



Security and Compliance Management. Redefined.

Technical Whitepaper

Compliance for Everyone

Implementing a Security Framework Approach to Address Compliance Mandates

eIQnetworks, Inc.,
World Head Quarters
31 Nagog Park
Acton, MA 01720
978.266.9933

www.eiqnetworks.com

TABLE OF CONTENTS

SECTION	PAGE
Introduction	03
From Tactical to Strategic Compliance – How We Got Here From There	03
Tactical (Regulation-Specific) Compliance	03
Strategic (Holistic) Compliance	04
The Top 5 Mistakes in Compliance Management	05
Managing Compliance the Right Way	06
The Strategic Approach to Compliance Management	08
Additional Information	09

INTRODUCTION

If you are an information security or IT audit professional, then you are in the business of securing your organization's information assets and complying with regulations. Many organizations have historically adopted a "rifle-shot" approach to complying with regulations. As new regulations popped up on the radar, IT implemented a tactical program to comply with each specific regulation.

Given the number of regulations and the emerging threat environment, organizations must now take a much more strategic approach to compliance initiatives.

Fortunately, in recent years information security and privacy compliance have made dramatic gains in becoming high-interest targets across Board Rooms –although for many organizations, "compliance" still equates to "regulations". This regulatory-focused approach is at odds with the reality that the scope of security and privacy compliance requirements that must be addressed and managed by organizations is increasing every day. No longer solely the domain of SOX, HIPAA, and other government-driven mandates, today's information security and privacy compliance programs must address a wide range of internal requirements dictated by business partnerships, established service level agreements (SLAs), known and emerging threats, and other factors driven by both business and technology.

Addressing all of these requirements separately is an exercise in futility. The most effective method to manage compliance with so many different – and sometimes contradictory – compliance drivers is through a disciplined, holistic approach that addresses compliance not as a reactive or point-in-time event, but as a proactive, comprehensive program. In this paper we will review a brief history of information security and privacy compliance, identify some of the most common problems associated with building a compliance program, and review some effective strategies to avoid these barriers.

From Tactical to Strategic Compliance – How We Got Here From There

In the field of information assurance, the track record of compliance management has not been easy. For decades, IT has been focused on factors such as operational efficiency and performance. Security of information rarely came to the forefront. In the early days of centralized and distributed systems, this was not due to lack of foresight; rather, in the pre-Web era most systems were either not connected to networks where they were publicly accessible, or if they were, they used more simple protocols and services which didn't necessarily expose them to significant risk. While Boards of Directors and other executives might have had significant interest in ensuring compliance with early regulations, they generally adopted a "checklist" mentality; they wanted a straightforward, clear assurance that the organization was meeting specific initiatives, but weren't particularly interested in how the organization achieved those compliance goals, as long as it made auditors happy.

Tactical (Regulation-Specific) Compliance

In 1996, the Health Insurance Portability and Accountability Act (HIPAA) permanently changed the landscape of information security and privacy compliance. HIPAA was one of the first broad, multi-industry regulations that contained significant information security and privacy requirements.

Because the scope of information that HIPAA tried to protect was so broad – protected healthcare information (PHI) – and also contained significant sanction penalties for non-compliance, this regulation sounded a warning bell in organizations to which it applied.

Implementing HIPAA compliance initially presented a problem for many organizations. Because HIPAA integrated provisions for many different business areas – IT operations, information security, HR, and audit – it forced organizations (many for the first time) to establish a program approach to compliance. No longer a confederation of separate groups, organizations had to adopt a broad governance model for compliance, bringing these groups together to achieve specific cross-functional compliance goals.

HIPAA was not the only driver during this era to promote a program-based approach to information security and privacy compliance. Many standards bodies were busy delivering comprehensive frameworks for managing information assurance, including ISACA's COBIT, and ISO's ISO17799 standard. Coupled with regulations like HIPAA, they promoted the idea of risk-based decision making for managing information security and privacy. While not mandatory for organizations to comply with these broad frameworks, they provided a great way for organizations to securely manage common IT processes, and usually mapped directly to security and privacy provisions in specific regulations, including HIPAA.

