InformationShield

PCI Policy Compliance Using Information Security Policies Made Easy

PCI Policy Compliance Using Information Security Policies Made Easy

By David J Lineman
Information Shield

Contents

Introduction

Many organizations are building or updating written information security policies in response to the newly updated Payment Card Industry Data Security Standard [1] (PCI-DSS).

Written information security policies are fundamental to an effective information security program and required for compliance with many frameworks and regulations, including PCI, HIPAA, COBIT and many others.

In this paper we describe how Information Shield security policy products can be used to save time and money and enable compliance with the PCI standard.

All Contents Copyright 2007, Information Shield, Inc.

All design elements and content are copyright © Information Shield, Inc. unless otherwise noted. All rights reserved. All trademarks cited herein are the property of their respective owners.

No part of this publication may be reproduced, stored in a retrieval system, or transmitted in any form or by any means, electronic, mechanical, photocopying, recording, scanning, or otherwise, except as permitted under § 107 or 108 of the 1976 United States Copyright Act, without the prior written permission of the copyright holder.

Limit of Liability/Disclaimer of Warranty: While the copyright holders, publishers, and authors have used their best efforts in preparing this work, they make no representations or warranties with respect to the accuracy or completeness of its contents and specifically disclaim any implied warranties of merchantability or fitness for a particular purpose. The advice and strategies contained herein are based on the author's experience and may not be usable for your situation. You should consult with an information security professional where appropriate. Neither the publishers nor authors shall be liable for any loss of profit or any other commercial damages, including, but not limited to, special, incidental, consequential, or other damages.

Security Policy Requirements

Written information security policies are the foundation of any information security program. Information security policies provide the high-level business rules for how an organization will protect information assets. Written policies are required so that each member of the organization understands their information security responsibilities for their job role. Written information security policies also provide documented evidence of management's intent to protect information, and a baseline for both internal and external auditors to validate the security posture of the organization.

The fact that written security policies are fundamental to any security program is underscored by Requirement 12 within the PCI-DSS standard - Maintain a policy that addresses information security. [2] At the highest level, ISPME is designed to address the core requirements of PCI.

(See Table 1 - PCI Security Policy Checklist - which shows how ISPME addresses each subsection within Requirement 12 of the PCI Self-Assessment Questionnaire Version 1.0.)

Addressing Specific PCI Compliance

PCI compliance can be addressed using Information Security Policies Made Easy [3] (ISPME) at two fundamental levels. First, ISPME provides time-saving policy development tools and advice to aid the entire policy development process. Second, ISPME provides pre-written policy statements covering each topic within the PCI standard. The combination of pre-written policy statements and expert advice on the policy development process will save organizations valuable time.

Policy Development Tools

ISPME provides a variety of time-saving tools to help organization manage the policy development process. We use the word "process" because policy development is not a one-time project. An effective written information security policy program requires organizations to regularly update policies based on the latest risks to the organization. This implies that organizations must develop a formal process for developing, approving, integrating, and deploying written policies on a regular basis.

ISPME provided the following time-savings tools:

Detail Policy Development Project Guidance – ISPME contains over 40 pages of expert advice on how to build and develop information security policies. This tutorial is based on the 20 year information security experience of Charles Cresson Wood, CISSP, CISM. The guidance includes helpful checklists to use in the development and deployment of policies, and includes an outline for a policy management program.

Valuable Policy Development Forms and Templates – ISPME contains a number of time-saving forms that are required within an effective written policy program. Examples include a sample Agreement to Comply with Information Security Policies (for all users) and a Sample Risk Assessment Form to process and manage exceptions to policy.

Policy Development Resources – ISPME contains a number of time-saving resources and references including periodicals, web sites and professional organizations that may help you develop policies more quickly and effectively.

Complete Pre-Written Documents – ISPME contains seventeen complete, pre-written information security policy documents addresses some of the most critical organizational security needs. Examples include electronic mail, internet acceptable use, firewalls, network security, data privacy and many others.

Addressing Specific PCI Information Security Topics

ISPME makes it easy to develop written policies that address each of the 12 requirement areas of PCI DSS.

