of credit cards and that outsources customer support to a business process outsourcing firm in the Far East. In accordance with regulatory requirements, the firm will have to assess internal risks and ensure that appropriate internal security controls are in place to protect access to consumer data. In accordance with the provisions of PCIDSS, the financial institution will have to ensure that a separate set of security controls are in place and adhered to, to protect credit card data. Because the financial institution is outsourcing customer support, it will have to assess risks and evaluate controls that are in place at the outsourcing partner. And it will have to evaluate the service provider for the core GLBA and Interagency Guidelines requirements and then also evaluate the service provider against the PCIDSS requirements. For firms that undertake compliance using separate silos and separate projects, these efforts are likely to be redundant and costly. From the service provider perspective, they will have to deal with multiple assessments (one per regulation) from each of their clients.

## Financial Industry Approach to Risk Assessment

---

The banking and financial services industry is taking an innovative approach to the risk-assessment process for third-party service providers. Service providers to financial institutions are frequently faced with completing “similar but different” assessment questionnaires from their financial institution customers. The current state of the industry is such that there is a tremendous amount of redundant effort associated with responding to these individual risk assessments.

An independent nonprofit financial industry consortium, BITS<sup>9</sup> (a part of the Financial Services Roundtable), is developing and publishing standard assessment questionnaires for use by banks in assessing risks from their third-party service providers. The Standardized Information Gathering questionnaire (SIG) was developed by a BITS work-

ing group comprised of financial institutions, service providers and audit firms. The SIG contains approximately 1,600 specific questions aimed at assessing risk across various areas of the business relationship, including technical security controls, disaster recovery plans and the financial stability of the partner. BITS has also developed a set of agreed upon procedures (AUP) that constitute a set of standard controls to be utilized by service providers to reduce risk. In effect, the AUP are a set of best practices for financial organizations.

BITS released the 2.0 versions of the SIG and AUP in July and October 2006. The BITS standards are freely downloadable and usable by end users,<sup>10</sup> regardless of their membership status in BITS and the shared assessments program. In addition, the BITS intellectual property may be licensed by developers of risk and compliance software.

The BITS shared assessment program seeks to drive efficiencies for both financial institutions and service providers through the use of these standard assessments. The benefits of this program to both service providers and financial institutions will be considerable. For service providers, the results of their SIG assessment will be reusable (at their discretion) to fulfill additional assessment requests from other financial institutions.

## Building a Unified Compliance Process

---

A recent survey of 132 IT executives by ControlPath<sup>11</sup> found that 70 percent of respondents use different projects to address multiple compliance regulations. In addition, the survey found that 74 percent of respondents are dealing with compliance in a manner that is either entirely manual or mostly manual.

This suggests that most organizations have a long way to go in creating an optimized compliance and risk-management program.

One challenge in optimizing compliance and risk management is that many regulations are high level and not detailed enough to allow organizations to easily

measure their compliance status or to manage their progress. The same survey by ControlPath found that more than 70 percent of respondents complained that a lack of education on compliance and a lack of

---

*70 percent of respondents use different projects to address multiple compliance regulations.*

