Security Standards Council®

Standard: PCI Data Security Standard (PCI DSS)

Version: 1.1

Date: September 2017

Author: Penetration Test Guidance Special Interest Group
PCI Security Standards Council

Information Supplement:
Penetration Testing Guidance

Document Changes

Date	Document Version	Description	Pages
March 2015	1.0	Initial release	All
September 2017	1.1	A number of clarifications, including: • Clarified intent of “social engineering” in Terminology. • Clarified guidance on black-box testing. • Restructured Section 2.2 for better flow, and clarified language describing intent of PCI DSS Requirement 11.3. • Expanded guidance related to back-end APIs. • Updated references to PCI SSC resources. • Minor grammatical updates.	Various

Table of Contents

1 Introduction 4
1.1 Objective 4
1.2 Intended Audience 4
1.3 Terminology 4
1.4 Navigating this Document 5
2 Penetration Testing Components 6
2.1 How does a penetration test differ from a vulnerability scan? 6
2.2 Scope 7
2.2.1 External Penetration Test 8
2.2.2 Internal Penetration Test 8
2.2.3 Testing Segmentation Controls 8
2.2.4 Critical Systems 9
2.3 Application-Layer and Network-Layer Testing 9
2.3.1 Authentication 9
2.3.2 PA-DSS Compliant Applications 9
2.3.3 Web Applications 10
2.3.4 Separate Testing Environment 10
2.4 Segmentation Checks 10
2.5 Social Engineering 11
2.6 What is considered a “significant change”? 11
3 Qualifications of a Penetration Tester 12
3.1 Certifications 12
3.2 Past Experience 12
4 Methodology 14
4.1 Pre-Engagement 14
4.1.1 Scoping 14
4.1.2 Documentation 14
4.1.3 Rules of Engagement 15
4.1.4 Third-Party-Hosted / Cloud Environments 16
4.1.5 Success Criteria 16
4.1.6 Review of Past Threats and Vulnerabilities 16
4.1.7 Avoid scan interference on security appliances. 17
4.2 Engagement: Penetration Testing 17
4.2.1 Application Layer 18
4.2.2 Network Layer 18
4.2.3 Segmentation 19
4.2.4 What to do when cardholder data is encountered 19

IPR2025-01085
Orca Security EX1041 Page 3

4.2.5 Post-Exploitation 19
4.3 Post-Engagement 19
4.3.1 Remediation Best Practices 19
4.3.2 Retesting Identified Vulnerabilities 20
4.3.3 Cleaning up the Environment 20
4.4 Additional Resources 20
5 Reporting and Documentation 21
5.1 Identified Vulnerability Reporting 21
5.1.1 Assigning a Severity Score 21
5.1.2 Industry Standard References 22
5.2 Reporting Guidelines 22
5.2.1 Penetration Test Report Outline 22
5.2.2 Retesting Considerations and Report Outline 23
5.3 Evidence retention 24
5.3.1 What is considered evidence? 24
5.3.2 Retention 24
5.4 Penetration Test Report Evaluation Tool 25
6 Case Studies / Scoping Examples 27
6.1 E-commerce Penetration Test Case Study 27
6.2 Hosting Provider Penetration Test Case Study 30
6.3 Retail Merchant Penetration Test Case Study 35
Appendix A: Quick-Reference Table to Guidance on PCI DSS Penetration Testing Requirements 40
Acknowledgements 41
About the PCI Security Standards Council 43

IPR2025-01085
Orca Security EX1041 Page 4

1 Introduction

1.1 Objective

This information supplement provides general guidance and guidelines for penetration testing. The guidance focuses on the following:

- **Penetration Testing Components:** Understanding of the different components that make up a penetration test and how this differs from a vulnerability scan including scope, application and network-layer testing, segmentation checks, and social engineering.
- **Qualifications of a Penetration Tester:** Determining the qualifications of a penetration tester, whether internal or external, through their past experience and certifications.
- **Penetration Testing Methodologies:** Detailed information related to the three primary parts of a penetration test: pre-engagement, engagement, and post-engagement.
- **Penetration Testing Reporting Guidelines:** Guidance for developing a comprehensive penetration test report that includes the necessary information to document the test as well as a checklist that can be used by the organization or the assessor to verify whether the necessary content is included.

The information in this document is intended as supplemental guidance and does not supersede, replace, or extend PCI DSS requirements. The current version of PCI DSS at the time of publication is v3.2; however, the general principles and practices offered here may also be applicable to other versions of PCI DSS.

1.2 Intended Audience

This guidance is intended for entities that are required to conduct a penetration test whether they use an internal or external resource. In addition, this document is intended for companies that specialize in offering penetration test services, and for assessors who help scope penetration tests and review final test reports. The guidance is applicable to organizations of all sizes, budgets, and industries.

1.3 Terminology

The following terms are used throughout this document:

- **Application-layer testing:** Testing that typically includes websites, web applications, thick clients, or other applications.
- **Black-box testing:** Testing performed without prior knowledge of the internal structure/design/implementation of the object being tested.
- **Common Vulnerability Scoring System (CVSS):** Provides an open framework for communicating the characteristics and impacts of IT vulnerabilities.
- **Grey-box testing:** Testing performed with partial knowledge of the internal structure/design/implementation of the object being tested.

- **National Vulnerability Database (NVD):** The U.S. government repository of standards based vulnerability management data. This data enables automation of vulnerability management, security measurement, and compliance (e.g., FISMA).
- **Network-layer testing:** Testing that typically includes external/internal testing of networks (LANS/VLANS), between interconnected systems, and wireless networks.
- **Penetration tester, tester, or team:** The individual(s) conducting the penetration test for the entity. They may be a resource internal or external to the entity.
- **Social engineering:** Manipulation or deception of individuals into divulging confidential or personal information.
- **White-box testing:** Testing performed with knowledge of the internal structure/design/implementation of the object being tested.

1.4 Navigating this Document

This document is organized in such a way to help the reader better understand penetration testing in a holistic sense. It begins by providing background and definitions for topics common to all penetration test efforts (including scoping the test, critical systems to test, application and network-layer test inclusions, etc.). The document then moves on to practical guidance on selecting a penetration tester, methodologies that are used before, during, and after a test, guidelines for reporting and evaluating test results. The document concludes with case studies that attempt to illustrate the concepts presented in this supplement.

Appendix A provides a quick-reference table to specific sections of this document where guidance on a particular PCI DSS requirement can be found. This may be useful for those wishing to quickly correlate the penetration testing requirements and guidelines presented in PCI DSS Requirement 11.3.