Policy Statement Library – The core of ISPME is a complete library of over 1400 individual security policy statements that address thousands of topics and technologies. The policy library is organized around the ISO 17799 (ISO 27001) security framework, and includes over 120 separate information security domains. While the ISPME is based upon the ISO security standard, easy search and browsing facilities make it easy to locate specific written policies related to PCI-DSS. Policy statements can be easily filtered by target audience, security environment (low, medium, high) and keyword.

Each policy within the library contains valuable commentary to help organizations implement the given policy. The commentary describes the risks that each policy is designed to address, which greatly aids a formal risk-assessment process.

Policy Mapping Documents – ISPME contains high-level mapping documents which provide a guide for locating specific PCI-DSS security policies. Also included are maps for COBIT 4.0 [6] (used for Sarbanes-Oxley) and HIPAA [7]. Many organizations are required to demonstrate compliance with more than one regulation or framework. ISPME is designed to facilitate a best-practices approach which allows for audits against multiple standards and regulations.

"ISPME contains over 1400 individual policy statements addressing all of the core areas of PCI-DSS."

Sample ISPME Topics:

- Firewall Configuration
- Secure Passwords
- Viruses and Malicious Code
- Application Security
- User Authentication
- Risk Assessments
- Data Classification
- Security Organization
- Network Access Control
- Encryption
- Data Destruction
- Electronic Records
- Incident Response
- System Testing
- Secure Application Development
- Data Privacy
- Physical Security
- And 100 others…

PCI Security Policies Step-by-Step

A complete set of information security policies for PCI-DSS can be developed with the help of ISPME using four basic steps:

1. **Perform a Gap-Analysis with Current PCI Policies** - A sound first step is to compare your existing security policies against the requirements from PCI DSS. The ISPME table of contents is a useful tool to identify possible content gaps between your existing policies and a best-practices set of policies.

2. **Prioritize Missing Policies** – The results of Step 1, along with any organizational risk-assessment, can be used to prioritize a list of policy topics that must be covered to enable compliance. This worksheet can be used to track the progress of policies throughout the development lifecycle.

3. **Develop a policy development and review plan** – Use the instructions within ISPME to develop a written information security policy plan. This plan should include, at a minimum, a policy review and exception process, and definition of roles and responsibilities for all members of the organization who may have a role in policy development. Information Security Roles and Responsibilities Made Easy [5] will be a useful tool in the role definition and documentation process.

4. **Build and deploy written policies** – Once the plan has been developed and approved, organizations can beginning developing specific written policies based on existing content within ISPME. ISPME contains fifteen complete sample policy documents that can be used as an excellent starting point. The policy library provides 1400 individual policy statements that can easy be incorporated into existing documents.

Staying Up to Date – PolicyShield Policy Subscription

PolicyShield is a new information security policy subscription service based on ISPME. The goal of PolicyShield is to allow your organization to build and maintain a robust set of written information security policies with the least amount of effort. To achieve this goal, the PolicyShield library is regularly updated with new policies and resources to help you address new risks.

PolicyShield acts as your “on-demand” security policy consultant. Our team of information security professionals continually monitors the technology landscape to look for new risks to your organization’s information assets. These risk may include new threats (such as botnets), regulatory changes (including enforcement actions) and new technologies (instant-messaging, VOIP, etc.)

Each quarter we compile a list of new additions to the existing PolicyShield library. New additions may include pre-written information security policies, policy development resources, sample documents, news items and policy-related incidents. PolicyShield is an extremely cost-effective way for an organization to keep written policies up to date and help protect against the latest threats.