While these regulations and frameworks helped organizations establish a more comprehensive approach to information security and privacy compliance management, they still promoted a "checklist" approach to information assurance. This would change rapidly as organizations began dealing with the confluence of multiple regulations, standards, best practices, and control frameworks that began to emerge over time.

Strategic (Holistic) Compliance

As regulatory compliance for information security goes, the Sarbanes-Oxley Act of 2002 (SOX) became gold standard of regulatory heartburn for every publicly traded company in the United States. Sections 302 and 404 of SOX, although small in size (less than two pages of text), had tremendous ramifications for corporate America. For the first time, not only civil but criminal sanctions were mandated for certain conditions of non-compliance, and these penalties applied to C-level executives. Needless to say, once SOX was in effect corporate Boards of Directors throughout the country began to show a tremendous interest in security compliance – and this, more than the value of SOX security controls themselves – was the real value of SOX.

By enforcing a compliance mentality on senior executives, SOX helped organizations to adopt a holistic, program-based approach to security and privacy compliance, in which compliance reporting and metrics across all applicable compliance drivers became critical to the operational success of the company. Suddenly, the ability to report on a single regulatory driver – SOX, HIPAA, and others – made less sense than a centralized security and privacy compliance program because many of these requirements overlapped and they often shared risk-based decision making models. Instead of a "SOX compliance program", organizations began developing what has today become in many companies an IT Compliance program to help executives and board members answer more important business questions such as:

- How are we consistently measuring and reporting compliance?
- Can we show auditors adequate evidence of our compliance efforts?
- Are we reasonably reducing or eliminating our exposure to sanctions?
- Are our compliance efforts consistent with other organizations of our size and in our industry?
- How much is compliance costing us, and are we spending more than we have to?

Around the same time, the very definition of “compliance” began to change; organizations began to realize that their responsibility to secure data extended to their business partners due to standards such as the PCI Data Security Standard (PCI-DSS) and the Gramm-Leach-Bliley Act (GLBA). Consequently, businesses began seeing a noticeable uptick in partner agreements containing security and privacy controls language, and had to begin addressing these concerns – and reporting on compliance with them – as part of their comprehensive compliance program. Similarly, organizations also began to realize that any compliance program needed to include their own policies, standards, and procedures, as well as address the influx of ever-increasing threats to information and assets across the enterprise. Coupled with these new compliance drivers was an increase in service level agreements (SLAs) and other performance-based compliance criteria, which augmented security and privacy requirements.

Today, there is no end in sight to the broad range of compliance drivers that organizations must address. New federal and state security and privacy regulations continue to be drafted, international groups such as the European Union continue to refine their data security and privacy requirements, new and updated best practices and control frameworks are developed, new threats emerge on a daily basis, and business partners continue to share the mitigation of risk by mandating security and privacy controls with their business partners. Today, only a holistic, program-based approach provides the necessary capability to address security and privacy compliance across most enterprises.

The Top 5 Mistakes in Compliance Management

Unfortunately, building a holistic security and privacy compliance program is not a simple process. It requires buy-in across the organization, from senior executives to IT, finance, HR, and other operational groups across the enterprise. Organizations typically encounter a wide range of barriers (sometimes self-imposed) when building a program, and the following list represents some of the more common mistakes encountered.

- **Mistake #1: Making Compliance Tactical (Regulation-Specific).**
With regulations that have far-reaching implications and significant sanctions (such as SOX), it can become easy to take a myopic view of information assurance by concentrating the majority of security and privacy efforts on a single regulatory element, rather than through a holistic compliance program. The danger of this regulation-specific mentality is that the organization can fall back into the “checklist” mentality, which promotes compliance over the actual purpose of a security and privacy compliance program: reducing risk to make the organization more secure.
- **Mistake #2: Viewing Compliance as a Point-In-Time Event.**
There is no doubt that audits (both internal and external) can provide organizations with great feedback and recommendations on their information assurance efforts. However,

when the organization makes audit events the focus of compliance – rather than risk-based decisions that are designed to continuously protect the organization – the threat of those risks being realized during “non-audit” periods can become significantly higher.