2 Penetration Testing Components

The goals of penetration testing are:

1. To determine whether and how a malicious user can gain unauthorized access to assets that affect the fundamental security of the system, files, logs and/or cardholder data.
2. To confirm that the applicable controls required by PCI DSS—such as scope, vulnerability management, methodology, and segmentation—are in place.

There are three types of penetration tests: black-box, white-box, and grey-box. In a black-box assessment, the client provides no information prior to the start of testing. In a white-box assessment, the entity may provide the penetration tester with full and complete details of the network and applications. For grey-box assessments, the entity may provide partial details of the target systems. PCI DSS penetration tests are typically performed as either white-box or grey-box assessments. These types of assessments yield more accurate results and provide a more comprehensive test of the security posture of the environment than a pure black-box assessment. Performing a black-box assessment, when the entity provides no details of the target systems prior to the start of the test, may require more time, money, and resources for the deliverables to meet the requirements of PCI DSS.

2.1 How does a penetration test differ from a vulnerability scan?

The differences between penetration testing and vulnerability scanning, as required by PCI DSS, can be summarized as follows:

	Vulnerability Scan	Penetration Test
Purpose	Identify, rank, and report vulnerabilities that, if exploited, may result in an intentional or unintentional compromise of a system.	Identify ways to exploit vulnerabilities to circumvent or defeat the security features of system components.
When	At least quarterly and after significant changes[1].	At least annually and upon significant changes[2].
How	Typically a variety of automated tools combined with manual verification of identified issues.	A manual process that may include the use of vulnerability scanning or other automated tools, resulting in a comprehensive report.

[1] Refer to Section 2.6 of this document for guidance on significant changes.

[2] Some entities may be required to perform penetration tests more frequently. Refer to the current version of PCI DSS to understand specific requirements.

IPR2025-01085
Orca Security EX1041 Page 7

	Vulnerability Scan	Penetration Test
Reports	Potential risks posed by known vulnerabilities, ranked in accordance with NVD/CVSS base scores associated with each vulnerability. For PCI DSS, external vulnerability scans must be performed by an ASV and the risks ranked in accordance with the CVSS. Internal vulnerability scans may be performed by qualified personnel (does not require an ASV) and risks ranked in accordance with the organization's risk-ranking process as defined in PCI DSS Requirement 6.1. An external vulnerability scan is conducted from outside the target organization. An internal vulnerability scan is conducted from inside the target organization.	Description of each vulnerability verified and/or potential issue discovered. More specific risks that vulnerability may pose, including specific methods how and to what extent it may be exploited. Examples of vulnerabilities include but are not limited to SQL injection, privilege escalation, cross-site scripting, or deprecated protocols.
Duration	Relatively short amount of time, typically several seconds to several minutes per scanned host.	Engagements may last days or weeks depending on the scope of the test and size of the environment to be tested. Tests may grow in time and complexity if efforts uncover additional scope.

2.2 Scope

PCI DSS defines the cardholder data environment (CDE) as "the people, processes, and technology that store, process, or transmit cardholder data or sensitive authentication data."

The scope of a penetration test, as defined in PCI DSS Requirement 11.3, includes the entire CDE perimeter and any critical systems. This applies both to the external perimeter (public-facing attack surfaces) and the internal perimeter of the CDE (LAN-LAN attack surfaces).

The scope of testing may include locations of cardholder data, applications that store, process, or transmit cardholder data, critical network connections, access points, and other targets appropriate for the complexity and size of the organization. This should include resources and assets utilized by personnel to maintain systems in the CDE or to access cardholder data, as the compromise of such assets could allow an attacker to obtain credentials with access to or a route into the CDE.

All penetration testing should only be conducted as defined by the rules of engagement agreed upon by both parties. See Section 4.1.3, "Rules of Engagement."

2.2.1 External Penetration Test

The scope of an external penetration test is the exposed external perimeter of the CDE and critical systems connected or accessible to public network infrastructures. It should assess any unique access to the scope from the public networks, including services that have access restricted to individual external IP addresses. Testing must include both application-layer and network-layer assessments. External penetration tests also include remote access vectors such as dial-up and VPN connections.

2.2.2 Internal Penetration Test

The scope of the internal penetration test is the internal perimeter of the CDE and critical systems from the perspective of the internal network. Testing must include both application-layer and network-layer assessments.

Where the CDE is also the only internal network and there is no internal CDE perimeter, the scope of testing will typically be focused on critical systems. For example, testing activities may include attempting to bypass internal access controls intended to prevent unauthorized access or use of systems that store, process, or transmit CHD from those that do not.

In cases where there is an internal CDE perimeter, the scope of testing will need to consider the CDE perimeter as well as critical systems within and outside of the CDE. For example, the testing may attempt to exploit permitted access paths from systems on an internal network segment into the CDE.

When access to the CDE is obtained as a result of the testing, the scope of the penetration test may allow the tester to continue exploring inside the network and further the attack against other systems within the CDE, and may also include testing any data-exfiltration prevention (data-loss prevention) controls that are in place.

In all cases, the scope of internal testing should consider the specific environment and the entity's risk assessment. Entities are encouraged to consult with their assessor and the penetration tester to ensure the scope of the penetration test is sufficient and appropriate for their particular environment.

2.2.3 Testing Segmentation Controls

The intent of segmentation is to prevent out-of-scope systems from being able to communicate with systems in the CDE or impact the security of the CDE. When properly implemented, a segmented (out-of-scope) system component could not impact the security of the CDE, even if an attacker obtained control of the out-of-scope system.

If segmentation controls are implemented, testing of the controls is required to confirm that the segmentation methods are working as intended and that all out-of-scope systems and networks are isolated from systems in the CDE. The scope of segmentation testing should consider any networks and systems considered as being out of scope for PCI DSS to verify they do not have connectivity to the CDE and cannot be used to impact the security of the CDE.

The intent of this assessment is to validate the effectiveness of the segmentation controls separating the out-of-scope environments from the CDE and to ensure the controls are operating as intended.

2.2.4 Critical Systems

The term “critical systems” is used in PCI DSS to reference systems that are involved in the processing or protection of cardholder data. PCI DSS provides examples of critical systems that may be impacted by identified vulnerabilities including “security systems, public-facing devices and systems, databases, and other systems that store, process, or transmit cardholder data” (Requirement 6.1). However, for the purposes of a penetration test, there may be additional systems outside the CDE boundaries that could affect the security of the CDE. These systems should also be considered to be critical systems. Common examples of critical systems relevant to a penetration test might include: security systems (for example, firewalls, intrusion-detection systems/intrusion-prevention systems (IDS/IPS), authentication servers, e-commerce redirection servers, etc.), or any assets utilized by privileged users to support and manage the CDE. Please note that critical systems are defined by the entity, as each environment is different.

