CHAPTER 9

Security Compliance Management and Auditing

INFORMATION IN THIS CHAPTER:

- Establishing an information security compliance management program
- Publishing an information security compliance policy
- Deploy an information security compliance process
- Information security compliance management in mergers and acquisitions

Information security compliance is both an operational and a legal concern for organizations in many industries today. However, it is not about the fear of lawsuits or fines (albeit this fear is well founded), but due to the increased reliance on information technology (IT), the value of information assets has increased significantly and maintaining repeatable, standardized operations relies on strong control compliance framework. Organizations depend mainly on IT to provide a platform for conducting business. As a result, controlling risks to information assets via security controls has become a dominating topic.

To comply with security practices, enterprises must develop comprehensive information security compliance management programs to comply with multiple regulations, such as Sarbanes–Oxley (SOX), Gramm–Leach–Bliley Act, Health Insurance Portability and Accountability Act (HIPAA), Payment Card Industry Data Security Standards (PCI DSS), and many others. These regulatory standards prescribe recommendations for protecting data and improving information security management in the enterprise.

- SOX requirements mean that any electronic communication must be backed up and secured with reasonable disaster recovery infrastructure,
- Health care providers that store or transmit e-health records, like personal health information, are subject to HIPAA requirements, and
- Financial services companies that transmit credit card data are subject to PCI DSS requirements.

Building a Practical Information Security Program. http://dx.doi.org/10.1016/B978-0-12-802042-5.00010-X

Failure to protect information assets may result in high financial and public cost and may also cause disruption of business activities, and even brand erosion. In some cases, such as with HIPAA, failure to achieve and maintain security compliance may potentially result in financial and legal penalties. What, precisely, is examined in a compliance audit will vary depending on whether an organization is a public or private company, what kind of data it handles, and if it transmits or stores sensitive financial data.

If managed properly, information security compliance standards can be used to strengthen an organization's overall information security program. Integrating compliance efforts with an organization's overall information security program can save money and time, reduce complexity, and help create long-term, sustainable solutions for an organization's information security challenges. In demonstrating security compliance, enterprises are better able to define and achieve specific IT security goals as well as mitigate the threat of network attacks through processes like vulnerability management.

ESTABLISHING AN INFORMATION SECURITY COMPLIANCE MANAGEMENT PROGRAM

An information security compliance management program comprises a minimum set of security requirements for protecting data that apply to any organization that stores, processes, or transmits that data. Maintaining information security compliance requires that an organization have well-defined programs, practices, and processes in place to review and reassess information security practices, even in highly dynamic business environments. To understand how an organization's security program performs on a day-to-day basis, organizations must implement an information security compliance program to continuously monitor and document the implementation, effectiveness, adequacy, and status of all of their security controls. These programs should be well aligned with the organization's business and security goals; address any changes within the organization, operating environment, and implemented technologies; and produce sufficient evidence to illustrate continued adherence to security requirements.

The information security leader should ensure the right stakeholders involved in the process—senior management support is essential for an information security compliance management program. Information security leader should use these various compliance mandates to get with senior leadership, who are often removed from day-to-day information security challenges and processes, to understand the compliance requirements and the organization's security state of compliance against these requirements.

Thankfully, senior leadership understands compliance; however, information security concepts, such as authentication, access controls, and logging and monitoring, continue to be abstract requirements to many senior executives. Senior leadership does understand many regulations come with penalties and fines that could impact the business, such as imprisonment for SOX noncompliance or fines for PCI DSS noncompliance. When discussing regular updates about compliance efforts and compliance projects, information security leader should also use the time to identify managers' security concerns and risk appetite, and educate senior leadership about information security efforts to reduce noncompliance risk.

For organizations that lack a senior executive dedicated to overseeing overall compliance, it is essential that a business risk steering committee be solicited to review the compliance audit process and outputs, including the recommendations. Be sure to include participants from all relevant business groups in the process, as well as line-of-business representatives. Even if the information security leader owns the information security compliance audit, great care should be taken to be sure the involvement of business risk steering committee usually comprises Internal Controls, Internal Audit, and Financial Executives, and the process is not dominated by the IT organization.