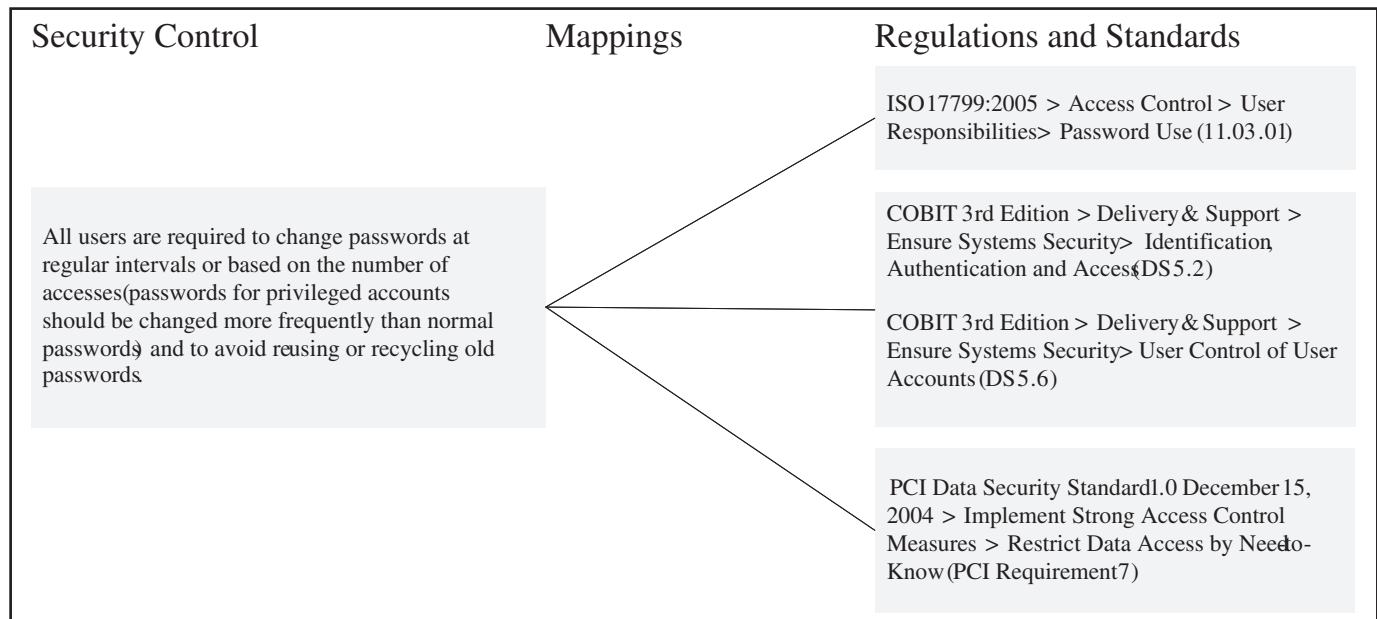
---

detail in the regulations were impediments to achieving compliance. What is required is the creation of more granular controls that are specific and measurable. Forward-thinking organizations are starting to move aggressively to build a better compliance architecture by creating a unified compliance process capable of assessing both internal assets and third-party service providers in a single process. Such a unified approach will allow more granular controls to be mapped to the various regulations. One example of a control mapped to several regulations is depicted in Exhibit 1.

Once the controls are mapped to the relevant regulations, it is straightforward to perform assessments and to automatically report the results against each regulation simultaneously. This allows a single compliance and risk management program and process to support all regulations affecting the business.

To the extent that automation is applied to the unified compliance process, further benefits can be realized, including greater program effectiveness and significantly reduced costs for manual labor. Increases in program effectiveness are possible because automated compliance systems typically use extensive work flow to ensure that assessment and remediation tasks are completed, with automatic reminders and escalations

Exhibit 1. A Control Mapped to Several Regulations



being sent as necessary. Reductions in labor costs can be significant as well, because the automated system and work flow can more efficiently track activities and can automatically develop status reports.

## Conclusion

The financial industry has long been highly regulated. The recent surge in IT security breaches and the continued growth in outsourcing of critical business processes have caused financial regulators to heighten their oversight of financial institutions and to pay particular attention to the risks that are inherited from each outsourcing relationship.

Recent progress by BITS in developing standards for third-party risk assessment is a welcome development for financial institutions and service providers alike, as they provide a standard approach that can ease some of the pain of frequent and redundant risk assessments. In addition, progressive organizations are developing unified and automated compliance programs that can enable simultaneous risk assessment and compliance

against multiple regulations and standards, at a greatly reduced cost to the organization.

## Endnotes

- <sup>1</sup> AMR Research, *Spending in an Age of Compliance*, 2005.
- <sup>2</sup> Financial Executives Institute.
- <sup>3</sup> [www.ftc.gov/privacy/privacyinitiatives/glbact.html](http://www.ftc.gov/privacy/privacyinitiatives/glbact.html).
- <sup>4</sup> [www.ffiec.gov/exam/InfoBase/documents/02-joi-safeguard\\_customer\\_info\\_final\\_rule-010201.pdf](http://www.ffiec.gov/exam/InfoBase/documents/02-joi-safeguard_customer_info_final_rule-010201.pdf).
- <sup>5</sup> For more, see Joel Lanz, *Technology Risk Assessment and Mitigation: Recent Best Practices*, BANK ACCOUNTING & FIN., Feb.–Mar. 2007, at 3.
- <sup>6</sup> [www.ffiec.gov/ffiecinfobase/booklets/outsourcing/outsourcing\\_booklet.pdf](http://www.ffiec.gov/ffiecinfobase/booklets/outsourcing/outsourcing_booklet.pdf).
- <sup>7</sup> [www.ffiec.gov/ffiecinfobase/resources/retail/con-12usc1861\\_1867c\\_bank\\_service\\_company\\_act.pdf](http://www.ffiec.gov/ffiecinfobase/resources/retail/con-12usc1861_1867c_bank_service_company_act.pdf).
- <sup>8</sup> [www.pcisecuritystandards.org/tech/index.htm](http://www.pcisecuritystandards.org/tech/index.htm).
- <sup>9</sup> [www.bitsinfo.org](http://www.bitsinfo.org).
- <sup>10</sup> [www.bitsinfo.org/FISAP/index.php?action=register](http://www.bitsinfo.org/FISAP/index.php?action=register).
- <sup>11</sup> 2006 Compliance Progress Survey, ControlPath, [www.controlpath.com/press](http://www.controlpath.com/press).

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](http://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.