2.3 Application-Layer and Network-Layer Testing

Any software written by or specifically for the organization that is part of the penetration test scope should be subject to both an application and network-layer penetration test. This assessment helps identify security defects that result from either insecure application design or configuration, or from employing insecure coding practices or security defects that may result from insecure implementation, configuration, usage, or maintenance of software.

The remediation of vulnerabilities identified during an application-layer assessment may involve redesigning or rewriting insecure code. The remediation of vulnerabilities identified during a network-layer assessment typically involves either reconfiguring or updating software. In some instances, remediation may include deploying a secure alternative to insecure software.

2.3.1 Authentication

If the application requires user authentication to the custom software, testing should be performed against all roles or types of access assumed by these parties. Also, testing should be performed against any role or access type that *does not* have explicit authorization to cardholder data to verify accounts without access cannot compromise such data.

For customers running applications on multitenant servers that provide customers access to their cardholder data, authenticated testing should be performed to ensure customer access is properly restricted to only their own cardholder data. The customer should provide the penetration tester with credentials that have equivalent permission(s) as a customer user, to allow the penetration tester to determine whether those credentials allow access to data beyond the entity’s data.

2.3.2 PA-DSS Compliant Applications

If a payment application has been PA-DSS validated, the application’s functionality does not need to be tested as part of the entity’s PCI DSS compliance validation. However, the implementation of the application does need to be tested. This includes both the operating system and any exposed services, but not the payment application’s functionality (e.g., authentication, key management, transaction processing, etc.) since this was validated as part of the PA-DSS application validation.

2.3.3 Web Applications

It is common for an environment to host a web application that was not specifically coded for the organization such as commercial, off-the-shelf web-mail interfaces, document-sharing tools, file-transfer services, network-device administrative interfaces, etc. In these instances, the web application does not typically need an application-layer penetration test as the entity is not responsible for the source code of this type of software. Instead, the tester should perform a network-layer test and ensure the software was implemented, configured, and is currently being maintained in a secure manner (disabling or uninstalling unused services, blocking unused ports, applying current updates, etc.).

2.3.4 Separate Testing Environment

Because of the nature and the intent of penetration testing, such testing in a production environment during normal business hours may impact business operations, and attempts to avoid disruption may increase the time, resources and complexity of the testing. This is especially important for high availability systems that may be impacted by penetration testing in a production environment. To avoid disruptions and to speed up testing, a separate environment that is identical to the production environment may be used for testing instead of the production environment. The penetration tester would need to ensure the same application and network-layer controls as production exist in the testing environment. This may be accomplished through methods to map out the production environment to verify it matches the testing environment. This should be included in the rules of engagement. All exploitable vulnerabilities identified during the testing must be corrected on production systems and testing repeated to verify that security weaknesses have been addressed.

2.4 Segmentation Checks

PCI DSS Requirement 11.3.4 requires penetration testing to validate that segmentation controls and methods are operational, effective, and isolate all out-of-scope systems from systems in the CDE.

Therefore, a robust approach to penetration testing is recommended to satisfy this requirement by actively attempting to identify routes and paths from networks outside the CDE into the CDE. All segmentation methods need to be specifically tested. In very large networks, with numerous internal LAN segments, it may be infeasible for the penetration tester to conduct specific tests from every individual LAN segment. In this case, the testing needs to be planned to examine each type of segmentation methodology in use (i.e., firewall, VLAN ACL, etc.) in order to validate the effectiveness of the segmentation controls. The level of testing for each segmentation methodology should provide assurance that the methodology is effective in all instances of use. In order to effectively validate the segmentation methodologies, it is expected that the penetration tester has worked with the organization (or the organization's QSA) to clearly understand all methodologies in use in order to provide complete coverage when testing.

The penetration tester may choose to include systems located in these isolated LAN segments not directly related to the processing, transmission, or storage of cardholder data to ensure these systems could not impact the security of the CDE if compromised. See Section 4.2.3 for specific guidance on testing methodologies for validating segmentation controls.

IPR2025-01085
Orca Security EX1041 Page 11

2.5 Social Engineering

Social engineering is the attempt to gain information, access, or introduce unauthorized software into the environment through the manipulation of end users. PCI DSS reconfirms testing by requiring industry accepted penetration-testing approaches (many of which include social engineering as part of their approach) and to have an approach to penetration testing that "considers the threats and vulnerabilities experienced by merchants in the last 12 months." This may include social-engineering attacks as a method used for introducing malware into the environment.

Social-engineering tests are an effective method of identifying risks associated with end users' failure to follow documented policies and procedures. There is no blanket approach to social-engineering engagements. If an organization chooses to include social-engineering testing as part of its annual security review, the tests performed should be appropriate for the size and complexity of the organization and should consider the maturity of the organization's security awareness program. These tests might include in-person, non-technological interactions such as persuading someone to hold open a door, remote interactions such as having someone provide or reset a password, or convincing the end user to open a vulnerable e-mail attachment or hyperlink.

While PCI DSS does not require testing to include social-engineering techniques, an entity can incorporate it into its penetration testing methodology as an ongoing method to determine the effectiveness of the security awareness program. The frequency of social-engineering tests would be determined by the entity when establishing its security awareness program. End-user security awareness re-education might be sufficient remediation for users who fail a social-engineering test. The objective is that, over time, fewer and fewer employees are making poor decisions that could allow an attacker to compromise security. Additional guidance on establishing an effective and robust security awareness program can be found in the Document Library on the PCI SSC website.

Social-engineering testing may not be appropriate or provide a meaningful result for all organizations. Although social-engineering testing is not a requirement of PCI DSS, an organization may consider documenting the reason(s) for foregoing social-engineering testing and include applicable documentation with the internal and external penetration test reports, particularly if social-engineering attacks were encountered in the last 12 months.

2.6 What is considered a "significant change"?

Per PCI DSS Requirements 11.3.1 and 11.3.2, penetration testing must be performed at least annually and after any significant change—for example, infrastructure or application upgrade or modification—or new system component installations. What is deemed "significant" is highly dependent an entity's risk- assessment process and on the configuration of a given environment. Because of this variability, a significant change is not prescribed by PCI DSS. If the change could impact the security of the network or allow access to cardholder data, it may be considered significant by the entity. Penetration testing of significant changes is performed to ensure that controls assumed to be in place are still working effectively after the upgrade or modification.