- **Mistake #3: Addressing Technology Without Addressing the Business.**

The purpose of a compliance program is to protect the security and privacy of information and assets that ultimately are used as part of a business process. When organizations take a “throw technology at the wall, and see what sticks” mentality toward compliance, the real, underlying value of information security and privacy to the business is lost. Also, by excluding the business side of the organization from the compliance program, the organization may not properly evaluate risks, and as importantly, may spend too little – or too much – protecting information and other assets.

- **Mistake #4: Failure to Achieve Organizational Buy-In First.**

Compliance is a broad-reaching initiative that requires both buy-in and action across a broad range of constituents, including IT, HR, finance, and other operational groups. Unfortunately, in many organizations a “stovepipe” mentality exists across these groups; by not acquiring championship by senior executives, an enterprise-wide compliance program is (at best) minimally effective, or (at worst) doomed to fail.

- **Mistake #5: Inconsistent Metrics and Reporting.**

Perhaps the most dangerous mistake that can affect any compliance program is inconsistent measurements and metrics. One of the most common examples of this is in the realm of risk management: one group within the organization (such as IT operations) may recognize three different levels of risk, while information security may recognize seven, and IT audit may maintain a more granular, continuously-variable risk map that provides dozens of risk categories. Unfortunately, all three groups are part of a compliance program; trying to align IT operations’ definition of a “critical risk” with IT audit’s definition of the same can be a difficult process, and is likely to result in real risks not being recognized or addressed.

Managing Compliance the Right Way

Sidestepping these mistakes while addressing a complex myriad of security and privacy drivers can be a daunting task, even for the most knowledgeable of organizations. How can the enterprise establish a comprehensive business process to address compliance management from the top down? How can a single set of policies, standards, procedures, and controls be established to address so many different compliance requirements mandated by government agencies, business partners, and internal needs? While an enterprise-wide compliance program is a great starting point, it’s important to build that program in a manner that avoids the most common mistakes outlined above.

Sidestepping Mistake #1: Make Compliance a Strategic Effort

Effective information assurance efforts address all the factors that drive compliance, including regulations, adopted best practices and frameworks, business partner agreements, and established internal policies, standards, and procedures, as well as emerging known threats. In addition, a truly efficient program should identify the overlapping requirements and controls between compliance drivers, and allow organizations to plan and budget appropriate controls by normalizing against the greatest common denominator among similar requirements.

Undoubtedly, standardizing on a software platform to help manage security and privacy compliance efforts provides huge value; however, it's important to standardize on tools that are flexible enough to support any arbitrary compliance driver, rather than only supporting selected regulations and best practices. Also, solutions which are based on a specific "best practice" framework – such as ITIL, COBIT, or ISO17799/27002 – are only useful if the particular framework works for your environment; don't rely on solutions which force your organization to adopt standards which are not appropriate for your business.

Sidestepping Mistake #2: Build a Structured Compliance Program

A compliance program is a full-time business process; it requires dedicated personnel, coupled with communication and management tools. While these tools provide value to the compliance process, however, they do not (and cannot) replace the people and processes that form the foundation of a compliance initiative. The core foundation of a compliance program is a risk management process, and a series of written policies, standards, and procedures that comprise the "operating rules" of the organization when it comes to information security and privacy. Organizational standards flow from these policies, and in turn specific business and technology processes and procedures flow from these standards.

While there is no such thing as a "turnkey compliance program" (and you should be wary of any solution vendor that promises such), using a unified software platform for compliance can dramatically improve the success of information assurance efforts. However, it is critical to ensure that any software solutions have the flexibility to match your compliance efforts; your information assurance program should drive your compliance automation software, not the other way around!

