

# Automation in Compliance Mapping and Assessments

by Steve McCalmont and Jeri Teller-Kanzler

Organizations increasingly rely on relationships with vendors, partners, and service providers to better manage their businesses. Lean economic times help accelerate the outsourcing trend, and the software as a service (SaaS) market is experiencing double-digit growth as businesses seek to avoid costly acquisition costs and financial commitments of supporting a full-system lifecycle. The rapid growth in SaaS, cloud computing, and offshoring continues to move information security risks from inside the enterprise to outside. Given the current challenging business climate, enterprise IT organizations can expect more pressure to outsource functions to reduce costs.

Companies seeking to take advantage of the economic and operational benefits of outsourcing vendors come with their own set of operational, financial, and security processes. Matching the risk factors brought by customers are the inherent risks an outsourcing partner adds, which forms a new hybrid risk environment. The ability of an organization to effectively select and manage its vendor relationships affects not only the financial health of the organization but also the organization's safety and soundness.

This *Executive Update* looks at some important issues of vendor risk as well as at the opportunities for efficiency that automating the mapping and assessment phases of a compliance and risk program can provide.

## VENDOR RISK MANAGEMENT FOR INFORMATION SECURITY AND PRIVACY

In many organizations, effectively leveraging outsourced vendors is a key part of business strategy. Various business risks can be introduced through

vendors. These risks can be to the privacy of customer personally identifiable information (PII) that the vendor is processing or storing on behalf of the organization. Numerous other risks can also exist, based on the security controls the vendor employs. Management of these risks requires a close relationship between the organization and the vendor, as well as an effective process to manage vendor risk. In essence, the decision to outsource certain functions, the selection of a vendor, and the supervision of that relationship are important components of the organization's overall process to manage risk and regulatory compliance obligations, including privacy requirements.

As an organization manages risk, its principal goals are to protect the organization and to sustain the company's ability to perform its mission. Managing risk plays an important operational role in implementing business strategies and assigning accountability to responsible organizational decision makers. Firms use the process to identify and manage risks to achieving business objectives.

An organization's size, complexity, industry, culture, management style, and other attributes all affect how it approaches managing risk and subsequently how it makes decisions regarding its relationships with vendors. The regulatory climate, competitive forces, and corporate organization all create unique variables that affect risk management.

Across industry sectors, regulations, standards, and various guidelines highlight the obligation to manage risk. These requirements and controls identify, understand, and mitigate risks to the organization via various local, national, and international privacy laws. They include the Gramm-Leach-Bliley Act (GLBA), the Health Insurance Portability and Accountability Act (HIPAA), the Sarbanes-Oxley Act (SOX), North American Electric Reliability-CIP, the USA PATRIOT Act, Payment Card Industry Data Security Standard (PCI-DSS), and ISO 27001 and 27002. Their provisions also apply to external partner relationships.

The challenge to manage vendors extends to risks that enterprises have in protecting access to private customer

information. A recent study by PricewaterhouseCoopers highlights the challenges in this area:<sup>1</sup>

- Only 22% of respondents have an inventory of all third parties handling sensitive data.
- Only 25% of respondents audit privacy standards through third-party assessments.
- 28% conduct due diligence of third parties handling personal data of employees/customers.
- Asked how confident they were in their partners' or suppliers' information security practices, 10% of respondents said "not at all confident," 53% indicated "somewhat confident," 15% indicated "don't know," and only 22% were "very confident."

Clearly, organizations have work to do in becoming more effective in assessing and managing risk from third-party vendors, as well as in managing the privacy obligations of the enterprise for sensitive data processed by third-party vendors.

## THE CHALLENGE

The concepts of assessing, understanding, and managing risk are not only required by regulations, but they are prudent business practices that can help strengthen a company's management and competitiveness. Taking steps to identify the importance of potential outsourced functions to the organization, the nature of the activities the vendor will perform, and the inherent riskiness associated with vendor relationships are critical to the success of the outsourced function as well as to the organization's bottom line.

Various analyst research reports show organizations spending thousands of staff hours per year on vendor risk assessments — clearly, an area where organizations are expending a great deal of effort and money. Efficiently executing a risk assessment, particularly one that extends to vendor partner organizations, is a challenging undertaking.

As the number of regulatory requirements continues to climb, the challenge of keeping track of multiple requirements with overlapping controls can quickly escalate.