3 Qualifications of a Penetration Tester

Qualified internal resources or a qualified third party may perform the penetration test as long as they are organizationally independent. This means the penetration tester must be organizationally separate from the management of the target systems. For example, in situations where a third-party company is performing the PCI DSS assessment for the entity, that party cannot perform the penetration test if they were involved in the installation, maintenance, or support of target systems.

The following guidelines may be useful when selecting a penetration tester (or team) to understand their qualifications to perform penetration testing.

3.1 Certifications

Certifications held by a penetration tester may be an indication of the skill level and competence of a potential penetration tester or company. While these are not required certifications, they can indicate a common body of knowledge held by the candidate. The following are some examples of common penetration testing certifications:

- Offensive Security Certified Professional (OSCP)
- Certified Ethical Hacker (CEH)
- Global Information Assurance Certification (GIAC) Certifications (e.g., GIAC Certified Penetration Tester (GPEN), GIAC Web Application Penetration Tester (GWAPT), or GIAC Exploit Researcher and Advanced Penetration Tester (GXPN))
- CREST Penetration Testing Certifications
- Communication Electronic Security Group (CESG) IT Health Check Service (CHECK) certification

Note: *The PCI SSC does not validate or endorse these certifications.*

3.2 Past Experience

Appropriate penetration testing experience and qualifications cannot be met by certifications alone. Therefore, confirmation of additional criteria is necessary. For example, review of the extent of actual engagements that have been performed and relevant work experience are important considerations when selecting a penetration tester or team. The following questions are examples for assessing the qualifications and competency of a penetration tester or team. This is not an exhaustive list:

Q How many years' experience does the penetration tester have?

- If the penetration tester is in their first year of penetration testing, careful consideration should be given to the following questions to ensure the penetration tester has sufficient knowledge and is adequately trained to perform the penetration test. Consideration should also be given to the organization itself by verifying the training and QA processes to ensure penetration tester is qualified.

Q How many years has the organization that employs the penetration tester been performing penetration tests?

- References from other customers may be useful in consideration.

Q Has the penetration tester performed assessments against organizations of similar size and scope?

- For environments with high availability constraints, unstable system components, or large infrastructures, it is important to evaluate a tester's ability to handle those restrictions (bandwidth constraints, time constraints, etc.).

Q What penetration testing experience has the penetration tester or team had with the technologies in the target environment (i.e., operating systems, hardware, web applications, highly customized applications, network services, protocols, etc.)?

- When selecting a penetration tester, it is important to evaluate the past testing experience of the organization for which the tester works as it pertains to technologies specifically deployed within the target environment.
- Even if the penetration tester has not performed an assessment against certain specific technologies, if the tester has managed, maintained, been trained on, or developed said technologies, the tester may still be qualified to perform the penetration test.

Q Consider what other skills/qualifications the penetration tester has that will contribute to their ability to assess the environment.

- Are there industry-standard penetration testing certifications held by the penetration tester? (See Section 3.1.)
- What type of experience does the penetration tester have conducting network-layer penetration testing? Discussion of examples of network penetration testing efforts conducted by the organization may be warranted.
- Does the penetration tester have experience conducting application-layer penetration testing? Discussion of the penetration tester's familiarity with testing to validate the OWASP Top 10 and other similar application secure-coding standards and examples of application penetration testing efforts conducted by the organization may be warranted**.**

Note: *An organization may want to consider having a development-environment lab where penetration tests can be performed outside of the production environment and internal resources can train and increase their experience to help both their skills and potential certifications.*

4 Methodology

To ensure a successful penetration test, there are several activities and processes to be considered beyond the testing itself. This section provides guidance for these activities and is organized by the typical phases that occur during a penetration test: pre-engagement, engagement, and post-engagement.

4.1 Pre-Engagement

Before the engagement or testing begins, it is recommended that all parties involved (the organization, the tester, and where applicable, the assessor) be informed of the types of testing (i.e., internal, external, application-layer or network-layer) to be performed, how testing will be performed, and what the testing will target. By coordinating these details first, issues where the CDE scope is defined improperly or other issues arise that would require a retest might be avoided. This information may be gathered by conducting a pre-engagement call or during an on-site pre-engagement meeting.

4.1.1 Scoping

The organization being assessed is responsible for defining the CDE and any critical systems. It is recommended that the organization work with the tester and, where applicable, the assessor to verify that no components are overlooked and to determine whether any additional systems should be included in scope. The scope of the penetration test should be representative of all access points, critical systems, and segmentation methodologies for the CDE.

4.1.2 Documentation

Whenever possible, detailed documentation of any components within the scope should be made available to the tester. Common examples of such documents are application-interface documentation and implementation guides. This information will ensure the tester understands how functionality should work and whether results received are expected for the given scenario.

As a part of the scoping process, the organization should consider supplying the tester with the following documentation:

- A network diagram depicting all network segments in scope for the test (Refer to PCI DSS Requirements 1.1.2 and 1.1.3.)
- Cardholder data flow diagram
- A list of all expected services and ports exposed at the CDE perimeter
- Details of how authorized users access the CDE
- A list of all network segments that have been isolated from the CDE to reduce scope

The penetration tester will use this information during the assessment to identify unexpected attack vectors of the CDE in addition to known attack vectors, insufficient authentication controls, and to confirm the proper segmentation of out-of-scope environments.

IPR2025-01085
Orca Security EX1041 Page 15

4.1.3 Rules of Engagement

Prior to the commencement of any testing, it is important to document and agree upon the conditions in which testing is to be performed and the degree of exploitation, if any, that is permitted. This authorizes the tester to test the environment and ensure the organization understands what to expect from the penetration test.

Below are some examples of considerations that may be included in the rules of engagement:

- During what time window will testing need to be performed?
- Are there any legacy systems that have known issues with automated scanning? If so, how should testing be performed against these systems?
- Is there a preferred method of communicating about scope and issues encountered during the engagement?
- Does the entity want updates regarding ongoing exploitation of systems during the test? If so, the entity will need to determine whether they will or will not act upon such information or make changes to the environment. The entity may also want to implement its incident response plan in response to an exploit.
- Are there security controls that would detect or prevent testing? Consider whether these should be disabled or configured to not interfere during testing. (See Section 4.1.7 for further guidance.)
- If passwords or other sensitive data are compromised during the testing, does the tester need to disclose a list of all passwords and/or sensitive data accessed?
- If equipment owned by the tester is to be connected to the organization's network, what steps must be taken to ensure the equipment does not pose a threat to the environment (updated to the latest operating system, applied service packs and/or patches, etc.)?
- Does the tester need to provide all IP addresses from which testing will originate?
- Will sensitive data shown to be accessible during the test be retained by the tester during and after the penetration test? Only a proof-of-concept test should be performed, any cardholder data obtained must be secured in accordance with PCI DSS. (See Section 4.2.4 for more guidance.)
- What steps will be taken if the tester detects a previous or active compromise to systems being tested? (For example, activate incident response procedures and stop penetration test until resolution of the compromise situation.)