Once the information security leader has established support for a compliance management program with senior leadership, a qualified information security compliance manager should be assigned overall responsibility for these activities and be given adequate funding and the proper authority to effectively organize and allocate such resources. Maintaining security compliance requires a well-managed program to integrate security into the day-to-day activities of the organization. Ongoing compliance also requires centralized coordination of numerous resources, actions, projects, and people.

The information security compliance manager would be responsible for engaging management support, coordinating monitoring and assessment activities, and engaging key personnel or functional groups as part of the efforts to ensure all security functions, such as patching systems, security-log reviews, wireless network scans, internal/external vulnerability scans, and internal/external penetration tests are performed as required. Additionally, the information security compliance manager should be responsible for collecting, collating, and storing evidence to demonstrate security controls are operating effectively on a continuous basis. Although the compliance manager is not typically tasked with generating or organizing all of the evidence, the compliance manager would be responsible for making certain the evidence is prepared, indexed, and stored in a central repository for use during assessments or internal reviews. Often the compliance manager and

team rely on governance, risk, and compliance (GRC) tools to manage the process through workflow and hold evidence for inspection.

PUBLISHING AN INFORMATION SECURITY COMPLIANCE POLICY

To ensure organizational understanding of the information security compliance management mandate, a policy is an important tool to state the mandate's objective, goals, purpose, roles, and responsibilities, and its relationship to the overall information security program. The policy formally articulates the requirements that assist management in defining a framework that ensures compliance with the overall information security goals with security-related laws, regulations, policies, standards, and contractual provisions to which their IT resources and data are subject. The policy also has ties to the subordinate procedures and guidelines that may explain the "how" compliance is implemented.

It is equally important to review and update the information security compliance management policy and procedures. As discussed in Chapter 4, the organization may have irrelevant or stale policies, lacks policies that are routinely adhered to, or does not follow the ones it does have in place. In any organization that relies on IT, policies need to be fluid and dynamic, and continually evaluated and updated for appropriateness toward changing IT environment or business conditions. The IT and information security functions should determine together which compliance policies need to be updated, which need to be overhauled, which need to be added, and which need to be retired.

DEPLOY AN INFORMATION SECURITY COMPLIANCE PROCESS

Organizations confronted with multiple regulatory requirements, as well as their own security policies, are often stretched about how to meet so many laws and regulations obligations. Some organizations allow information security compliance to be addressed by more than just the information security function. For example, they may allow the business units most directly affected by the regulatory requirement to perform their own compliance assessment in addition to the organizational compliance assessment and perhaps even a third Internal Audit assessment. As a result, efforts are often incomplete, redundant, duplicative, and even costly. In addition, these organizations may not have the rigor or discipline to execute an evidence-based audit and may simply "self-attest" to a state that is not reflected by reality.

A piecemeal approach may also undermine the integration of information security compliance into other institutional compliance programs, such as information privacy and institutional governance. For example, a decentralized approach to information security compliance management could make it harder to monitor and report the controls that are increasingly a part of audits. For all of these reasons, organizations should consider a unified approach to meeting information security compliance. By using a unified approach to information security compliance, organizations subject to multiple information security laws, regulations, and guidelines will be able to comply with all of them at one time. This is commonly known as a "test once, comply many" approach. By determining which organizational policies, laws, and regulations are applicable, the compliance team then conducts a comprehensive compliance analysis that covers these multiple requirements, and then recommends the minimum level of required safeguards to meet these requirements. Where there are conflicting requirements, such as password strength, encryption strength, or audit settings, compliance should focus on the most stringent requirement as a "high water mark."

Step 1: Determine Applicable Security Policies, Laws, and Regulations

The first step in the process is to determine the security policies, laws, and regulations applicable to the organization. This is an important preliminary step to set compliance's scope. This determination not only will assist in preparing the compliance assessment plan but also will guide the compliance assessor in selecting the information to be collected and the type of compliance assessment methodology that should be performed.

