Security Standards Council®

Standard: PCI Data Security Standard (PCI DSS)

Version: 1.0

Date: October 2014

Author: Security Awareness Program Special Interest Group
PCI Security Standards Council

Information Supplement:

Best Practices for Implementing a Security Awareness Program

Table of Contents

1 Introduction 1
1.1 Importance of Security Awareness 1
1.2 Intended Audience 2
1.3 Terminology 2
2 Best Practices in Organizational Security Awareness 3
2.1 Assemble the Security Awareness Team 3
2.2 Determine Roles for Security Awareness 3
2.2.1 Identify levels of responsibility 3
2.2.2 Establish Minimum Security Awareness 4
2.2.3 Determine the content of training and applicability based on PCI DSS 5
2.3 Security Awareness throughout the Organization 5
3 Security Awareness Training Content 7
3.1 All Personnel 8
3.2 Management 9
3.3 Specialized Roles 9
3.3.1 Cashier/Accounting Staff 10
3.3.2 Procurement Team 10
3.3.3 IT Administrators and Developers 10
3.4 Define Metrics to Assess Awareness Training 11
4 Security Awareness Program Checklist 12
Appendix A: Sample Mapping of PCI DSS Requirements to Different Roles, Materials and Metrics 13
Appendix B: Security Awareness Program Record 20
Acknowledgements 24

1 Introduction

In order for an organization to comply with PCI DSS Requirement 12.6, a formal security awareness program must be in place. There are many aspects to consider when meeting this requirement to develop or revitalize such a program. The best practices included in this information supplement are intended to be a starting point for organizations without a program in place, or as a minimum benchmark for those with existing programs that require revisions to:

- Meet PCI DSS requirements;
- Address the quickly and ever-changing data security threat environment;
- Reinforce the organization's business culture.

Establishing and maintaining information-security awareness through a security awareness program is vital to an organization's progress and success. A robust and properly implemented security awareness program assists the organization with the education, monitoring, and ongoing maintenance of security awareness within the organization.

This guidance focuses primarily on the following best practices:

- **Organizational Security Awareness:** A successful security awareness program within an organization may include assembling a security awareness team, role-based security awareness, metrics, appropriate training content, and communication of security awareness within the organization.
- **Security Awareness Content:** A critical aspect of training is the determination of the type of content. Determining the different roles within an organization is the first step to developing the appropriate type of content and will also help determine the information that should be included in the training.
- **Security Awareness Training Checklist:** Establishing a checklist may help an organization when developing, monitoring, and/or maintaining a security awareness training program.

The information in this document is intended as supplemental guidance and does not supersede, replace, or extend PCI DSS requirements. While all references made in this document are to PCI DSS version 3.0, the general principles and practices offered here may be applied to any version of PCI DSS.

1.1 Importance of Security Awareness

One of the biggest risks to an organization's information security is often not a weakness in the technology control environment. Rather it is the action or inaction by employees and other personnel that can lead to security incidents—for example, through disclosure of information that could be used in a social engineering attack, not reporting observed unusual activity, accessing sensitive information unrelated to the user's role without following the proper procedures, and so on. It is therefore vital that organizations have a security awareness program in place to ensure employees are aware of the importance of protecting sensitive information, what they should do to handle information securely, and the risks of mishandling information. Employees' understanding of the organizational and personal consequences of mishandling sensitive information is crucial to an organization's success. Examples of potential consequences may include

penalties levied against the organization, reputational harm to the organization and employees, and impact to an employee's job. It is important to put potential organizational harm into perspective for personnel, detailing how such damage to the organization can affect their own roles.

1.2 Intended Audience

This guidance is intended for any organization required to meet PCI DSS Requirement 12.6 to implement a formal security awareness program within their organization. The guidance is applicable to organizations of all sizes, budgets, and industries.

1.3 Terminology

Data Loss Prevention (DLP) Scanning: A process of monitoring and preventing sensitive data from leaving a company environment.

Phishing: A form of social engineering where an attempt to acquire sensitive information (for example, passwords, usernames, payment card details) from an individual through e-mail, chat, or other means. The perpetrator often pretends to be someone trustworthy or known to the individual.

Privileged Access: Users who generally have elevated rights or access above that of a general user. Typically, privileged access is given to those users who need to perform administrative-level functions or access sensitive data, which may include access to cardholder data (CHD). Privileged Access may encompass physical and/or logical access.

Social Engineering: As defined by (ISC)[2]: An attack based on deceiving users or administrators at the target site—for example, a person who illegally enters computer systems by persuading an authorized person to reveal IDs, passwords, and other confidential information.

2 Best Practices in Organizational Security Awareness

Security awareness should be conducted as an on-going program to ensure that training and knowledge is not just delivered as an annual activity, rather it is used to maintain a high level of security awareness on a daily basis.

Protecting cardholder data (CHD) should form part of any organization-wide information security awareness program. Ensuring staff is aware of the importance of cardholder data security is important to the success of a security awareness program and will assist in meeting PCI DSS Requirement 12.6.

2.1 Assemble the Security Awareness Team

The first step in the development of a formal security awareness program is assembling a security awareness team. This team is responsible for the development, delivery, and maintenance of the security awareness program. It is recommended the team be staffed with personnel from different areas of the organization, with differing responsibilities representing a cross-section of the organization. Having a team in place will help ensure the success of the security awareness program through assignment of responsibility for the program. The size and membership of the security awareness team will depend on the specific needs of each organization and its culture.