4.1.4 Third-Party-Hosted / Cloud Environments

Below are examples of considerations that may be included in the rules of engagement for third-party-hosted/cloud environments of the entity:

- If a service-level agreement requires approval from a third party before penetration tests can be conducted, the organization must receive approval from the third party (i.e., hosting provider, etc.) before the assessment is to take place.
- The scope may not include the infrastructure provided by the third party to the entity. The scope may include any systems managed, built, or utilized by the organization.
- Unless otherwise noted in the scope, web-management portals provided by the third party for the entity to manage its infrastructure should not be included in the penetration test—these interfaces should be tested and validated as part of the third party's PCI DSS compliance efforts, and evidence or attestation of validation should be provided to the customer.

4.1.5 Success Criteria

The intent of a penetration test is to simulate a real-world attack situation with a goal of identifying how far an attacker may be able to penetrate into the environment. Defining the success criteria for the penetration test allows the entity to set limits on the depth of the penetration test. Without agreeing upon the point at which the penetration test is complete, there is a possibility of the tester exceeding the boundaries and expectations of the target entity. This should be documented in the rules of engagement.

Possible success criteria may include:

- Direct observation of restricted services or data in the absence of expected access controls
- Compromise of an intermediary device used by privileged users to access the CDE
- Compromise of the domain used by privileged users
- No compromise of the target systems

The success criteria will be different for every environment and should be established during initial pre-engagement meeting prior to testing.

4.1.6 Review of Past Threats and Vulnerabilities

PCI DSS Requirement 11.3 requires a review and consideration of threats and vulnerabilities encountered by the assessed entity within the past 12 months. This is an historical look at real vulnerabilities experienced or discovered in the entity's environment since the last assessment. This information may provide insight to the process in place to handle these vulnerabilities.

IPR2025-01085
Orca Security EX1041 Page 17

The penetration tester should be familiar with current vulnerabilities seen by the industry over the past 12 months as well as take a detailed look at recent vulnerabilities experienced by the entity. Depending on the type of test to be performed (i.e., white box, grey box, black box), the following may or may not be considered in such a review:

- Vulnerabilities discovered by the entity which have not been remediated within the time period required by PCI DSS (example: quarterly), and/or by the vulnerability remediation requirements documented in the corporate security policy
- Existing compensating controls mitigating the noted vulnerabilities
- Deployments or upgrades in progress (consider both hardware and software)
- If applicable, threats or vulnerabilities that may have led to a data breach
- Validation of the remediation of previous years' penetration test findings
- Identification of industry "state of existing vulnerabilities" for purposes of tracking vulnerabilities that may have not been detected at the time of the most recent penetration test

The tester may gain additional insight of the target environment for this review by:

- Reviewing prior penetration test reports
- Reviewing previously issued Reports on Compliance or Attestations of Compliance
- Reviewing current vulnerability scan test results

4.1.7 Avoid scan interference on security appliances.

In many environments, active protection controls such as an intrusion prevention system or web active protection systems such as intrusion protection systems (IPS) and web application firewalls (WAF) may be deployed to protect exposed services. Because the intent of the penetration test is to evaluate the services' susceptibility to exploitation (vs. the active protection systems' ability to prevent attacks), interference with the penetration test should be avoided—entities are encouraged to review and be familiar with the section titled "Scan Interference" in the ASV Program Guide and configure active protection systems accordingly during testing.

This practice helps ensure that the services themselves are configured properly and have the minimal risk of being exploited in the event the active protection system fails or is somehow defeated or bypassed by an attacker.

4.2 Engagement: Penetration Testing

Each environment has unique aspects/technology that requires the tester select the most appropriate approach and the tools necessary to perform the penetration test. It is beyond the scope of this document to define or outline which approach, tools, or techniques are appropriate for each penetration test. Instead, the following sections provide high-level guidance on considerations for the approach, tools, or techniques.

Penetration testing is essentially a manual endeavor. In many cases, tools exist that can aid the tester in performing the test and alleviate some of the repetitive tasks. Judgment is required in selecting the appropriate tools and in identifying attack vectors that typically cannot be identified through automated means.

Penetration testing should also be performed from a suitable location, with no restrictions on ports or services by the Internet provider. For example, a penetration tester utilizing Internet connectivity provided to consumers and residences may have SMTP, SNMP, SMB, and other ports restricted by the Internet provider to minimize impact by viruses and malware. If testing is performed by a qualified internal resource, the test should also be performed from a neutral Internet connection unaffected by access controls that might be present from the corporate or support environments.

4.2.1 Application Layer

As mentioned in Section 2.3, the penetration tester should perform testing from the perspective of the defined roles of the application. The organization is strongly encouraged to supply credentials to allow the tester to assume the required roles. This will allow the tester to determine if, at any given role, the user could escalate privileges or otherwise gain access to data they are not explicitly allowed to access.

In instances where the organization has created new accounts for the tester to use, it is important that the organization ensure all roles and applicable security in the application have been set up to allow the tester to effectively test all functionality.

In instances where a web application utilizes a back-end API, the API may be in scope for the testing. The tester should understand the interaction between the web application and the backend, the functionality exposed by the API, as well as any security controls implemented to protect access to the API. Those, and other factors, will help determine whether the back-end API should be tested independently from the web application.

4.2.2 Network Layer

Since most protocols are well defined and have standard modes of interaction, network-layer testing is more suitable for automated testing. This makes automation the first logical step in a network-layer test. Because of such standardization, tools may be used to quickly identify a service, the version of the software, test for common misconfigurations, and even identify vulnerabilities. Automated tests can be performed much faster than could be expected of a human. However, simply running an automated tool does not satisfy the penetration testing requirement. Automated tools cannot interpret vulnerabilities, misconfigurations, or even the services exposed to assess the true risk to the environment. The automated tool only serves as a baseline indication of the potential attack surface of the environment. The penetration tester must interpret the results of any automated tools and determine whether additional testing is needed.

Using the documentation provided by the organization during the pre-engagement, the tester should:

- Verify that only authorized services are exposed at the CDE perimeter.
- Attempt to bypass authentication controls from all network segments where authorized users access the CDE, as well as segments not authorized to access the CDE.