Identifying the appropriate requirements is not always a straightforward process. Depending on their activities and operations, organizations can be affected by a number of laws and regulations. In addition, some policies, laws, and regulations apply only to specific organizational departments or functional activities. In other cases, more than one requirement on the same control area or domain may be applicable. Once the applicable information security requirement law is determined, an appropriate information security risk or compliance analysis framework, such as International Organization for Standardization (ISO) 27004 or National Institute of Standards and Technology (NIST) 800-series, can be selected. It is often worth the effort to map these several requirements when the target of evaluation is governed by several information security framework requirements. For example, if the information system password authentication requirement for system access is six characters for one requirement, eight character for another, and eight characters and special characters for yet a third, it may be helpful for a single requirement (the most stringent) and evaluate the system accordingly.

The analysis model to be used will depend on the organizational type, applicable information security requirements, and information security framework aligned to both type and requirements. An example is a government agency that is aligned to NIST 800-series may require the compliance framework of NIST Special Publication 800-37 "Guide for Applying the Risk Management Framework to Federal Information Systems." A second example is a commercial entity that is aligned to ISO 27000-series may find the ISO 27004 method of risk management more appropriate. Some helpful qualifying questions can be asked to determine the scope and focus of the compliance assessment:

- What is the type of organization (i.e., privately held, publically traded, government agency)?
- What type of industry or markets does the business participate in?
- What type of information is stored, processed, transmitted?
- What processes have legal or regulatory implications (i.e., does the organization provide health care service, process credit cards for payment purposes)?

Step 2: Prepare the Information Security Compliance Management Plan

After the information security compliance requirements are identified, a thorough compliance management plan is prepared by the compliance manager. This management plan is used to guide the individual compliance activities—number and type of compliance audits by business unit or entity, schedules of the compliance activities including senior leadership reviews, policy and supporting procedure and guideline updates, staffing mixes and training requirements for the conduct of audits, and any technology road maps for tools used during compliance audits. This is traditionally an annual process, adjusted periodically as schedules or resources become released or constrained.

Step 3: Data Collection and Asset Identification

Information gathering includes the identification of assets to be protected, document review, and interviews with both management and other stakeholders. The individuals who are interviewed may be line-of-business personnel, functional staff, senior management, legal counsel, audit and compliance personnel, and, of course, the IT staff. It may also involve vendors and other third parties, particularly if certain functions are outsourced but are in scope of the audit. The scope of the interviews will differ slightly, depending on the state, federal, and international laws and regulations that are applicable.

The data collection process will review information security technical, operational, and risk management practices, processes, and procedures. Technical security reviews includes asset management, configuration management,

security management, as well as assessment of IT architecture, application, and network policies. Operational security includes vulnerability management, patch management, incident management, business continuity/disaster recovery, and other operational service or functions. Risk management reviews cover policies and procedures, risk assessments, compliance audits, third-party security reviews, and other analytical functions in managing and governing IT security risk. It is also important to ensure that physical security is included to evaluate compliance for the protection of information security facilities.

Evidence is collected through either manual or automated methods, mainly documentary, interviews, and automated collection through system or security tools. Documentary evidence include written policies and procedures, Internet policies and procedures, sanctions and disciplinary procedures, and other documents evidencing organizational efforts to protect information, such as contracts, procedures for assigning, modifying, or removing access rights, and password-management policies. Auditors will generally ask chief information officers, chief technology officers, and IT administrators a series of pointed questions over the course of an audit. Interviews are particularly helpful to elicit how the program is implemented and personal observations of its effectiveness. Some important areas to cover during interviews are:

- the individual(s) responsible for information privacy and security (organizational and departmental levels);
- information assets that need to be protected to support the business and operations;
- how the information security program is structured; how compliance policies and procedures are implemented and integrated with other activities;
- how well departments work together to ensure that information security practices are uniform; which third parties have access to the institution's information system.

IT administrators prepare for compliance audits using event log managers and robust change management software to allow tracking and documentation authentication and controls in IT systems. These tools' output may include what users were added and when, who has left the company, whether user IDs were revoked and which IT administrators have access to critical systems. Beyond the common system management tools, the growing technological landscape of GRC software now enables the IT staff to quickly show auditors that the organization is in compliance.