Sidestepping Mistake #3: Risk-Based Decision Making

Identifying and measuring risk to information and other assets is a core function of information assurance! Being compliant isn't very interesting if the organization continues to accept undue risks to information assets. Determining risk can be done in different ways, but generally involves the following:

- **Documenting Assets.** If the organization doesn't know what information assets it has – data, systems, and networks – and their value, then it can't possibly know what to protect and how to protect it.
- **Threat Identification.** Knowing what the organization has is a good first step, but real risk management requires understanding what the threats to these information assets, whether physical or logical, human or environmental, accidental or deliberate. By understanding these threats, metrics such as likelihood and consequence of risks can be accurately measured.
- **Risk Metrics.** Risk metrics, based on known information assets and threats, allow the organization to establish appropriate controls and mitigations, or (if appropriate) accept risk, based on minimal likelihood or consequence.

Any compliance automation software solutions used by the organization must understand risk, and must categorize and measure risk consistently. If the organization uses a single integrated platform, this usually isn't a problem since this solution provide a single, consistent risk model. However, if using multiple point solutions to manage compliance, it is important to ensure that these tools are flexible enough to support multiple definitions of risk.

Sidestepping Mistake #4: Communicate First

Because compliance is ultimately a business process, it should be socialized and established within the organization before any implementation efforts begin, and all stakeholders and constituents should be involved from the beginning in the development of any compliance initiatives. To ensure success, executive buy-in is particularly critical; C-level executives can often break down barriers that might exist in the organization, establishing authority and circumventing “turf wars” and other political constraints that might otherwise hinder the program. Ongoing, consistent communications are integral to an IT GRC program once it’s established; consequently, it is critical to provide tools to allow stakeholders an up-to-date view into the compliance program.

To support effective communications, compliance automation software platforms should provide the ability for different categories of users – IT operations, security operations, risk managers, auditors, and C-level executives, to name a few – to view risk and compliance data in a way that is relevant to them, while providing a way to compartmentalize data to ensure appropriate separation of duty across constituents.

Sidestepping Mistake #5: Establish Measurement and Reporting Baselines

While maintaining a communications framework for IT GRC activities is critical, it is just as important to ensure what is communicated is accurate and consistent across the enterprise. A compliance program must use consistent measurements and metrics, to ensure that one group’s view of risk and compliance (such as IT operations) is consistent with another’s (such as IT audit). By standardizing on a compliance automation software platform, rather than a series of point solutions that are cobbled together, organizations can ensure that they present a consistent definition of compliance and risk across the enterprise, regardless of constituent.

The Strategic Approach to Compliance Management

As the regulatory landscape for information security and privacy continues to increase, organizations must also address a broad range of “new” compliance requirements including business partner agreements, internal SLAs, changing technologies, and continuously emerging threats. In the past, addressing a smaller number of security and privacy requirements through separate efforts was a reasonable approach; however, in today’s environment, the only reasonable solution is a compliance program that identifies the overlap and ambiguity between compliance requirements, establishes a centralized set of business processes and tools to address compliance, and allows appropriate stakeholders to identify and address the organization’s security and privacy posture using consistent measurements and metrics.

As the compliance landscape continues to change – and the definition of “compliance” itself matures over time – organizations that take the time to establish a holistic, program-based approach to compliance management will be in the best position to reap the benefits of reduced risk and improved security and privacy.

ADDITIONAL INFORMATION

About eIQnetworks

eIQnetworks, Inc., is redefining security and compliance management by fostering collaboration across security, network, data center and audit teams to more quickly isolate the root cause of security issues and ensure compliance mandates are being enforced. Global financial, media, healthcare, manufacturing, and government enterprises rely on eIQnetworks to make sense of formerly disparate data sources to react faster to emerging threats, automate their compliance efforts, and more effectively monitor security policies. Headquartered in Acton, Mass., eIQnetworks is located online at www.eIQnetworks.com and can be reached at +1 877.564.7787.

World Head Quarters

31 Nagog Park
Acton, MA 01720
(978) 266-9933

© 2008-2009 eIQnetworks, Inc. eIQnetworks and SecureVue are registered trademarks of eIQnetworks, Inc. All other trademarks, servicemarks, registered trademarks and servicemarks are the property of their respective owners.