4.2.3 Segmentation

The segmentation check is performed by conducting tests used in the initial stages of a network penetration test (i.e., host discovery, port scanning, etc.). It should verify that all out-of-scope LANs truly have no access to the CDE. For environments with a large number of network segments considered to be out of scope or isolated from the CDE, a representative subset can be used for testing to reduce the number of segmentation checks that need to be performed. Each unique segmentation methodology should be tested to ensure that all security controls are functioning as intended.

If it is determined during the segmentation check that a LAN segment thought to be out of scope has access into the CDE, the organization will either need to adjust the segmentation controls to block that access, or perform a full network-layer penetration test to characterize the access and the impact on PCI DSS scope.

4.2.4 What to do when cardholder data is encountered

If cardholder data is accessed during the penetration test, it is important that the tester notify the organization immediately. The tester should keep detailed documentation as to exactly what data was accessed and how it was accessed.

After being notified, the organization should immediately review how the cardholder data was retrieved and, as appropriate, should take steps to execute its incident response plan.

If the output of testing tools or activities includes cardholder data that was accessed by the tester during the engagement, it is important this output be secured in accordance with PCI DSS.

4.2.5 Post-Exploitation

The term “post-exploitation” refers to the actions taken after the initial compromise of a system or device. It often describes the methodical approach of using privilege escalation or pivoting techniques—which allows the tester, in this case, to establish a new source of attack from the new vantage point in the system—to gain additional access to systems or network resources. Penetration testers should be able to demonstrate the risk presented by exploitable systems to the CDE and what post-exploitation may likely occur with those systems.

4.3 Post-Engagement

After the engagement or testing has been performed, there are activities both parties should carry out.

4.3.1 Remediation Best Practices

Penetration testing efforts, while thorough, may not always guarantee exhaustive identification of every instance where a security control’s effectiveness is insufficient—e.g., finding a cross site scripting vulnerability in one area of an application may not reveal all instances of this vulnerability in the application. Often the presence of vulnerability in one area may indicate weakness in process or development practices that could have replicated or enabled similar vulnerability in other locations.

Therefore, it is important for the tested entity to carefully investigate systems or applications with the ineffective security controls in mind when remediating.

IPR2025-01085
Orca Security EX1041 Page 20

4.3.2 Retesting Identified Vulnerabilities

The organization should take steps to remediate any exploitable vulnerability within a reasonable period of time after the original test. When the organization has completed these steps, the tester should perform a retest to validate the newly implemented controls mitigate the original risk.

Remediation efforts extending for a long period after the initial test may require a new testing engagement to be performed to ensure accurate results of the most current environment are reported. This determination may be made after a risk analysis of how much change has occurred since the original testing was completed.

In specific conditions, the flagged security issue may represent a fundamental flaw in an environment or application. The scope of a retest should consider whether any changes occurring as a result of remediation identified from the test are classified as significant. All changes should be retested; however, whether a complete system retest is necessary will be determined by the risk assessment of those changes.

4.3.3 Cleaning up the Environment

It is important for the tester to document and disclose to the organization any alterations made to the environment (as permitted in the Rules of Engagement) during the test, including but not limited to:

- Accounts that were created as a part of the assessment either by the entity or the tester: the organization should then remove these accounts.
- Tools installed by the tester on the organization's systems: these tools should be removed at the end of the testing.

Removal of accounts and test tools will ensure the accounts or remnant tools could not be exploited or used against the organization.

4.4 Additional Resources

There are multiple industry-accepted methodologies that may provide additional guidance on penetration testing activities, including but not limited to:

- Open Source Security Testing Methodology Manual ("OSSTMM")
- The National Institute of Standards and Technology ("NIST") Special Publication 800-115
- OWASP Testing Guide
- Penetration Testing Execution Standard
- Penetration Testing Framework

5 Reporting and Documentation

The purpose of the report is to assist the organization in its efforts to improve its security posture by identifying areas of potential risk that may need to be remediated. Merely reporting lists of vulnerabilities is not helpful in this endeavor and does not meet the intent of the penetration test. The report should be structured in a way to clearly communicate what was tested, how it was tested, and the results of the testing.

This section provides guidance on documenting identified and/or exploited vulnerabilities, creating reporting templates, and evaluating a penetration test report.

5.1 Identified Vulnerability Reporting

Penetration test reports should include a discussion of the steps, vectors, and exploited vulnerabilities that lead to penetration during testing for which remediation and retesting are required. However, it is possible for the tester to identify vulnerabilities that were not necessarily exploitable but which are deemed to pose a potential risk to the environment. It is recommended that the report contain any findings that impact the security posture of the assessed entity even in cases where exploitation did not occur. Some examples of identified vulnerabilities that were not exploited for valid reasons and should be included in the report may be:

- Firewall misconfigurations that permit unauthorized traffic between secure and insecure zones
- Detection of credentials obtained through manipulation of a web-application error message that was not flagged during an ASV scan due to a low CVSS base score

5.1.1 Assigning a Severity Score

In order to prioritize remediation of the penetration test findings, it is a common practice during the reporting phase for a severity or risk ranking to be assigned for each detected security issue. The report should clearly document how the severity/risk ranking is derived.

In most cases, severity/risk ranking may be applied as a result of evaluating an industry-standard score (e.g., NVD, CVSS) against a threshold or value that indicates risk (i.e., high, medium, and low). However, it should be noted that it is possible for a vulnerability to exist that is inherent to a particular environment; therefore, a standardized score is not available.

When custom scoring is part of the risk-ranking process, the report should reflect a traceable set of reasoning for the modification of industry-standard scores or, where applicable, for the creation of a score for a vulnerability that does not have an industry-standard score defined.

5.1.2 Industry Standard References

Some well-known, industry-standard references include:

- National Vulnerability Database (NVD)
- Common Vulnerability Scoring System (CVSS)
- Common Vulnerabilities and Exposure (CVE)
- Common Weakness Enumeration (CWE)
- Bugtraq ID (BID)
- Open Source Vulnerability Database (OSVDB)

The Common Vulnerability Scoring System (CVSS) is an example of an open framework that may be referenced for assigning a baseline risk rating. The CVSS is the required scoring system for Approved Scanning Vendors (ASVs) to use for ranking vulnerabilities detected during PCI vulnerability scans. Using this system, a standardized vulnerability score can be adjusted through the evaluation of the traits of vulnerability within the context of a specific environment.

5.2 Reporting Guidelines

Comprehensive and consistent reporting is a critical phase of a penetration test. This section provides guidelines on common contents of an industry standard penetration test. It should be noted that these are only suggested outlines and do not define specific reporting requirements for PCI DSS penetration tests. Testers may have different sections, alternative titles, and/or report format, etc.; this outline represents data gathered from a number of penetration testing providers and the desires of customers.