2.2 Determine Roles for Security Awareness

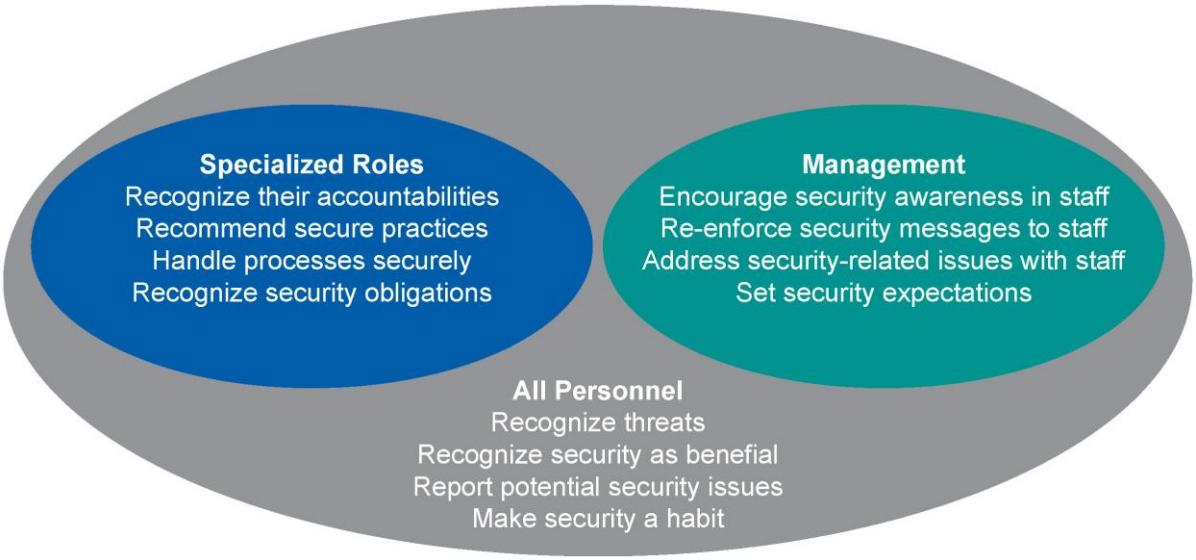
Role-based security awareness provides organizations a reference for training personnel at the appropriate levels based on their job functions. The training can be expanded upon—and subject areas combined or removed—according to the levels of responsibility and roles defined in the organization. The goal is to build a reference catalogue of various types and depths of training to help organizations deliver the right training to the right people at the right time. Doing so will improve an organization's security as well as help maintain PCI DSS compliance. Whether the focus is a singular, holistic, or a tiered approach, the content can be scoped to meet an organization's requirements.

All types of roles may not apply to all organizations, and some roles may need to be divided into subsections to align with responsibilities. This can be modified according to the requirements of the organization.

2.2.1 Identify levels of responsibility

The first task when scoping a role-based security awareness program is to group individuals according to their roles (job functions) within the organization. A simplified concept of this is shown in Figure 1 on the following page.

Figure 1: Security Awareness Roles for Organizations



The diagram above identifies three types of roles, **All Personnel, Specialized Roles,** and **Management.** A solid awareness program will help **All Personnel** recognize threats, see security as beneficial enough to make it a habit at work and at home, and feel comfortable reporting potential security issues. This group of users should be aware of the sensitivity of payment card data even if their day-to-day responsibilities do not involve working with payment card data.

Additional training for those in **Specialized Roles** should focus on the individual's obligation to follow secure procedures for handling sensitive information and recognize the associated risks if privileged access is misused. Examples of users in this category may include those processing payment cards, writing applications that process payment cards, building databases to hold CHD, or designing and building networks that CHD traverses. Each of these specialized roles requires additional training and awareness to build and maintain a secure environment. Additionally, specific training may be required to include understanding of PCI DSS and PA-DSS requirements.

Management has additional training needs that may differ from the two previous areas. Management needs to understand the organization's security policy and security requirements enough to discuss and positively reinforce the message to staff, encourage staff awareness, and recognize and address security related issues should they occur. The security awareness level of management may also need to include an overall understanding of how the different areas fit together. Accordingly, managers of staff with privileged access should have a solid understanding of the security requirements of their staff, especially those with access to sensitive data. Management training will also help with decisions for protecting the organization's information.