Step 4: Perform Risk Analysis

In Step 4, the collected data are integrated into the selected risk analysis (e.g., organizational, ISO, or NIST frameworks). The quality and effectiveness of compliance risk analysis results will depend heavily on how much data were collected

in Step 3. The compliance risk analysis includes technical, operational, and management security including organizational context and considerations.

Step 5: Report Findings and Recommendations

The results of the compliance risk analysis are then documented in an information security compliance audit report. The information security compliance audit report should list organizational context, identified threats and vulnerabilities, current controls, and control effectiveness or even absence. To ensure relevancy and due diligence, the information security compliance audit report should reference specific sections or paragraphs of the applicable security regulations for both existing and missing controls. The plan should encompass all the safeguards identified in the risk analysis and also include procedures for the selection of security system vendors or service providers, and the installation of security systems or services. To maximize the report's effectiveness, the information security compliance audit report should also contain an action plan and milestone schedule for implementing the necessary changes to attain compliance with applicable laws and regulations.

Step 6: Execute the Implementation Plan

The implementation plan provided in the information security compliance audit report is executed in this step. At this stage of the compliance process, it is important to integrate all new controls for meeting information security compliance with other compliance efforts currently under way (e.g., financial, contracts, legal). The integration of compliance programs will ensure uniformity and consistency across the compliance activities, or at the very least avoid duplication of effort redundancy. For example, rationalization and harmonization of compliance activities to support information security regulations can potentially save time, money, and other resources and procedures.

Step 7: Periodically Monitor, Test, Review, and Modify the Information Security Compliance Management Program

Information security, as any IT activity, is an ongoing process. Maintaining a state of continuous compliance requires focused effort and coordination. Due to the changing technology landscape, information security functions should continuously monitor and test the effectiveness of implemented controls against known or potential threats. This involves testing applications and networks or applications against emerging threats and recommending actions when threats are present and vulnerabilities are discovered. Organizations that are accustomed to traditional approaches of information security compliance that focus primarily on annual audits may find it difficult to build in the people, processes, and technology necessary to support sustained compliance. Organizations should perform periodic compliance risk analysis to validate

that control selection and implementation features continue to be reasonable, appropriate, and effective.

INFORMATION SECURITY COMPLIANCE MANAGEMENT IN MERGERS AND ACQUISITIONS

Mergers and acquisitions (M&A) can be extremely effective mechanisms for companies to achieve important business objectives. Information security and privacy compliance requirements play a critical role because they may impact the acquirer's business objectives, regulatory profile, and valuation model, particularly if the new acquisition introduces increased risk of an information security or privacy-related liability. Whether the M&A goal is gaining access to a new market, acquiring new technology, or gaining economies of scale, the acquiring organization needs to develop an information security compliance approach that addresses information security and privacy concerns that may manifest themselves before, during, and after the M&A. As the information security team reviews acquisition targets, as well as the M&A team's approach to evaluating targets, the team should consider the following elements:

- If the acquisition goal is expansion into new industries or geographic regions, there may be new regional regulatory or legal requirements for information security and privacy. It is important to identify what new markets will be entered. If the acquisition involves expansion into highly regulated sectors (e.g., health care, financial, business targeting children as consumers, etc.), then the information security program may require a change in the face of changing compliance obligations, both domestic and international, for the organization.
- If new business processes are introduced with new data types or categories transmitted, processed, or stored between the two parties, this may introduce a different level of required security or privacy compliance. During the due diligence process, if the acquirer finds that the acquisition target involves cross-border data transfers or privacy regulations, the acquirer will need to explore the target's compliance for transmission security. For example, if the seller or target has certified to the EU–US Safe Harbor replacement program ("Privacy Shield"), the acquirer will want to review any previous Safe Harbor assessments, as well as its publicly available Safe Harbor certification. If the seller or target is subject to HIPAA, the buyer would want to evaluate its HIPAA compliance measures. The compliance risk profile of the buyer or seller might change post sale.
- If the motivation for acquisition is the introduction of a new product, service, or technology, then the types of data categories or sensitivity of

privacy information must be identified. What privacy policies, notices, and other compliance efforts will be required to support new products, services, or technologies? This becomes particularly relevant if the acquisition uses the acquired technology in a different manner than earlier designed. For example, using a new platform for processing data types for which it was not designed may require rework and additional cost to the acquirer, and therefore may dilute the value proposition of the acquisition by introducing more cost to the transaction.