5.2.1 Penetration Test Report Outline

- Executive Summary
  - Brief high-level summary of the penetration test scope and major findings
- Statement of Scope
  - A detailed definition of the scope of the network and systems tested as part of the engagement
  - Clarification of CDE vs. non-CDE systems or segments that are considered during the test
  - Identification of critical systems in or out of the CDE and explanation of why they are included in the test as targets
- Statement of Methodology
  - Details on the methodologies used to complete the testing (port scanning, nmap etc.). See Section 4 for details on methodologies that should be documented.
- Statement of Limitations
  - Document any restrictions imposed on testing such as designated testing hours, bandwidth restrictions, special testing requirements for legacy systems, etc.

- Testing Narrative
  - Provide details as to the testing methodology and how testing progressed. For example, if the environment did not have any active services, explain what testing was performed to verify restricted access.
  - Document any issues encountered during testing (e.g., interference was encountered as a result of active protection systems blocking traffic).
- Segmentation Test Results
  - Summarize the testing performed to validate segmentation controls, if used to reduce the scope of PCI DSS.
- Findings
  - Whether/how the CDE may be exploited using each vulnerability.
  - Risk ranking/severity of each vulnerability
  - Targets affected
  - References (if available)
    - CVE, CWE, BID, OSBDB, etc.
    - Vendor and/or researcher
  - Description of finding
- Tools Used
- Cleaning up the Environment Post-Penetration Test

  After testing there may be tasks the tester or customer needs to perform to restore the target environment (i.e., update/removal of test accounts or database entries added or modified during testing, uninstall of test tools or other artifacts, restoring active protection-system settings, and/or other activities the tester may not have permissions to perform, etc.).
  - Provide directions on how cleanup should be performed and how to verify security controls have been restored.

5.2.2 Retesting Considerations and Report Outline

If the noted findings will require remediation and retesting before an assessor can determine the entity has met PCI DSS Requirement 11.3, a follow-up test report may be provided. All remediation efforts should be completed and retested within a reasonable period of time after the original penetration test report was provided.

It is expected that the remediation test report will cover all identified/exploitable vulnerabilities that require remediation. Those identified vulnerabilities is may be medium or high for external penetration tests and those defined by the organization as medium or high for internal tests.

The following is an example of the sections to include in a retest report as defined in Section 5.2.1:

- Executive Summary
- Date of Original Test
- Date of Retest
- Original Findings
- Results of Retest

5.3 Evidence retention

5.3.1 What is considered evidence?

A typical penetration test involves obtaining and evaluating evidence using a formal methodology; evidence collected from the penetration test is used to determine the conclusion. Evidence is considered all information that supports the penetration tester's conclusions about the effectiveness of the security controls and the environment's overall security posture. The penetration tester should follow a systematic process to securely collect, handle, and store evidence.

Examples of evidence include but are not limited to screenshots, raw tool output (i.e., NMAP, burp suite, Nessus, TCPDump Wireshark, etc.), acquired dumps in case of exploitation (i.e., database files, logs, configuration files etc.), photos, recordings, and anything that may support the final conclusion of the penetration test report.

It should be noted that if cardholder data is acquired during the penetration test, it is recommended that it be kept to a minimum. For example, a database full of cardholder data should not be dumped to the tester's machine or system.

5.3.2 Retention

It is recommended that procedures for retention and destruction of evidence be documented for all parties involved prior to commencing the penetration test. If a third party is used to perform the penetration test, contract language should be reviewed to confirm these procedures are clear.

While there are currently no PCI DSS requirements regarding the retention of evidence collected by the penetration tester, it is a recommended best practice that such evidence be retained by the tester (whether internal to the organization or a third-party provider) for a period of time while considering any local, regional, or company laws that must be followed for the retention of evidence. This evidence should be available upon request from the target entity or other authorized entities as defined in the rules of engagement.

If, however, a tester stores cardholder data obtained during the engagement, the data must be stored by the tester following the guidelines of the PCI DSS for the storage of account data—i.e., encrypted using strong cryptography, truncated/hashed, or not stored. Storage of account data by the tester is not recommended. This data should be securely wiped from tester systems at the conclusion of the engagement.

IPR2025-01085
Orca Security EX1041 Page 25

5.4 Penetration Test Report Evaluation Tool

This section is intended for entities that receive a penetration test report and need to interpret and evaluate the completeness of the report.

The intent is to provide a tool that could be used by merchants, service providers, and assessors to quickly determine the depth of testing and quality of the reporting based upon the contractual agreement between the organization and the tester. It should be noted that this checklist is not intended to take the place of thorough report inspection, interpretation of the findings, and taking appropriate action.

Table 1 details the questions, a place to record whether the item is included in the report and the page number where it is found. It is not the intent to generate any type of "score" from the results, as its intent is to provide a communication tool that may be used between the entity and the tester after a report has been written and the results evaluated. It should be noted that these items represent a suggested minimum set of items to look for in the report; additional content may be present.

Table 1: Report Evaluation Checklist

Report Question	Included In Report		Page
	Yes	No	
Penetration Tester Name/Organization			
Contact information	☐	☐	
Credentials/qualifications of analysts	☐	☐	
Is there sufficient evidence that the individuals are organizationally independent from the management of the environment being tested?	☐	☐	
Dates the engagement was performed	☐	☐	
Date the report was issued	☐	☐	
Executive Summary			
Summarizes testing performed	☐	☐	
Summarizes results of testing	☐	☐	
Summarizes steps for remediation	☐	☐	
Scope			
Is the scope clearly documented?	☐	☐	
How the scope was determined	☐	☐	
Is the attack perspective of the engagement clearly defined (internal, external, or both)?	☐	☐	

Report Question	Included In Report		Page
	Yes	No	
Is the type of testing clearly defined (application layer, network layer, or both)?	☐	☐	
Were there any constraints put on the testing (time, bandwidth limitations, etc.)?	☐	☐	
Methodology			
Is the methodology clearly stated?	☐	☐	
Does the methodology reflect industry best practices (OWASP, NIST, etc.)?	☐	☐	
Narrative			
Is there a clear discussion of the automated and manual testing that was performed?	☐	☐	
Is there clear documentation of any problems that were encountered during the testing (interference from active protection systems, target environment controls blocking or dropping packets, etc.)?	☐	☐	
Discovery			
Is there a section that documents all identified open network ports/services for the target scope and the originating perspective (external or internal exposure)?	☐	☐	
Results			
Is there a clear indication whether retesting is needed, and if so, what specific areas require retesting?	☐	☐	
Is there a summary listing of items that need remediation and retesting?	☐	☐	
Is there a detailed listing of items that need remediation and retesting?	☐	☐	
Did tester demonstrate attempts to exploit the identified vulnerability and clearly state the potential result/risk that each potential exploit may pose to the environment? (See Section 5.1.1 for risk-ranking discussion.)	☐	☐	

6 Case Studies / Scoping Examples

This section provides a number of case studies that illustrate various concepts and methodologies covered in this document.