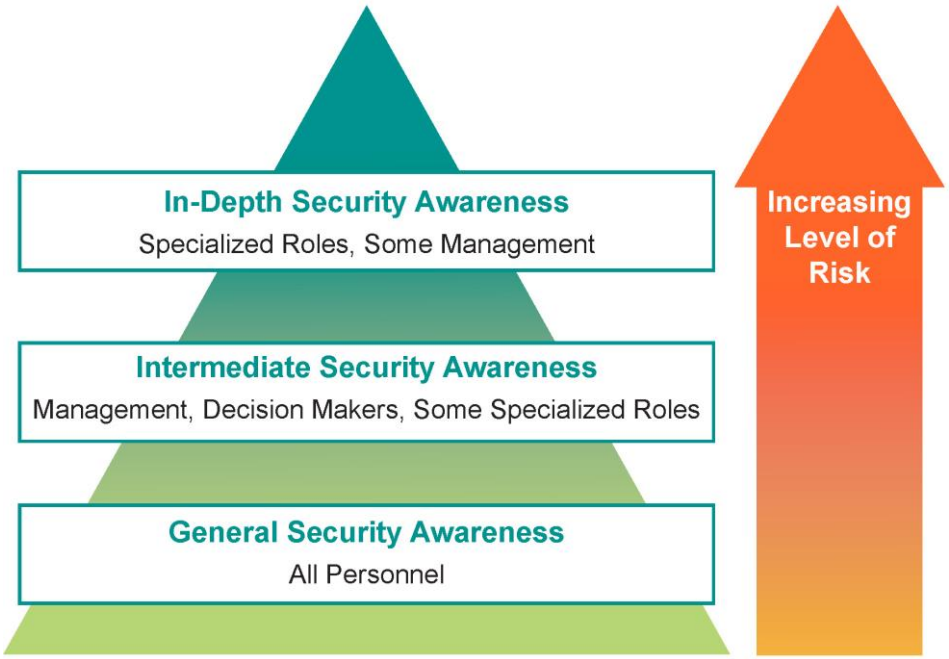
2.2.2 Establish Minimum Security Awareness

Establishing a minimum awareness level for all personnel can be the base of the security awareness program. Security awareness may be delivered in many ways, including formal training, computer-based training, e-mails and circulars, memos, notices, bulletins, posters, etc. The security awareness program

should be delivered in a way that fits the overall culture of the organization and has the most impact to personnel.

The following diagram depicts how the depth of awareness training should increase as the level of risk associated with different roles.

Figure 2: Depth of Security Awareness Training



2.2.3 Determine the content of training and applicability based on PCI DSS

Training content can be broken down further to map to applicable PCI DSS requirements. **Appendix A** contains a chart listing the high-level requirements of PCI DSS, with examples of roles listed that may need security awareness training in these control areas. Section 3, Security Awareness Training Content, contains further information related to training content for the different levels within an organization.

2.3 Security Awareness throughout the Organization

The key to an effective security awareness program is in targeting the delivery of relevant material to the appropriate audience in a timely and efficient manner. To be effective, the communication channel should also fit the organization's culture. By disseminating security awareness training via multiple communication channels, the organization ensures that personnel are exposed to the same information multiple times in different ways. This greatly improves how people remember the information presented to them. Content may need to be adapted depending on the communication channel—for example, the content in an electronic bulletin may be different than content in an instructor-led training seminar, even though both have the same underlying message. The communication channel used should match the audience receiving the training content and the type of content, as well as the content itself.

Electronic communication methods can include e-mail notifications, eLearning, internal social media, etc. It is important to target electronic security awareness notifications to the appropriate audience to ensure the information is read and understood. It is easier for electronic notifications to go unread or ignored by busy personnel. By targeting the material and communication channel to relevant personnel, the security awareness team can improve adoption of the security awareness program.

Non-electronic notifications may include posters, internal mailers, newsletters, and instructor-led training events. In-person security awareness events that involve active participation by personnel can be extremely effective. Audience size in an instructor-led presentation is important: the larger the group, the greater risk that content may not be communicated effectively, as individuals may lose focus on the material presented if they do not feel engaged. Including activities that engage the audience, such as scenario-based activities, helps ensure the concepts are understood and remembered. For example, a structured social-engineering exercise will teach personnel quickly how to identify a social-engineering attack and react appropriately. Internal seminars, training provided during lunch breaks (commonly called “lunch-and-learns” or “brown bag”), and employee social events are also great opportunities for the security awareness team to interact with personnel and introduce security concepts. **Appendix B** provides a list of the common methods to communicate security awareness throughout the organization.

It is recommended that communication of security awareness be included in new-hire processes, as well as role changes for existing personnel. Security awareness training may be combined with other organizational requirements, such as confidentiality and ethics agreements. Each job position in the organization should be identified based on level of data access required. See Section 2.2, Determine Roles for Security Awareness, for more information. To ensure that the security awareness team is notified whenever a role identified as needing security awareness is filled, it is recommended this step be included in the process for all new-hire/re-classifications. Inclusion in the new-hire/re-classification process ensures the overall training goals are promoted without reliance on individual organizational units.

Management leadership and support for the security awareness program is crucial to its successful adoption by staff. Managers are encouraged to:

- Actively encourage personnel to participate and uphold the security awareness principles.
- Model the appropriate security awareness approach to reinforce the learning obtained from the program.
- Include security awareness metrics into management and staff performance reviews.

3 Security Awareness Training Content

As discussed in Section 2.2, Determining Roles of Security Awareness, it is recommended training content be determined based on the role and the organization's culture. The security awareness team may wish to coordinate with the appropriate organizational units to classify each role in order to determine the level of security awareness training required for those specific job duties. This is vital in development of content, as it is just as easy to "over-train" an employee as it is to "under-train" an employee. In both cases, if information is not properly absorbed, it could lead to unnecessary organizational risk. Regardless of role, it is recommended that all staff receive basic security awareness training, developed in accordance with organizational policy. In addition to general security awareness training, it is recommended personnel be exposed to general concepts of cardholder data security, to promote proper data handling throughout the organization, according to their role in the organization.

