White Paper

Achieving Security through Compliance

Policies, plans, and procedures—Part I

By Jeff Tucker, Principal Security Consultant
McAfee® Foundstone® Professional Services

Table of Contents

Overview 3

The Rock Foundation 3

Governance 3

- Organization structure: The chief information security officer (CISO) 3
- Security governance committee 4

Policies 4

- General policy creation guidelines 4
- Compliance and exceptions 5
- Enterprise information security policy 5
- Critical data security policy 5

Plans, Designs, and Procedures 6

- Plans and designs 6
- Procedures 6

Tips for Success 7

- General 7
- Policies 7
- Procedures 7

Conclusion 7

About the Author 8

About McAfee Foundstone Professional Services 8

Overview

This is the first part of a six-part series on compliance-driven security. This paper will illustrate how a well-structured security governance program with fully developed and implemented policies, plans, and procedures will strengthen an organization's security posture.

Many have said achieving compliance does not mean security for the organization This is so very true when organizations implement security standards such as NIST 800-53, ISO 27002, and the PCI data security standard (DSS) with a "check box" mindset—doing the least required to check off the box for the specified control. In many cases, this is not a deliberate act, but a result of management not fully understanding how high the bar should be. This series of white papers will illustrate compliance-driven security by reviewing the well-known and widely adopted PCI DSS and the principles that should drive its implementation. Whether you are working with ISO, NIST, or PCI standards, the concepts remain the same and apply to all organizations that must implement requirements from a specified security standard.

Starting with policies, plans, and procedures may seem counterintuitive as most organizations begin rolling out IT environments to support their operations by implementing a network, standing up computer systems, addressing vulnerabilities, implementing access controls, and perhaps enabling logging on some systems. However, as with all things, planning is important so take a moment to think things thorough and establish policies, devise plans, create designs, develop procedures, and then implement your IT solutions.

The Rock Foundation

Building an information security program upon a solid foundation is necessary for success. The following items should be considered part of that foundation:

1. *Charter*—Define the objectives, stakeholders, and managers of the information security program.
2. *Governance*—Following the success of IT governance and independent audit committees, security governance has emerged as an independent discipline. Create a security governance committee to align the security program with needs of the business, and to integrate the security program throughout the enterprise. With this new order, it has been recognized that there is an inherent conflict of interest when security falls under the department of information technology. As a result, the organizational structure needs realignment as explained below in "Organizational Structure."
3. *Policies*—Detail the policies that are the framework of the program.
4. *Plans, Designs, and Procedures*—Document the components to build, maintain, and operate the critical-data environment.

The following sections detail the important components of a security governance committee, the important policies, as well as the plans, designs, and procedures that should be included within the information security program.

Governance

The organization should be structured to accommodate a successful information security program. A security governance committee with well-defined responsibilities further ensures this success. This section will cover the items as they apply to most organizations in today's world.

Organization structure: The chief information security officer (CISO)

The CISO should report to the chief executive officer (CEO), chief financial officer (CFO), risk management officer (RMO), or chief compliance officer (CCO) rather than within the department of information technology. Responsibilities of the CISO should include, but are not limited to the following:

1. Chair the security governance committee.
2. Oversee information security operations.
3. Establish, publish, maintain, and disseminate security policy.
4. Ensure that security-related plans are established and regularly tested.
5. Ensure that written security operational procedures are in place and maintained.

Security governance committee

Key C-level positions and department heads should be included across the enterprise in the security planning process as members of a security governance committee. The CISO or appointee should chair the committee. Responsibilities should include, but not limited to the following:

1. Provide oversight of the information security program.
2. Guide the program to meet the security needs of the business.
3. Review and approve policies provided by the CISO or appointee.
4. Review and approve the security budget.

Policies

It is common to see policies that can be so broadly interpreted that they do not meet the requirements set forth by the ISO, NIST, and PCI security standards. The missing piece is authoritative leadership that sets the security tone and direction. The corporate trend has been to write policies at a very high level and leaving the details to individual departments. This approach is not appropriate for security policies because it leaves every policy clause (statement) to independent interpretation and debate.

Information security policies manage and reduce risks, and thus it is important to draft policies that clearly set expectations. Use issue-specific or system-specific policies to bridge gaps between broad requirements and requirements that target unique topics. Provide the detailed requirements needed to implement the policy with standards. The recommended design should include:

- *Enterprise Information Security Policy (EISP)*—This applies to the entire organization and specifies the requirements and expectations of management to secure corporate information. This policy should clearly set the minimum bar height. There may be latitude on how to implement policy, but no room to avoid or circumvent policy.
- *Critical Data Security Policy (CDSP)*—Organizations that have a large general population (corporate, manufacturing, marketing, etc.) that has low security requirements while maintaining regulated or other critical data should create a CDSP[1] specifically for the environment in scope of regulatory requirements.
- *System and Issue Specific Policies*—Use additional issue-specific and system-specific policies to support the CDSP and support issue-specific policies with standards.

