

The Intersection of Compliance and Security

By James Hietala, CISSP, GSEC, GCFW
 jhietala@controlpath.com

IT organizations today face significant challenges in complying with numerous regulations affecting IT security, including Sarbanes-Oxley, Gramm-Leach-Bliley, PCI, HIPAA, and FISMA. In addition, the evolving security vulnerability and threat landscape continues to test corporate security policies and defenses. Savvy IT security and compliance professionals will select security controls that can address the threat landscape, while simultaneously satisfying regulatory mandates. In doing so, their organizations can benefit greatly by moving away from “compliance as an event” thinking, toward an optimized compliance process.

Compliance Challenges

Keeping up with the mandates of SOX, HIPAA, GLBA, and other compliance regulations has become a significant burden for regulated organizations. In a world where the amount of regulatory oversight has increased dramatically, developing and maintaining compliance presents some real challenges.

1. The cost of compliance efforts has skyrocketed. In 2005 businesses spent an estimated \$15.5 Billion on compliance-related activities.¹
2. In industries affected by multiple regulations, a schedule of overlapping and redundant activities is required to achieve and maintain compliance.
3. 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.
4. Few IT environments are static for long. While initially perceived by many to be a one-time event, compliance activities are now becoming a recurring task, because of the constant change in the IT and business environment at most large organizations.
5. Large corporations are spending far more on audits than planned. A recent study indicated that large firms spent an average of \$2.4M more than they had planned on audits in 2004. It is fair to assume that the overruns were primarily

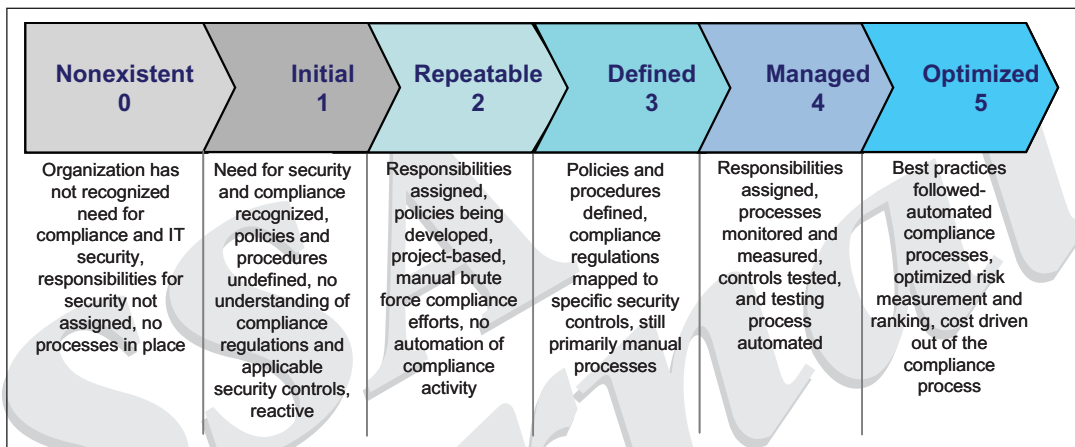


Figure 1: Organizational compliance efforts can be benchmarked against the Compliance Maturity Model

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 Sarbanes-Oxley compliance.²

The negative consequences of non-compliance, and generally of not having one’s security program in order, have escalated to the point where they are now boardroom issues. No one wants to be the next large organization to have to publicly disclose a security breach or a material weakness in their internal controls.

As a result of these challenges, IT organizations are left asking themselves some tough questions:

1. How do I measure compliance? How do I achieve it, given resource constraints? And once achieved, how do I maintain compliance?
2. Can I somehow systematically associate my technical security controls to compliance regulations and security standards?
3. Is it possible to enhance my security posture while satisfying compliance objectives?
4. Most importantly, can I more effectively manage compliance activities to reduce repetitive work and reduce the ongoing cost of compliance activities?

Compliance Maturity Model

The Compliance Maturity Model,³ shown in Figure 1, describes a continuum of organizational compliance practices. The model is useful in under-

standing the maturity of compliance efforts within an organization, and the next steps that are required to move toward an optimized state.