Training materials should be available for all areas of the organization. Security awareness and training materials may be developed in-house, adapted from a professional organization's work, or purchased from a vendor. There are security awareness vendors that provide prepared materials such as computer-based training (CBT), posters, and newsletters. For example, PCI SSC and other eLearning vendors offer training on topics such as understanding PCI DSS, secure password practices, avoiding social engineering, avoiding malicious downloads, etc.

The following are examples of reference materials that may help in the development of a Security Awareness Program:

- National Institute of Standards and Technology (NIST) Special Publication 800-50, *Building an Information Technology Security Awareness and Training Program,* www.nist.gov
- International Standards Organization (ISO) 27002:2013*, Information technology -- Security techniques -- Code of practice for information security controls,* www.iso.org
- International Standards Organization (ISO) 27001:2013, *Information technology — Security techniques — Information security management systems,* www.iso.org
- COBIT 5 Appendix F.2, *Detailed Guidance: Services, Infrastructure and Applications Enabler, Security Awareness*, www.isaca.org/cobit

Additionally, due to the increased focus on cyber security awareness, many government agencies and industry bodies provide training materials to the public at no cost.

Choosing which materials to use in a security awareness training program is highly dependent on the organization. Each organization should consider the time, resources, and culture when selecting the materials to use for the security awareness training. Please see "Training Materials" in **Appendix A** for more information and examples. All best practices listed here may be included in an organization's security awareness program; however, the best practices are not a requirement.

3.1 All Personnel

It is recommended that general security training for all personnel include defining what constitutes cardholder data (CHD) and sensitive authentication data (SAD) and the organization's responsibility to safeguard both. A high level overview of the importance of the PCI DSS may also be included; to ensure personnel fully understands the purpose behind an organizational policy to safeguard cardholder data. To ensure all personnel are engaged stakeholders in the security awareness program, the roles and responsibilities of all staff to protect CHD and SAD should be outlined during all security awareness training, in accordance with organizational policy.

Because data is at risk both in electronic form and in non-electronic (paper) form, it is recommended that the different ways to safeguard information for different media be covered at a basic level for all personnel. For instance, considerations for protecting data in electronic format may include secure storage, transmission and disposal. Considerations for paper-based formats may also include secure storage and disposal as well as a "clear desk" policy. Without an understanding of how different media types need to be protected, personnel may inadvertently handle data in an insecure manner.

Another important consideration for inclusion in general security training is awareness of social engineering attacks. One way an attacker may use social engineering is to acquire a user's credentials and work their way through the organization from a low-security area to a high security area. Tailoring this awareness to reflect the types of attacks that the organization may encounter provides the most effective results. Users should be aware of the common methods by which fraudsters, hackers or other malicious individuals might try to obtain credentials, payment card data, and other sensitive data, to minimize the risk of personnel unintentionally disseminating sensitive information to outsiders. Training in organizational policies and procedures that specify proper data handling, including sharing and transmission of sensitive data, is also recommended.

The training program should require personnel to acknowledge they have received and understand the content being delivered. This is crucial to the success of the security awareness program. If content is being delivered and not understood, the employee may still inadvertently put the organization's information at risk. Feedback on training content and comprehension are key to ensuring personnel understand the content and the organization's security policies.

Below is an example of content that is commonly included in general security awareness training:

- Organization's Security awareness policy
- Impact of unauthorized access (for example: to systems or facilities)
- Awareness of CHD security requirements for different payment environments
    - Card present environments
    - Card-not-present environments
    - Phone (individual or call center)
    - Mail
    - Fax
    - Online (eCommerce)
- Where to get further information on protecting CHD in the organization (for example, security officer, management, etc.)

- Importance of strong passwords and password controls
- Secure e-mail practices
- Secure practices for working remotely
- Avoiding malicious software – viruses, spyware, adware, etc.
- Secure browsing practices
- Mobile device security including BYOD
- Secure use of social media
- How to report a potential security incident and who to report it to (see PCI DSS Requirement 12.10)
- Protecting against social engineering attacks
  - In Person – Physical Access
  - Phone – Caller ID Spoofing
  - E-mail – Phishing, Spear Phishing – E-mail Address Spoofing
  - Instant Messaging
- Physical security
- Shoulder Surfing
- Dumpster Diving

NOTE: *General security awareness training should be implemented even for organizations that outsource all payment acceptance and processing, to ensure personnel are aware that sensitive information, including CHD, must be protected.*

3.2 Management

In addition to content for all personnel, management training should include more detailed information regarding the consequences of a breach to management stakeholders. Management should understand not only the monetary penalties of failing to safeguard CHD, but also the lasting harm to the organization due to reputational (brand) damage. This factor is often overlooked when organizations outsource payment processing, but is critically important.

As previously discussed, management will need to understand security requirements enough to discuss and reinforce them, and encourage personnel to follow the requirements. It is recommended that management security awareness training include specific content relevant to the area of responsibility, particularly areas with access to sensitive data.

Management that is security-aware better understands the risk factors to the organization's information. This knowledge helps them make well-informed decisions related to business operations. Managers who are security-aware can also assist with development of data security policies, secure procedures, and security awareness training.

3.3 Specialized Roles

The categories listed below are examples of some common roles and the training content that may be suitable for those users. Each organization's specialized roles may differ, and the type of training for each role will need to be carefully considered.