Another information security compliance concern is the M&A process itself. Both parties should be sensitive that sometimes providing other parties (such as the acquirer in an M&A) with the personal information of employees or clients can itself be a breach of privacy policies or laws. Questions should be asked before the diligence process actually takes place to ensure no violations will occur with performing the diligence process. Likewise, another aspect of due diligence is third-party information security compliance. It is during the diligence process that large amounts of sensitive and confidential information will be shared with bankers, attorneys, consultants, third-party vendors, and other parties. No matter how secure an organization is and how many process steps are taken to secure their data, both parties are reliant on third parties that host, access, and store the target organization's data. Parties, particularly the target company, should carefully assess third-party compliance to information security practices that will be hosting their data during the diligence process, particularly in their online data rooms.

SUMMARY

The increased number of government-mandated and private contractual information security requirements has caused organizations to view information security as another aspect of regulatory or contractual compliance. The existence of fines, penalties, or loss (including brand erosion) has also increased the appetite to implement comprehensive information security practices, such as information security compliance management. This approach begins by reviewing all of the information security requirements imposed by the emerging statutory, regulatory, and contractual legal standards. These standards are then compared with the more established information security standards. After a thorough risk assessment and analysis, the legal standards and the information security standards are blended to create a complete information security compliance program. A unified approach to information security compliance thus enables organizations not only to address identified risks but also to comply with the law.

ACTIONS

Identify the business need for an information security compliance program; compliance programs do not exist unto themselves.

- Industry involvement, regional orientation, business processes or product/services, and information types will generally indicate a requirement to protect. The compliance program will tie the requirement and validation together as a business requirement.

Develop an information security compliance management policy and supporting documentation according to the compliance requirement (legal, regulatory).

- An overarching policy provides the basis and justification of the information security compliance program. Subordinate procedures, guidelines, and checklists then provide the "tools" for implementing the program. Periodic information security compliance policy and other documentation reviews should be conducted as regulations and standards change—the policy, as a minimum, should be reviewed annually for relevancy and effectiveness.

Identify stakeholders that will champion the information security compliance management program.

- Usually these stakeholders will be involved in other compliance or compliance-related activities; the chief financial officer and chief compliance officer are typically the best champions for a compliance-based program that reduces financial risk, as well as any other compliance risks to the business that may cause some degree of materiality to the business.

Design and develop a compliance management process that is easy to understand and follow.

- Ensure traceability to the legal requirements to compliance audit framework—the requirement must have direct correlation to the audited control and data that support the analysis. Failure to demonstrate traceability will cause some to call into question the reason for the compliance audit if it is not relevant. Simplicity in compliance audit execution will be much more palatable than onerous, time-consuming audit processes.

Deliver business value through clear and concise reporting of findings and recommendations.

- Ensure that these recommendations are vetted against other risk and compliance management recommendations to eliminate redundancy and duplication. The overall finding should be easy to understand in business terms and relevant to the business risk than simply technical risk. The business leader who cannot translate the compliance gap to the effect on the business is less apt to invest in gap remediation than one who easily understands the gap and necessity to close it due to business impact.

Ensure information security has a role in M&A.

- M&A can have an impact on the organizational compliance posture through the integration of new business processes and information categories between the acquirer and target organizations. During due diligence, the information security team should understand the target acquisition compliance requirement, how the target is meeting them, and if any liability or risk of failures may be introduced into the acquirer's portfolio of information security risks. Post acquisition, the information security program will need to integrate the new acquisition into the existing information security compliance program.