

Compliance: Getting more secure or just a check in the box?

By Brad C. Johnson and Richard E Mackey Jr.

A secure environment can be accomplished in a number of ways, but at the core you need a framework that helps to guide you in decision making and priority setting.

The reason that organizations care about security is that it helps to make their business more stable as well as to protect their important data assets: client and corporate information. There is a phrase that captures the essence of this basic concept: Good security is good security. That is, an organization that promotes good security practices and builds on a foundation of sound fundamental principles is going to be better prepared to handle changes and problems. Security, like quality, is not something you add on later like a car accessory; it is something you build in at all levels. You think about security at the design level, at the implementation level, at the deployment level, and as part of maintenance.

In today's ever changing world and especially in light of the economic woes that have fallen upon us all, having a business built on sound security principles is the only way to stay relevant. Achieving this stable and secure environment can be accomplished in a number of ways, but at the core you need a framework that helps to guide you in decision making and priority setting.

There are two words that go hand-in-hand as part of defining this framework: *standards* and *compliance*. Standards provide a well-documented way to review your business environment within a particular context, and compliance is the act of having proven that you have met the requirements as set out by a particular standard. You can strive to be PCI-compliant, HIPAA-compliant, SOX-compliant, ISO-compliant, NIST-compliant, and many other standards that will denote that you are compliant in some either far-reaching or very specific way. So, while particular standards and regulations have a distinct focus (e.g., HIPAA for electronic personal health information, PCI for credit card data), the underlying fundamentals are consistent.

There is a natural tension in that you always want to do what is right (strive toward industry best practice), but you at least want to do what is required (industry standard practice). That

is, you want that "check in the box" to show others you are doing good things, but you do not want to be so focused on check marks that you lose sight of the bigger picture: running your business safely. Let's grapple with the issues of compliance and standards using two very well-known standards: PCI DSS and ISO 27002.

PCI DSS and ISO 27002 in a nutshell

The PCI Data Security Standard (PCI DSS) consists of 12 mandatory high-level requirements for all organizations that store, transmit, or process payment cards. These 12 requirements are further subdivided into six sections, describing activities that organizations must engage in while managing their networks, administering their systems, and, in general protecting the payment card data with which they have been entrusted.

PCI DSS

- Build and maintain a secure network
- Protect cardholder data
- Maintain a vulnerability management program
- Implement strong access control measures
- Regularly monitor and test networks
- Maintain an information security policy

While PCI DSS details compliance requirements in most areas, its directives make only passing reference to an overall security framework into which the required actions must fit. If organizations simply follow the PCI DSS blindly, they may not achieve their overall security goals because the DSS, by its very nature, is specifically focused on protecting credit card data and not necessarily on ensuring that a comprehensive and effective security framework is in place.

ISO 27002, also known as ISO 17799, is a security standard of practice. It is a comprehensive list of security practices that

can be applied to varying degrees to all organizations. It has 12 different sections that provide best practice recommendations on information security management. There are over 130 specific control objectives that are outlined in those sections.

ISO 27002

- Risk assessment
- Security policy
- Organization of information security
- Asset management
- Human resources security
- Physical and environmental security
- Communications and operations management
- Access control
- Information systems acquisition, development, and maintenance
- Information security incident management
- Business continuity management
- Compliance

At a high level one might come to the conclusion that you would either use one or the other. In practice, and running your business for the long-term, it would be better to think about using both as the use of one will help with the other. They, as it turns out, have a natural tendency to reinforce good security decisions across each other while at the same time leading to the desired state of being compliant in a specific one. ISO provides a good over-arching security framework while PCI details the expectations to ensure that critical customer information is handled correctly (for the specific purpose of dealing with credit card information).

Using two standards for compliance

The benefit of ISO 27002 to organizations attempting to comply with the PCI DSS is twofold. First, it provides a framework that allows organizations to demonstrably satisfy their PCI security requirements along with requirements from other sources, like industry or governmental regulations. Second, it provides guidance on how to fit some of PCI's governance and policy requirements into an organization's compliance program.

For example, ISO 27002 discusses the necessity of involving business, management, human resources, and technology representatives in the security program. It also provides references for high-level policies for important areas such as data classification, data handling, and access control. While PCI DSS describes specific technical practices and organizational activities, it does not talk about the overall program in which these activities exist or the specific policies that require these activities.

When a company establishes a program based on a broad standard like ISO 27002, it can treat the PCI DSS requirements as a subset of those required by ISO. Further, a program structured according to ISO 27002 will require organizations to employ critical support systems required by many regulations (and PCI DSS in particular).