3.3.1 Cashier/Accounting Staff

When developing cashier/accounting staff security awareness training, it's important to remember that personnel in these roles are often the "first line of defense" as they are interacting directly with the customers and those customer's payment cards. Training for cashiers may include how to inspect point-of-sale (POS) devices for tampering at the beginning of each shift, and being on the lookout for suspicious behavior in areas where the public has access to payment terminals. PCI DSS Requirement 9.9.3 has additional information on training for the protection of payment-acceptance devices, such as verifying the identity of third-party persons claiming to be repair or vendor personnel and verifying requests to replace and return payment terminals.

3.3.2 Procurement Team

If an organization shares CHD or outsources a function that can impact the security of the cardholder data environment (CDE), certain requirements to ensure continued protection of the CHD and the CDE should be understood.

It is important that the personnel involved in the third-party procurement process understand how the security of the information shared with third parties can be impacted and the role the third parties play in the security awareness program. PCI DSS Requirement 12.8 outlines the steps for managing service provider relationships. The PCI DSS Third-Party Security Assurance Information Supplement provides further guidance for engaging with and maintaining relationships with third party service providers.

3.3.3 IT Administrators and Developers

System, Database, and Network Administrators and other staff with privileged access to computer systems that may store, process, or transmit CHD will require more detailed security awareness training that includes understanding the importance of secure system configurations for the protection of sensitive information.

While general security awareness training (as described in Section 3.1) forms the basis for the security awareness program for these job roles, additional training may be necessary to address the different methods by which the role handles CHD. It may also be appropriate for these roles to have a general understanding of the how the organization receives and processes payments.

For specialized roles, such as those who support systems and networks, vendor-provided recommendations and industry best-practice guides for secure configurations can be useful content to include in training. For example, the Centre for Internet Security (CIS) provides security benchmarks and recommended configurations for a variety of systems.

Application developers, system developers, and testing staff have access to underlying code base, which is critical to environment security. These users should be aware of their responsibilities to follow the organization's security policy, secure coding practices, and change control procedures as outlined in PCI DSS Requirement 6, and be aware of current information on security threats and effective countermeasures.

3.4 Define Metrics to Assess Awareness Training

Metrics can be an effective tool to measure the success of a security awareness program, and can also provide valuable information to keep the security awareness program up-to-date and effective. The particular metrics used to measure the success of a security awareness program will vary for each organization based on considerations such as size, industry, and type of training. The table below displays some metrics of a successful security awareness program and can be used as a starting point for developing metrics.

Metric	Training Effectiveness Indicator
Operational Metrics	
Reduced system downtime and network or application outages	Consistent, approved change-management processes; fewer malware outbreaks; better controls
Reduction in malware outbreaks and PC performance issues related to malware	Fewer opened malicious e-mails; increased reports from personnel of malicious e-mails
Increase in reports of attempted e-mail or phone scams	Better recognition by personnel of phishing and other social-engineering attempts
Increase in reporting of security concerns and unusual access	Increased understanding by personnel of risks
Increase in the number of queries from personnel on how to implement secure procedures	Better awareness by personnel of potential threats
DLP scanning and network traces are active but not detecting cardholder data outside the CDE	Better understanding by personnel of potential threats
Vulnerability scans are active and detect high or critical vulnerabilities	Decrease in time between detection and remediation
Vulnerabilities are addressed or mitigated in a timely manner	Better understanding by personnel of potential threats and risks to sensitive information
Training Program Metrics	
Increase in number personnel completing training	Attendance tracking and performance evaluations
Increase in number of employees with privileged access who have received required training	Attendance tracking and performance evaluations
Increase in personnel comprehension of training material	Feedback from personnel; quizzes and training assessments

4 Security Awareness Program Checklist

Having a checklist may help organizations plan and manage their security awareness training program. The information listed below may be used to assist with security awareness training and education planning. Inclusion and use of this information is not a requirement.

Creating the Security Awareness Program

- Identify compliance or audit standards that your organization must adhere to.
- Identify security awareness requirements for those standards.
- Identify organizational goals, risks, and security policy.
- Identify stakeholders and get their support.
- Create a baseline of the organization's security awareness.
- Create project charter to establish scope for the security awareness training program.
- Create steering committee to assist in planning, executing and maintaining the awareness program.
- Identify who you will be targeting—different roles may require different/additional training (employees, IT personnel, developers, senior leadership).
- Identify what you will communicate to the different groups (goal is shortest training possible that has the greatest impact).
- Identify how you will communicate the content—three categories of training: new, annual, and ongoing.

Implementing Security Awareness

- Develop and/or purchase training materials and content to meet requirements identified during program creation.
- Document how and when you intend to measure the success of the program.
- Identify who to communicate results to, when, and how.
- Deploy security awareness training utilizing different communication methods identified during program creation.
- Implement tracking mechanisms to record who completes the training and when.

Sustaining Security Awareness

- Identify when to review your security awareness program each year.
- Identify new or changing threats or compliance standards and updates needed; include in annual update.
- Conduct periodic assessments of organization security awareness and compare to baseline.
- Survey staff for feedback (usefulness, effectiveness, ease of understanding, ease of implementation, recommended changes, accessibility).
- Maintain management commitment to supporting, endorsing and promoting the program.

Documenting the Security Awareness Program

- Document security awareness program including all previously listed steps within "Creating the Security Awareness Program," "Implementing Security Awareness," and "Sustaining Security Awareness."