Table 1: Specific Security Policy Requirements for PCI DSS

Requirement 12: Maintain a policy that addresses information security.	
12.1 Are information security policies, including policies for access control, application and system development, operational, network and physical security, formally documented?	ISPME contains over 1400 individual pre-written security policies covering 123 different security topics as defined in ISO 17799:2005/ISO 27001. ISPME also contains 15 complete security policy documents covering key aspects of information security.
12.2 Are information security policies and other relevant security information disseminated to all system users (including vendors, contractors, and business partners)?	ISPME contains over 100 separate information security policy controls that related to outsourcing and third-party contracts
12.3 Are information security policies reviewed at least once a year and updated as needed?	ISPME helps organizations maintain an updated set of written policies by providing content updates with each new version. ISPME also provides time-saving tutorials on the policy development and review cycle from Charles Cresson Wood, CISSP, CISA
12.4 Have the roles and responsibilities for information security been clearly defined within the company?	Information Security Roles and Responsibilities Made Easy provides over 70 different pre-written information security related job descriptions and department mission statements, allowing organizations to quickly document roles and responsibilities. ISR&R also includes time-saving tools and techniques for developing an information security program.
12.5 Is there an up-to-date information security awareness and training program in place for all system users?	ISPME contains pre-written policies that allow organizations to document and develop and information security awareness program. ISPME contains over 1500 policy commentaries with detailed advice that can help drive awareness activities.
12.6 Are employees required to sign an agreement verifying they have read and understood the security policies and procedures?	ISPME comes with pre-written information security policies that document the responsibilities and rights of users, including a sample Agreement to Comply with Information Security Policies.
12.7 Is a background investigation (such as a credit- and criminal record check, within the limits of local law) performed on all employees with access to account numbers?	ISPME contains over 100 different pre-written information security policies covering the entire lifecycle of employee management, including pre-screening, during employment, and after termination.
12.8 Are all third parties with access to sensitive cardholder data contractually obligated to comply with card association security standards?	ISPME contains over 100 different information security controls relating the management of security with outsourcing contracts and third party access to sensitive information.
12.9 Is a security incident response plan formally documented and disseminated to the appropriate responsible parties?	ISPME contains over 80 different information security policies covering each aspect of incident reporting, management, handling and disclosure.
12.10 Are security incidents reported to the person responsible for security investigation?	ISPME contains pre-written policies for the reporting and documentation of security incidents.
12.11 Is there an incident response team ready to be deployed in case of a cardholder data compromise?	ISPME contains pre-written policies for the formation and documentation of a Computer Incident Response Team (CIRT), while ISR&R provides specific pre-written job responsibilities and mission statements for members of a Computer Incident Response Team.

References

[1] *Payment Card Industry (PCI) Data Security Standard, Self-Assessment Questionnaire Version 1.0*, Release: December 2004, PCI Standards Council.

[2] Payment Card Industry (PCI) Data Security Standard, Version 1.1 – Published September 2006, PCI Security Standards Council.

[3] *ISO/IEC 17799:2005 (ISO 27001) – Code of practice for information security management* - Published by ISO and available at BSI [http://www.bsi-global.org/]

[4] *Information Security Policies Made Easy, by Charles Cresson Wood* - Published by Information Shield, Inc. 2002-2005. [http://www.informationshield.com]

[5] *Information Security Roles and Responsibilities Made Easy, by Charles Cresson Wood* - Published by Information Shield, Inc. 2002-2005. [http://www.informationshield.com]

[6] *Control Objectives for Information Technology (COBIT™) 4th Edition* – Published by ISACA, November 2005. [http://www.isaca.org]

[7] *Health Insurance Portability and Accountability Act of 1996 (HIPAA): Final Security Rule.* Department of Health and Human Services; Published in the Federal Registrar. [http://aspe.hhs.gov/admnsimp/index.shtml]

About the Author

David Lineman is President and CEO of Information Shield. Mr. Lineman has 20 years of experience in software development, business consulting and security. He is the author of Information Protection Made Easy – A Guide for Employees and Contractors and is a frequent speaker on the subjects of information security policy and regulatory requirements.

About Information Shield

Information Shield is a global provider of security policy, data privacy and security awareness solutions that enable organizations to effectively comply with international security and privacy regulations. Information Shield products are used by over 7000 customers in 59 countries worldwide.

Information Shield, Inc.
2660 Bering Dr.
Houston, TX 77057
www.informationshield.com
sales@informationshield.com
P: 888.641.0505
F: 866.304.6704