General policy creation guidelines

Regardless of the topic of a particular security policy, certain key considerations should be made during its creation. This section outlines the major considerations and sections that should be in place for an effective policy.

Tone and direction

A strong security policy must set tone and direction as there is strength in the details. It must clearly set expectation and define the minimum bar height. Thus, they must provide more detail than is normally seen in policies. Policy will not drive strong authentication by stating access computer systems should require strong authentication. They will not clearly define data protection by mandating that critical data will be protected. Strong policy statements are necessary to drive security. These statements presented here are weak because they do not set clear direction or minimum requirements. The following are examples of strong policy statements.

> *Example 1:* User access to all systems require strong authentication commensurate with the system's security classification. At a minimum, authentication will require a unique user ID and strong password, but may require stronger methods of authentication based on risk determination. At a minimum, passwords must be the strongest of the following; 1) as mandated by regulatory requirements, 2) vendor recommendations, 3) security best practices, or 4) risk assessment recommendations of the accessed data systems.

> *Example 2:* Data owners will use strong cryptography to protect all data with a security classification of high. At a minimum, the implementation of cryptographic algorithms, modules, and components must be FIPS compliant. The CISO will establish, implement, and maintain written cryptographic key management procedures, and will review these procedures at least annually, and update them as needed.

Establishment of plans and procedures

Policy must require the establishment and maintenance of written security operational procedures. Policy must identify required security plans for vital functions such as information security incident response, disaster recovery, business continuity, etc. If not required by policy, management cannot expect the creation of plans and procedure.

Compliance and exceptions

The policy should address compliance and exceptions. Some organizations avoid writing a strong policy statement fearing a state of non-compliance with their own policy. It is better that policy issue strong policy clauses, and address exceptions with and the enforcement of policy as follows:

- *Grace Period for New Requirements*—Owners of any system not compliant with this policy at the time of publication[2] must submit a security plan to the CISO no later than [time-period defined by policy] of the published date. The security plan will describe in detail, any existing security controls, additional compensating controls to be employed, and a road map to bring the system into compliance within [time period defined by policy] of the publish date of this policy.
- *Exceptions*—Include an exception clause to establish the process for cases where a system or process cannot currently comply with a policy. Exceptions should be:
  1. Granted on a case-by-case basis.
  2. Granted based on established criteria.
  3. Temporary, with an expiration date set in the exemption.
  4. Reviewed when the exemption expires.
- *Enforcement*—Failure to follow policy without an authorized exemption should have consequences. Either explicitly or by reference to the EISP or appropriate corporate policy, state enforcement measures in the policy.

Enterprise information security policy

A strong security policy sets the security tone for the whole entity and informs personnel[3] management's security expectations. All personnel should be aware of the sensitivity of data and their responsibilities for protecting it. ISO, NIST, and PCI security standards require policies, plans, and procedures because experience has shown that their absence leaves ambiguity concerning the level of effort, controls, and safeguards management expects to be implemented in order to protect sensitive information. This ambiguity may lead to significant security gaps and thus it is important to add great detail to the policy.

Critical data security policy

A CDSP is an issue-specific policy that addresses the elevated security requirements for the in-scope data environment. Extra care should be taken when developing the scope and design of the CDSP as described in this section.

Scope

The CDSP must clearly define the scope. This does not mean that it should list every in-scope person, process, and system, but it should provide a clear definition.

Example Scope: This policy applies to the environment comprised of the critical data environment (CDE) and the people, processes, and system components in or that can connect to the CDE, and to systems and personnel that directly support the processing, transportation, or storage of 'critical data.' From a technology perspective, the CDE is the network(s) that host any system component that processes, transmits, or stores 'critical data' (that is, critical data systems). However, the critical data environment is also comprised of people and processes that handle 'critical data.'

Design

The CDSP should be designed as a single document with a section for each major topic or control family that maps to the regulatory requirements to which you must comply. These sections will contain subsections for each main requirement.

Example Design: The PCI data security policy will contain six sections that map directly to the DSS control groups listed below. Each of these sections will contain policy to implement each of their DSS Requirements. Therefore, "Build and Maintain a Secure Network" will address requirements 1 and 2.

1. Build and Maintain a Secure Network.
2. Protect Cardholder Data.
3. Maintain a Vulnerability Management Program.
4. Implement Strong Access Control Measures.
5. Regularly Monitor and Test Networks.
6. Maintain an Information Security Policy.

Plans, Designs, and Procedures

The organization needs plans, design documents, and procedures to build, maintain, and operate the critical data environment. Many organizations view these documents as time-consuming inconveniencies. However, these documents can do wonders for your organization whether contractual requirements as with PCI or legislative action as with the Federal Financial Institutions Examination Council (FFIEC), FISMA, and HIPAA are driving the security requirements you must implement. If for no other reason, create these documents to make quick work of security audits and assessments.