Moving from the nonexistent state toward an optimized state requires the creation of policies and procedures, applying security controls to regulations, and ultimately automating the compliance assessment, remediation, and control testing processes. The opportunity for IT security professionals is to create a solid set of security controls, and to use these as the basis for compliance measurement. This database can serve as a cornerstone of compliance management activities. In addition, establishing a repository of security controls improves the security posture, as the controls can be more uniformly applied, and testing of controls can be automated.

Mapping Information Security Controls to Compliance

Depending on how specifically each requirement in a compliance regulation is written, it may have a one-one mapping to a given security control, or more likely will have a one-many mapping, whereby addressing one compliance requirement will require the use of numerous security controls. See Figure 2.

Consider a simple example of a publicly traded organization that processes credit card data in the course of their business. They are subject to SOX and PCI regulations and, in addition, are working toward using ISO 17799 as a baseline for information security. In this example, they are using COBIT as their basis for measuring compliance with SOX section 404. For password change policy, they have implemented the following security control:

The detailed security control shown in Figure 3 maps to specific requirements found in ISO 17799, COBIT, and PCI. This control will need to be applied to all servers and applications which process credit card data, and the organization will likely also apply it generally to servers and applications in their environment, if they are moving toward ISO 17799/27001 compliance and possible certification.

Extrapolate the simple control mapping example described above to an environment where there are hundreds of servers and applications, multiple locations and business units, and various third-party service providers. All of these require the application of numerous controls, assessment and measurement regarding compliance, and remediation to close gaps. A typical large organization can easily have 1,000 (or more) detailed security controls addressing all ten domains of information security.

These security controls will need to be mapped against multiple regulations. And the regulations, which generally are much higher level than the specific controls, have numerous specific requirements that compose the entire compliance regulation. The magnitude of the task is clear, and it is considerable.

Given the scope of the compliance challenge, it should be obvious that management of compliance efforts for complex organizations with largely manual efforts and spreadsheets to track activity is not a sustainable (nor enjoyable) approach.

A knowledgebase containing security control and compliance regulation data is an effective tool for managing compliance activities. Once the security controls are selected or created, it becomes far easier to map the controls to various portions of the regulations.

The compliance knowledgebase will serve as a living repository of organizational compliance, including mapping the various parts of the organization being measured for compliance. The database can also serve as the

Regulation	Number of Specific Requirements
HIPAA Security Rule	74 organizational, policy and procedure, documentation, administrative, physical, and technical safeguards requirements
PCI	12 high-level requirements, with ~212 detailed requirements
FISMA/FIPS-200	Defines 17 areas of security requirements, each of which reference numerous controls from NIST 800-53
COBIT (V3, 2000)	Defines 4 domains, 34 high-level objectives, and 318 control objectives
GLBA/Interagency Guidelines	Defines 7 high-level requirements, each of which comprises numerous detailed requirements

Figure 2: Relative scope and level of detail for various compliance regulations

focal point for storing evidence of compliance, which will make the audit process less painful and less costly. In addition, applying a workflow capability to the assessment and remediation process will eliminate much of the costly manual work associated with these activities.

Creating an enterprise repository of security controls and compliance regulations offers another intriguing possibility. Heretofore, the process of assessing risk has been periodic in nature. If a company hired a consultant to perform a risk assessment yearly, the output of that effort provided a good measure of what their risks looked like—at a single point in time each year. Between assessments, the risks are constantly changing, as new elements are added to the environment, remediation efforts are completed, new third-party vendors are added, and so on. A database of compliance knowledge, security controls, and organizational structure, coupled with workflow capabilities, provides the building blocks necessary to measure risk on an ongoing basis. As corrective actions are completed, the real-time organizational risk measurements will be dynamically lowered to reflect this. Similarly, as new risks are identified, the dynamic risk measurement will be increased until corrective actions are completed. This capability provides security, risk management, and compliance professionals with immediate, actionable information needed to improve the organizational or business unit risk posture.