## RISK ASSESSMENTS AND COMPLIANCE MAPPING

In risk management, the component to assess risk is an iterative interplay of actions that take place, a continual process, or lifecycle. Performing an assessment is not a serial process, where assessing for one control affects only that specific control or a related one. On the contrary, the act of assessing a control is multidirectional. In most cases, the assessment of one control can and will influence another control, or even an adjacent phase of the risk management lifecycle.

Assessments are the most critical step in this lifecycle because they take the most time. The risk management lifecycle begins with assessing global threats and vulnerabilities, then develops policies, procedures, and controls to manage or mitigate the risk. To evaluate the effectiveness of the policies and controls, assessments are the next step, followed by remediation. The entire lifecycle is repeated as often as necessary.

An example of assessment complexity is the following real-world scenario that illustrates the complexity of overlapping and redundant regulations:

- Organizations often develop their business practices or policies based on regulatory requirements and/or proven industry best practices.
- Privacy assessments seeking to define where PII exists often need to also determine what sorts of controls are provided to adequately protect access to this information.
- Often, the regulatory requirements overlap, consisting of common logical threads or implying similar controls.
- Consider the ISO 27002 control: "An information security policy document should be approved by management and published and communicated to all employees and relevant external parties." This control is identified as a requirement in multiple regulations, including HIPAA 164.308(a)(1)5; HIPAA 164.308(a)(7)3; GLBA Title V-FFIEC [17]19.1 and 20.1; 201 CMR 17 MA Privacy 17.03[c]; PCI-DSS 12.1.1, 12.1.2, and 12.1.3; and others.

The simple example above clearly illustrates how manual assessments can become unmanageable. Manual assessment methodologies support risk management by

The *Executive Update* is a publication of the Enterprise Risk Management & Governance Advisory Service. ©2009 by Cutter Consortium. All rights reserved. Unauthorized reproduction in any form, including photocopying, faxing, image scanning, and downloading electronic copies, is against the law. Reprints make an excellent training tool. For information about reprints and/or back issues of Cutter Consortium publications, call +1 781 648 8700 or e-mail [service@cutter.com](mailto:service@cutter.com). Print ISSN: 1554-7035 (*Executive Report*, *Executive Summary*, and *Executive Update*); online/electronic ISSN: 1554-7043.

evaluating each specific compliance requirement linked to an individual control. In the example above, performing multiple assessments as to the existence of this control to satisfy each regulation is clearly inefficient for both those who manage compliance and to the business owners. The process is further complicated when an organization has to assess and manage external vendor relationships.

## RISKS TO PII

In an outsourcing arrangement, many of the risks to PII are the same as for internally processed information. Controlling the spread of PII within the outsourcer's IT environment is key, as is ensuring that access controls are effectively used, the outsourcers networks are secure, and encryption is used in association with organizational sensitive data and PII. Even administrative controls, such as employee background checks, have applicability in an outsourcing arrangement. Numerous security breaches have been made public involving call center personnel auctioning off PII for their client's customers.

Ensuring that PII is adequately protected by a vendor comes down to thorough and regular privacy and security assessments.

## THE CHALLENGES OF MANUAL ASSESSMENTS

Manual assessments to avoid complexity and confusion almost always are done individually to avoid costly mistakes by slowing the process down for humans. Each specific compliance requirement and related control is evaluated one at a time. When one compliance requirement and related control is properly assessed, the process can move along to the next. This continues in series until all requirements and all controls are evaluated. Multiple regulations often mean a dedicated analyst assigned to each.

Manual efforts to meet the requirements of each regulation quickly become impractical even for such rudimentary automated tools as spreadsheets. Spreadsheets cannot map the required one-to-many or many-to-many linkages between related regulatory requirements without adding confusion. Spreadsheet mapping systems between multiple requirements are difficult to efficiently maintain as regulations and the controls environment evolve and change.

Manual assessment methods suffer from two major weaknesses. First, they do not efficiently assess

compliance for global operations. Internal operations and external service providers scattered in many locations and jurisdictions are almost impossible to adequately evaluate manually. Secondly, manual methods do not scale well for compliance with multiple regulations. They require costly and redundant parallel management efforts, one for each regulation, increasing staffing costs and forcing a bottom-up management view that limits correlations and weakens the linkage with governance and strategy.

Manual approaches to compliance assessment have largely resulted from the different regulatory silos that have developed in many organizations. This includes the general silos of information security and privacy. As new regulations and regulatory guidance have been issued, organizations have frequently initiated new project teams to manage compliance with each new regulation. The silos that frequently resulted have contributed to redundancies and inefficiencies. Besides the obvious implications for the costs of compliance programs, fielding multiple redundant assessments can result in assessment fatigue on the part of vendor staff.