Appendix A: Sample Mapping of PCI DSS Requirements to Different Roles, Materials, and Metrics

The table in this appendix provides a sample format for organizations wishing to document how PCI DSS requirements could be incorporated into their training program frameworks. For each PCI DSS requirement, the table identifies potential roles that may be subject to training, sources for training materials, and metrics to measure the effectiveness of training in those control areas.

Roles and responsibilities are different for each organization, and any mapping of PCI DSS requirements to roles, training materials, and metrics will therefore vary from one organization to the next. The information in this Appendix is intended as an example and may be useful as a starting point for determining how PCI DSS requirements could apply to training for different roles within the organization, the materials that could be used for training in those areas, and how to measure results of the training.

The columns listed in the table are:

PCI DSS Requirements: This column contains both the requirement number and the description of the PCI DSS Requirement. There are both high-level and specific requirements included to better convey the applicability of requirements to specific roles within the organization.

Target Audience for Training: The audiences included in these columns are examples of roles within an organization that may need security awareness training. This column may be used to identify which roles need training related to the different PCI DSS Requirements. Please note that all personnel should receive the general security awareness training in addition to any training specific to the role and PCI DSS control area(s).

Source Content for Training Material: This column may be used to identify appropriate material for security awareness training on the specific PCI DSS control.

Metrics: This column contains examples of metrics that may be used to measure the success of the security awareness training in the specific PCI DSS control area.

Note: *This appendix is intended as guidance only and is for optional use at the discretion of the organization; completion of this appendix is not a requirement. The use of this checklist ultimately will depend on the specific type of training chosen by the organization.*

PCI DSS Requirement		Target audience for training[1]					Source Content for Training Materials	Metrics
		All	M	C/A	PT	IT		
Build and Maintain a Secure Network and Systems								
1.x	Install and maintain a firewall configuration to protect cardholder data.					X	• Industry standards and best practices for network and systems security—e.g., NIST, ISO, CIS, HIPAA. • Vendor reference materials and best practice documentation • Organization firewall change and approval policy, personal firewall policy, system standard build policy.	• Few if any network outages. • Changes implemented successfully with minimal disruption. • Reductions in standard build deviations.
1.4	Install personal firewall software on any mobile and/or employee-owned devices that connect to the Internet when outside the network—e.g., laptops used by employees—and which are also used to access the network.	X						
2.x	Do not use vendor-supplied defaults for system passwords and other security parameters.					X		

[1] A = All; M = Management; C/A = Cashiers/Accounting; PT = Procurement Team; IT = IT Admin & Developers

PCI DSS Requirement	Target audience for training[1]					Source Content for Training Materials	Metrics
	All	M	C/A	PT	IT		
Protect Cardholder Data							
3.x Protect stored cardholder data.		X			X	• Industry standards or regulations related to the protection of consumers private information—e.g., Gramm-Leach-Bliley Act (GLBA) for protection of consumer's private information, Sarbanes-Oxley (SOX) for protection of sensitive data related to financial reporting. • Vendor reference materials and best-practice documentation • Organization data retention and disposal policy, encryption key management policy, secure e-mail policy.	• DLP scanning and network traces do not detect PCI data.
3.7 Ensure that security policies and operational procedures for protecting stored cardholder data are documented, in use, and known to all affected parties.	X						
4.x Encrypt transmission of cardholder data across open, public networks					X		
4.2 Never send unprotected PANs by end-user messaging technologies—for example, e-mail, instant messaging, chat, etc.	X						

[1] A = All; M = Management; C/A = Cashiers/Accounting; PT = Procurement Team; IT = IT Admin & Developers

PCI DSS Requirement	Target audience for training[1]					Source Content for Training Materials	Metrics
	All	M	C/A	PT	IT		
Maintain a Vulnerability Management Program							
5.x Protect all systems against malware and regularly update anti-virus software or programs	X				X	• Vendor reference materials for anti-virus or anti-malware software. • Organization anti-virus/malware policy, vulnerability management policy, secure coding methodology, change control policy. • PCI DSS, OWASP Top 10, CWE/SANS TOP 25 Most Dangerous Software Errors, NIST, COBIT 5 Appendix F, CIS Security Benchmarks.	• Solid, consistent counts of malware being detected, cleaned, quarantined over time. • Reduction in PC performance issues caused by malware. • Few or no internally spread infections to multiple systems.
6.x Develop and maintain secure systems and applications		X			X		• Few if any system or application outages. • Updates and changes implemented successfully with minimal disruption. • Monthly reports show consistent, appropriate patching. • Reduction in build deviations. • Regular vulnerability scans show no high or critical vulnerabilities.
6.4 Follow change control processes and procedures for all changes to system components.					X		

[1] A = All; M = Management; C/A = Cashiers/Accounting; PT = Procurement Team; IT = IT Admin & Developers

PCI DSS Requirement		Target audience for training[1]					Source Content for Training Materials	Metrics
		All	M	C/A	PT	IT		
Implement Strong Access Control Measures								
7.x	Restrict access to cardholder data by business need to know		X			X	• Vendor reference materials on implementing detailed access controls within authentication/authorization environments. • Organization access control policy including information on how business need to know is determined and approved for different roles.	• No alerts of unusual access. • Regular access reviews show few required changes.
8.x	Identify and authenticate access to system components		X			X	• Vendor reference materials on two-factor authentication, password management, session controls, and implementing detailed access controls. • Organization access control policy, password policy, information security policy.	• Reviews of audit logs for failed access attempts show no inconsistencies.
9.x	Restrict physical access to cardholder data		X			X	• Physical security policy requirements. • General user awareness. • Organization visitor access policy, secure device-handling procedures, data retention and disposal policy.	• Monitoring show minimal inconsistent behavior. • Surveys of employee understandings of secured areas return high awareness quotient. • Reporting of unusual access or behaviors increases.
9.9	Protect devices that capture payment card data via direct physical interaction with the card from tampering and substitution.			X				