Compliance Process Optimization

Compliance Process Optimization describes an effort to move from the initial stages of the Compliance Maturity Model toward a fully optimized state. The goal is to deliver a compliance program that is standards-based, reliable, cost-effective, automated, and sustainable.

Compliance Process Optimization requires:

1. Mapping of requirements (from compliance regulations to controls);
2. Development of a security and compliance program (policies, standards, procedures);
3. Creation of a compliance process (achieve, measure, and maintain security and control requirements);
4. Automation of the entire process to reduce repetitive manual tasks and reduce overall compliance program costs.

A fully optimized compliance program makes the ongoing compliance effort simpler, and far more manageable. Compliance Process Optimization delivers numerous other benefits:

1. Security professionals can now get out in front of the compliance challenge, proactively defining the security controls and managing the process of measuring and documenting compliance, as opposed to constantly reacting to audit requests.

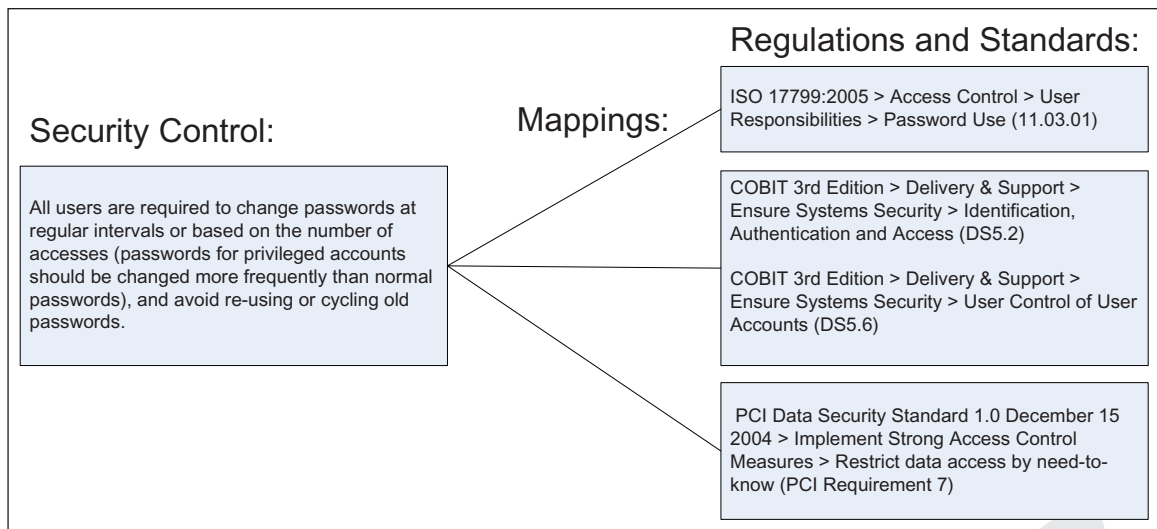



Figure 3: Mappings from a single security control to multiple regulations and standards

2. IT staff can leverage the work that is done to define a security controls database (and it can be significant) by enabling the application of controls and controls testing in a uniform way, to address the twin objectives of improving the security posture, and of developing, documenting, and demonstrating compliance.
3. Companies can realize real improvements in compliance and security processes, and significant cost reductions.
4. Organizations gain the ability to measure and track enterprise risk, and show changes to the risk profile in real time, as corrective actions are completed.

Summary

Using a central controls and compliance database as the cornerstone of the compliance effort improves the security posture, and eliminates manual efforts required to develop and maintain compliance. Considering compliance as a process, rather than as an event, can transform the effort, making it more productive, highly sustainable, and far less costly. 

Jim Hietala, CISSP, GSEC, GCFW, is Director of Product Marketing, ControlPath, Inc. (www.controlpath.com). ControlPath is a developer of compliance and risk management software solutions that enable Compliance Process Optimization.

¹ AMR Research, "Spending in an Age of Compliance," 2005

² FEI

³ ITGI, SOX Compliance Maturity Model. Descriptions of phases provided by ControlPath.