Plans and designs

Plans prepare for an event. It may be deployment of systems, developing software, or responding to a security incident. The saying "failure to plan, planning to fail" rings true in nearly every case. Design documents should supplement plans when needed, or be standalone documents that describe system or environment architecture and how the pieces fit together. Designs provide an understanding of interdependencies between components, and an understanding of the consequences of a failure of a single component. Design documentation is a job-saver for those who need to make changes to a system, network, or environment. Required plans and designs should include, but not limited to the following.

- System design.
- Security architecture.
- Network architecture.
- Systems security plan.
- Security awareness training.
- Risk management and treatment.
- Information security incident response.
- Disaster recovery and business continuity.

Procedures

Procedures, in this case, are not systematic instructions, but rather, a guide on how to operate something or execute a group of tasks to achieve an outcome. Technical areas may need task-level procedures to guide technicians through complicated tasks. However, in general, task-level procedures are not what auditors are looking for when they ask for procedures. Procedures should drive security operations, and integrate security in areas not operated by the security department. Policy should require CISO review and approval for all procedures for processes that may affect data security. For example, IT operations may perform user account management. This process has a significant security impact, and the CISO should review and approve the procedures for this process and work with IT operations to establish a secure process.

Tips for Success

Policy creation can be a time-consuming and somewhat cumbersome task however once this "barrier to entry" is passed, your organization will be in a better overall position. This section provides tips to help you avoid the common pitfalls.

General

1. Engage security professionals experienced in technical writing to author policies so that they are clear and precise, and set clear direction.
2. Do NOT rely on canned generic security policies and procedures or templates. These will not address your organization's needs.

Policies

1. Establish policies based on an assessment of the organization's raw fundamental risks without consideration of any security controls, safeguards, and countermeasures. The policies will establish security controls, safeguards, and countermeasures.
2. Reply on experience security-management professionals to create policies.
3. CISO should create information security policies.
4. Do not permit the governed (IT, operations, call center, etc.) to create their own security policies. They should be included in the creation of procedures.

Procedures

1. Make them relevant to operations.
2. Write them to front line managers and lead personnel.
3. Include subject matter experts during the development of procedures.
4. CISO should review and authorize operational security procedures.

Conclusion

Regulatory requirements mandate security policies and procedures. Compliance with these requirements drives the security program when policies are strong, clear, and complete. Policy must set expectations by defining minimum requirements. Incorporating issue-specific and system-specific policies and standards set further requirements and will add clarity. Structuring the organization chart so the CISO is independent from the technology department removes conflicts of interest and established higher integrity. Finally, establishing a security governance process incorporates strong security through the organization.

About the Author

Jeff Tucker is a principal consultant for McAfee® Foundstone® Professional Services and a graduate of Bellevue University Nebraska earning a Master of Science Degree in Security Management and a Bachelor of Science Degree in Computer Information Systems focusing on web-based networking. Jeff is a member of the Strategic Consulting Team in the capacity of Service Line Lead for PCI and FISMA. Jeff's certifications include CISA, CISSP, QSA, and MCSE. Jeff serves McAfee as an Engagement Manager of Security Control Assessment teams that include database analyst, network security testers, web-application penetration testers, and compliance assessors.

About McAfee Foundstone Professional Services

McAfee Foundstone Professional Services, a division of McAfee, offers expert services and education to help organizations continuously and measurably protect their most important assets from the most critical threats. Through a strategic approach to security, McAfee Foundstone identifies and implements the right balance of technology, people, and process to manage digital risk and leverage security investments more effectively. The company's professional services team consists of recognized security experts and authors with broad security experience with multinational corporations, the public sector, and the US military. http://www.mcafee.com/us/services/mcafeefoundstone-practice.aspx

About McAfee

McAfee, a wholly owned subsidiary of Intel Corporation (NASDAQ: INTC), empowers businesses, the public sector, and home users to safely experience the benefits of the Internet. The company delivers proactive and proven security solutions and services for systems, networks, and mobile devices around the world. With its visionary Security Connected strategy, innovative approach to hardware-enhanced security, and unique global threat intelligence network, McAfee is relentlessly focused on keeping its customers safe. http://www.mcafee.com

[1] These policies could be labeled as FISMA, GLBA, HIPAA, or PCI data security policies.

[2] This is the date that the security governance committee approved and signed the policy for use.

[3] Personnel include full-time and part-time employees, temporary employees, contractors, and consultants who are "resident" on the entity's site or otherwise have access to the data environment, networks, and systems.

McAfee
An Intel Company

2821 Mission College Boulevard
Santa Clara, CA 95054
888 847 8766
www.mcafee.com

60534wp_security-compliance_1013_fnl_ETMG