[1] A = All; M = Management; C/A = Cashiers/Accounting; PT = Procurement Team; IT = IT Admin & Developers

PCI DSS Requirement	Target audience for training[1]					Source Content for Training Materials	Metrics
	All	M	C/A	PT	IT		
Regularly Monitor and Test Networks							
10.x Track and monitor all access to network resources and cardholder data		X			X	• Industry standards or regulations related to access to sensitive data—e.g., NIST, ISO, GLBA, SOX. • Vendor reference materials and best-practice documentation. • Organization log-review procedures, change control policy, vulnerability-testing policy, penetration-testing methodology. • Common vulnerabilities found in the National Vulnerability Database, SANS CWE Top 25, etc.	• Reduced network, system, application outages. • Updates and changes implemented successfully with minimal disruption. • Monthly reports show consistent, appropriate patching. • Regular vulnerability scans show no high or critical vulnerabilities. • Vulnerabilities discovered are addressed in a timely manner or mitigated appropriately.
11.x Regularly test security systems and processes					X		

[1] A = All; M = Management; C/A = Cashiers/Accounting; PT = Procurement Team; IT = IT Admin & Developers

PCI DSS Requirement	Target audience for training[1]					Source Content for Training Materials	Metrics
	All	M	C/A	PT	IT		
Maintain an Information Security Policy							
12.x Maintain a policy that addresses information security for all personnel		X			X	• Industry standards or regulations related to background checks, privacy, and information security policies—e.g., FFIEC, SOX, HIPAA, NIST, ISO. • Organization information security policy, risk assessment process, third-party service provider management and monitoring policy, and incident response plan	• Malware infections reduced over time. • Increase in reporting of phishing attempts. • Increase in reporting of security concerns.
12.2 Implement a risk-assessment process		X					
12.6 Implement a formal security awareness program to make all personnel aware of the importance of cardholder data security.	X						
12.8 Maintain and implement policies and procedures to manage service providers with whom cardholder data is shared, or that could affect the security of cardholder data		X		X			
PCI DSS Appendix A: Additional PCI DSS Requirements for Shared Hosting Providers							
Shared hosting providers must protect the cardholder data environment		X			X	▪ Shared hosting provider policies and procedures for securing hosted environments	

[1] A = All; M = Management; C/A = Cashiers/Accounting; PT = Procurement Team; IT = IT Admin & Developers

Appendix B: Security Awareness Program Record

The sample table below provides a method for an organization to record how it is managing a security awareness program. The table includes the following columns:

- **Activity:** This column contains some of the key tasks that could be performed when implementing a security awareness program. Examples of how an organization may choose to implement each activity are also provided, such as types of training content, delivery methods, tracking and recording options, employee acknowledgements, and so on. The particular activities in this column will vary for each organization according to their individual program.
- **Implementation Details**: This column may contain details of how different elements of the program are implemented; for example, details of purchased training products or vendors, assignment of responsibilities for managing different delivery channels, roles those different training methods will apply to, and so on.
- **Frequency:** This column may be used to track the frequency that each training or activity is expected to occur—for example, upon hire or upon role change, annually, bi-annually, etc.
- **PCI DSS Reference**: This column may be used to map the information contained in the first three columns to particular PCI DSS requirements and/or testing procedures, which an organization may find useful when documenting its PCI DSS compliance during a self-assessment or completion of a ROC.

Note: *This appendix is intended as guidance only and is for optional use at the discretion of the organization; completion of this appendix is not a requirement. The use of this checklist ultimately will depend on the specific type of training chosen by the organization.*

Sample Activity	Implementation Notes	Frequency	PCI DSS Reference
Identify methods for creating security awareness materials:			Testing Procedure 12.6.1.a
Classroom training • Consider third-party on-site training. • Security Awareness Training team conducts training.			
Computer-based training • Also consider having a third party who has PCI experience train personnel. • Websites for training information—e.g., www.pcisecuritystandards.org.			
Poster campaigns • Display posters in break rooms and other employee areas.			
Newsletters • Provide employee newsletters highlighting PCI DSS security as it applies to the employees.			
E-mail communications • E-mails can be used to remind employees about security requirements responsibility.			
Screensavers • Screensavers can be used to remind employees to log off computers when away from their workstations and other useful security information.			
Security meetings / roundtables / lunch-and-learn sessions • Have lunch-and-learns to discuss card data security and allow employees to ask questions.			
Information Security Team branding • Elect a security team to arrange trainings and other functions as it relates to security awareness.			