Implementing compliance mapping, however, can improve the situation by creating a single target for focusing investments on compliance. Historically done using spreadsheets or static databases, mapping of compliance regulations and requirements identifies common requirement threads among controls. The common threads are linked and organized in a unified regulatory knowledge database. This process creates economies but is limited due to rigid relationships that require updating as regulations change over time.

Compliance mapping is a powerful enabler, delivering efficiency and scalability. Organizations using compliance mapping can put into practice an "assess once, comply to many" assessment methodology. An optimized assessment can test for controls status regarding PII and privacy, while also assessing other general security controls. Compliance mapping is an important piece of the puzzle, but, to really drive efficiencies as well as more effective compliance and risk programs, it needs to be coupled with advanced automation. With these capabilities, compliance mapping significantly reduces the number of assessment activities, alleviates redundancy, and provides for robust reporting. In addition, workflow capabilities can automate reminders, escalations, and followups. These ensure that assessments and remediation tasks are carried out and do not fall through the cracks, as is often the case with manual processes.

## CONCLUSIONS

The business drivers discussed in this *Update* will continue to result in the increased outsourcing of business activities and functions. The inherent risks to enterprises that outsource must be managed carefully. The costs of managing this risk are real and increase with outsourcing activity.

Manually mapping compliance regulations and requirements to required policies, procedures, and technical controls is inefficient and unsustainable. Manual compliance management methods introduce errors and do not scale. They limit business agility and quickly become costly and inefficient.

Organizations can eliminate the inefficiencies of manual compliance management methods by deploying automated tools to streamline compliance. A lifecycle approach, managed by a unified set of redundant regulations, maps the overlapping regulatory requirements to a single set of compliance policies, procedures, and controls. A well-crafted assessment process can evaluate controls related to the privacy of customer PII, while simultaneously assessing general information security controls.

## ENDNOTE

<sup>1</sup>“Safeguarding the New Currency of Business: Findings from the 2008 Global State of Information Security Study.” PricewaterhouseCoopers, October 2008 ([www.pwc.com/en\\_GX/gx/information-security-survey/pdf/safeguarding\\_the\\_new\\_currency.pdf](http://www.pwc.com/en_GX/gx/information-security-survey/pdf/safeguarding_the_new_currency.pdf)).

## ABOUT THE AUTHORS

**Stephen A. McCalmont** is Chairman and CEO of Avior Computing. Before Avior, Mr. McCalmont founded Altaworks and Net2Net (now merged with Visual Networks). Altaworks produced a system management application for IBM’s WebSphere and BEA’s WebLogic environments. Net2Net produced a network management system for Asynchronous Transfer Mode networks. Customers included AT&T, MCI, Sprint, HP, and Network General. With his previous two companies, he raised more than US \$50 million in venture capital. Mr. McCalmont has been through multiple successful IPOs and numerous leading M&As.

Prior to these ventures, Mr. McCalmont founded CrossComm’s OEM group. During his tenure, key partnerships were formed with GDC, ODS, and Harris. Mr. McCalmont held various sales, marketing, and management positions at Workstation Solutions and International Telematics. He began his career in applied cryptography at Technical Communications Corporation. He can be reached at [stevem@aviorcomputing.com](mailto:stevem@aviorcomputing.com).

**Jeri Teller-Kanzler**, CISM, is President and Principal Consultant for Risk-MAPP, LLC. She is also an adjunct professor at the Rochester Institute of Technology. Before forming Risk-MAPP, Ms. Teller-Kanzler provided senior-level consulting services to Xerox, implementing an enterprise-wide risk management process and providing guidance in the development of a SOX compliance program. She is a former VP and regional CISO at Citigroup, where she was responsible for a highly visible, strategically significant security management and compliance process. Ms. Teller-Kanzler also provided leadership to the training and awareness staff as well as guidance to various agencies of the federal government in information security assessment, evaluation, training, awareness, and program implementation.

Ms. Teller-Kanzler is the inventor of record for the patent application ComplianceAuthority, a self-assessment program and methodology for information security. She is also the inventor of record for two patent applications: Citi-ISEM (Information Security Evaluation Model) and the Information Security Metrics Program. She can be reached at [jtkanzler@riskmapp.com](mailto:jtkanzler@riskmapp.com).