Let's take a look at another example. ISO 27002 requires change control in network administration, system configuration, policy management, procedure management, and software development. PCI DSS calls out the need for accurate diagrams and documentation for its network and systems as well as change control processes to ensure discipline in administration of the PCI DSS-related components.

ISO 27002's broad requirements for change control associated with all aspects of administration encourage a consistent approach across an enterprise. This kind of approach, when applied to PCI DSS, would help improve the consistency, effectiveness, and efficiency of change control across a company and increase the likelihood that an auditor would find a company's practices acceptable.

Another benefit of combining the structure of ISO 27002 and the specific requirements of PCI DSS is that the PCI DSS helps organizations define three of the most challenging aspects of ISO compliance: scope of compliance, data classification, and data handling. Armed with these constraining requirements, organizations can define policies and procedures that are consistent with best practice as specified by ISO and directly address PCI DSS compliance.

For example, PCI DSS defines what aspects of credit card data are sensitive. It describes access control requirements for credit card information, encryption requirements for transmission and storage, and even the testing necessary to verify effectiveness of controls. These requirements allow organizations to state how systems must be configured, how employees must treat data, and how an organization monitors the effectiveness of its controls.

Dealing with the complexity of compliance assessments

As has been pointed out in many different ways, good security is not an end-game state; it is a way of life: a process for continually making your environment more stable and your critical assets better protected. Looking at these standards as a way of reaching a certain level of compliance can be a daunting task.

We believe this is all much easier if you take a life cycle approach and remember that the process is something that will be iterated many times: education, assessment, and remediation. Running through over 200 requirements for PCI DSS and over 130 control objectives for ISO 27002 can be an overwhelming exercise if done as a monolithic task.

A better way is to think of it as a 3-part cycle. In the first part of the cycle you are trying to educate. Go through the high-level sections of each section and try to come to consensus on

what each of the them means to your business and talk about how you deal with them now. This can be achieved in a small amount of time and helps to crystallize your thoughts and get you all on the “same page” for the more detailed analysis to follow.

In the second part of the cycle you actually perform an assessment: you literally walk through all (200 or 130+) control requirements and specifically note if you are compliant, partially compliant, non-compliant, or not applicable to your business. In those areas where you are deficient, you note what needs to change to get you to a compliant state.

You can do this assessment in two different, ways: validated or not. That is, if you are performing a validated assessment you not only ask the question, “How do you satisfy this requirement?” you then literally inspect everything that was involved for that requirement, e.g., read the actual policy, look at the system configuration, or review the documented process. A validated assessment is obviously very time-consuming and thorough. You need to decide what level of review makes sense in your business context based on market need and available resources.

In the last part of the cycle, after you have had time to make changes to those controls that were not in full compliance, you review the remediation steps that have been taken and decide if you are now in the desired state. The process of going through this cycle will not only educate your organization on where you stand, but give you opportunity to think about each requirement or control objective not only on a one-by-one basis, but also as a whole. You’ll understand what you are doing well, what you are doing poorly, and most importantly, what you are not yet doing at all.

Putting it all together

A growing number of organizations are building security programs according to standard frameworks like ISO 27002. These frameworks are allowing organizations to factor com-

pliance with multiple regulations and contracts into their security programs in a consistent and effective manner.

Using a standard as the underlying security framework enables organizations to plan and invest strategically. They can develop multi-year security and compliance road maps based on business priorities. They can invest in solving root cause problems, rather than treating symptoms.

At the same time, depending on your line of business, your organization will need to comply with other industry-specific standards (HIPAA, SOX, PCI DSS) as well. It may not be obvious, but using ISO 27002 as the underlying framework will help ensure a better overall security stance while at the same time satisfying the need to prove that you are compliant with other specific security requirements.

About the Authors

Brad Johnson, vice president of SystemExperts Corporation, is a well-known authority in the field of distributed systems, security standards, penetration testing, middleware, and practical intrusion detection, participating in the Open Software Foundation (OSF), X/Open, and the IETF, and has published extensively about open systems. He may be reached at brad.johnson@systemexperts.com.



Richard E. Mackey, SystemExperts Corporation, has advised a wide range of companies on the security aspects of compliance with regulations like Sarbanes Oxley, PCI, HIPAA, and Gramm Leach Bliley. Most recently he has been focusing his efforts on standards-based compliance, identity management, Web services, and the security aspects of Service Oriented Architectures. He may be reached at dick.mackey@systemexperts.com.