Sample Activity	Implementation Notes	Frequency	PCI DSS Reference
Information Security promotions • Give personnel small prizes for answering questions correctly. Arrange ad-hoc security awareness events.			
Information Security Intranet • Display security messages on organizational intranet to remind personnel of the importance of cardholder data security.			
Identify methods for delivering security awareness training upon hire and annually:			Testing Procedure 12.6.1.b

Computer-based training
• Also consider having a third party who has PCI experience train personnel.
• Websites for training information:
  ○ www.pcisecuritystandards.org
  ○ www.mastercard.us/merchants/support/rules.html
  ○ usa.visa.com/merchants/protect-your-business/index.jsp			

HR onboarding (instructor-led training)			
HR onboarding (policy review and sign-off)			
Information Security Team presentations			
Identify methods for recording attendance on training:			Testing Procedure 12.6.1.b
Meeting agendas with attendees • Prepare an agenda for security items to be discussed with employees.			
Signed attendance sheets • Require signed acknowledgements that the employee understands and has completed security awareness training.			

Sample Activity	Implementation Notes	Frequency	PCI DSS Reference
HR onboarding checklists • Records of new hires requiring security awareness training.			
Computer-based training records • Ensure tracking and recording of who takes the training and whether it was completed successfully.			
Identify methods for ensuring all employees attend training:			Testing Procedure 12.6.1.b
HR monitoring of attendance and/or checklists			
Employee performance reviews • Making security awareness part of the review process for personnel who have access to cardholder data helps ensure personnel attend training.			
Computer-based training completion reports • Ability to pull reports from computer based training that shows who took the training, date taken, pass or fail.			
Identify methods for employees to acknowledge they have read/understood the information security policy at least annually:			Testing Procedure 12.6.2
E-mail acknowledgements • Employee e-mail acknowledgement of completion and understanding of the information security policy as proof of annual reviews.			
Signed policies • Obtain signed employee acknowledgement of reading of the security policy as proof of the annual requirement.			
Electronic signatures in computer-based training • Ability to electronically sign an acknowledgement that computer-based training has been completed.			

Acknowledgements

PCI SSC would like to acknowledge the contribution of the Best Practices for Implementing a Security Awareness Program Special Interest Group (SIG) in the preparation of this document. The Best Practices for Implementing a Security Awareness Program SIG consists of representatives from the following organizations:

403 Labs, LLC
Air Products & Chemicals
Akamai Technologies
Allstate
American Express
American Family Insurance
Aon
Aperia Solutions
atsec (Beijing) Information Technology Co., Ltd
Bally Total Fitness
Bank Of New Zealand
Bashas' Inc.
BB&T Corporation
bet365
Board of Trustees of the University of Arkansas
Bozzuto's Inc
Bridge Point Communications Pty Ltd
BrightLine CPAs & Associates, Inc.
British Airways PLC
BT PLC
CBIZ Security & Advisory Services, LLC
CDG Commerce
China Unionpay Co Ltd
Cisco
Citigroup Inc
Clydesdale Bank
Coalfire Systems, Inc.
Compass IT Compliance, LLC
Comsec
CradlePoint
Crosskey Banking Solutions
Crowe Horwath LLP
DataFlight Europe A/S
Deluxe Corporation
Diamond Resorts Corp.
Digital Defense, Inc.
Domino's Pizza Inc.
DST Output
DSW Inc.
Elavon Merchant Services
Ergonomic Solutions
EVO Payments International
Experian Information Services
Exxon Mobil Corporation
Fiscal Systems, Inc.
FishNet Security
Foresight IT Consulting Pty Ltd
Fortrex
Games Workshop Ltd
Gap Inc.
Gemserv Limited
Global Payments Direct Inc.
GuidePoint Security, LLC
Hitachi-Omron Terminal Solutions, Corp.
IBM Corporation
IQ Information Quality
Isis Mobile Commerce
Kiwibank Limited
KnowIT Secure AB
Lloyds Banking Group
MegaPath Inc
MobileIron, Inc.
Módulo Security Solutions S.A.
MTI Technology Ltd
Nettitude Ltd
Paciolan Inc.
Payment Software Company (PSC)
PayPal Inc.
Pier 1 Imports
Post Office
Princeton Payment Solutions LLC (dba CardConnect)
Progressive Casualty Insurance Company
Promocion y Operacion SA de CV (PROSA)
RBC Royal Bank
RBS
Secure Enterprise Computing
Secure Enterprise Computing
Secured Net Solutions Inc.
Security Risk Management
Sense of Security Pty Ltd
SISA
SIX Payment Services Ltd
Solutionary, Inc.
Starwood Hotels & Resorts Worldwide, Inc.
State Farm Mutual Automobile Insurance Company
Suncor Energy Inc.
Sword & Shield Enterprise Security Inc.
Sysnet Global Solutions
Telstra
Tesco Stores Ltd
The Brick Group
The Walt Disney Company
Tieto Latvia SIA
Transport For London
Trustwave Holdings, Inc
TUI Travel Plc
U.S. Bancorp
U.S. Cellular
UL Transaction Security PTY Ltd.
UPS (United Parcel Service)
Vendorcom
Verizon/CyberTrust
VigiTrust Ltd
Visa Inc.
Vodat International Limited
Xpient Solutions LLC
ZZ Servers

About the PCI Security Standards Council

The PCI Security Standards Council is an open global forum that is responsible for the development, management, education, and awareness of the PCI Data Security Standard (PCI DSS) and other standards that increase payment data security. Created in 2006 by the founding payment card brands American Express, Discover Services, JCB International, MasterCard and Visa Inc., the Council has more than 650 Participating Organizations representing merchants, banks, processors and vendors worldwide. To learn more about playing a part in securing payment card data globally, please visit: pcisecuritystandards.org.