6.1 E-commerce Penetration Test Case Study

Case Introduction

The Client is a level-one merchant and retailer of women's clothing. Client has three unique brands running on multiple e-commerce web sites. Brand A runs on a third-party e-commerce platform written using a Java platform with Apache Tomcat and IBM's DB2 database and utilizes a content-delivery network for image distribution. Brand B and Brand C utilize an in-house coded e-commerce shopping cart written in ColdFusion with Microsoft SQL and share the same underlying code. All brands submit cardholder data for processing over HTTPS. All sites are hosted at a third-party hosting provider on dedicated systems. The Client's firewalls have integrated intrusion prevention features. Client has exclusive control of the code and the content. Product Managers update product information using staging servers in the corporate environment, and the updates are promoted to production by IT support staff. Client has full control of DNS.

Description of Environment

The environment for Brands A, B, and C is comprised of five networks. The web DMZ contains the firewalls, DNS servers, load balancers, and web servers for all brands. Only the load balancers are NAT'd and have publicly routable IP addresses.

The application tier contains the Apache Tomcat and ColdFusion middleware servers. It is segmented from the DMZ and database tiers using firewall access controls. The database tier contains the Microsoft SQL and IBM DB2 servers. It is segmented from the application tier using firewall access controls. The management network is used for backups, patch-management servers, NTP Servers, network-traffic analysis devices, and syslog collectors. The management network is accessible using jump boxes with two-factor authentication from the corporate network over a point-to-point VPN.

Pre-Engagement Activities (Planning)

Once the engagement is confirmed, the Pen Test Company scheduled a kick-off call and provided the Client with a testing questionnaire and test-authorization form to be completed before the next meeting.

The kick-off call is generally used to review the rules of engagement, define the success criteria, and review the methodology to be used. An examination of this type could be conducted in accordance with information system security assessment best practices such as described by the *Open Source Security Testing Methodology Manual* ("OSSTMM"), *The National Institute of Standards and Technology ("NIST") Special Publication 800-115, Technical Guide to Information Security Testing and Assessment,* or the Open Web Application Security Project (OWASP) testing methodology as defined in the *OWASP Testing Guide v.3.0*.

IPR2025-01085
Orca Security EX1041 Page 28

Scoping is critical, and the more complex the environment, the more difficult it becomes. In this case, all external IPs used for the DMZ and web tier were included in the scope. This would include all systems that directly store, process, or transmit cardholder data. Because the Client has full control and full responsibility for its security, the DNS server was included in the scope of the test to determine whether an attacker could compromise the server and redirect traffic intended for the Client's sites to a malicious intermediary or fraudulent site. The image CDN servers were determined out of scope because no PAN data is transmitted or processed and the systems are otherwise fully segmented. The staging systems are unavailable from the Internet and therefore cannot be tested.

The web applications for Brand A and Brand B will be completely in scope. The web application for Brand C is presumed to be an exact copy, exclusive of product information and look and feel. The tester will sample the web application for Brand C to verify that the applications are the same as Brand B. If it is determined that there are material differences between Brand B and Brand C web applications, Brand C will be brought fully into scope.

The Client and Pen Test Company have agreed that testing will be conducted against the production systems, as no suitable staging or review system is publicly available. Because of this limitation, testing must be performed with the intrusion prevention system enabled. However, because the timeline for testing cannot accommodate the time required to use techniques that might bypass the IPS, the Client has agreed to remove any blocks enabled by the system during testing.

For this engagement the Client has requested that additional rules of engagement include that testing be limited to non-peak hours, and any attempts to run exploit code on the remote systems be performed only after notifying the Client. Also, any accounts created by the tester or successful orders placed in the system must be identified at the end of each day's testing.

All parties have agreed that no further testing is required if the penetration tester is able to extract data from either of the databases or obtain shell access on any server in the web farm.

Engagement Phase (Discovery and Attack/Execution)

The penetration tester began by comparing the scope provided by the Client with the latest ASV report to ensure they agreed on the assets and targets under examination. Any differences in scope were noted and investigated.

The penetration tester then gathered information on the target organization through web sites and mail servers, public records, and databases. This open-source intelligence (OSINT) gathering is an important next step in confirming scope and determining that all the appropriate assets have been included in the test. Newly discovered assets were vetted by the Client to determine whether they should be included in the penetration test. During this phase of the assessment, an additional disaster recovery site was identified in DNS, and Client confirmed this to be a warm backup in the event of failure of the primary sites. All relevant assets were added to the scope.

Once the assets were confirmed, the penetration tester enumerated the publicly available services provided by the targets. The tester actively tried to obtain usernames, network-share information, and application-version information of all running services and applications. In this phase, the penetration tester began to spider and map the applications, with and without credentials, in preparation for the exploitation phase. The tester was provided with the ability to complete a full transaction all the way through checkout and order confirmation.

With target enumeration complete, the tester performed vulnerability mapping of identified services using automated tools and by comparing the port and service fingerprint against well-known vulnerability databases. This produced a list of unconfirmed vulnerabilities that were further examined in the exploitation phase of testing.

The exploitation phase included tests and techniques designed to meet the objectives of the test. (These must be exploitive and may also be used to confirm the effectiveness of ancillary security controls such as intrusion detection systems or web application firewalls.) It was during this step that testing of the applications for issues related to the OWASP Top 10 and other web application frameworks took place.

The final phase of testing included post-exploitation techniques. The term “post-exploitation” refers to the actions taken after the initial compromise of a system or device. It often describes the methodical approach of using privilege escalation techniques to gain additional access to systems or network resources. The extent to which post-exploitation techniques were performed were defined prior to the start of test to prevent the tester from putting production systems at risk of destabilization.

Main vulnerabilities identified were:

High:	▪ Apache Tomcat Manager Application Deployer Authenticated Code Execution ▪ Cross-site scripting (reflective) ▪ Directory traversal
Medium:	▪ Deprecated protocols - SSLv2, SSLv3 ▪ SSL weak ciphers ▪ Internal IP address disclosure
Low:	▪ IPS not enabled for disaster-recovery site ▪ Slow HTTP denial-of-service attack

Post-Engagement (Post-Execution Phase)

At the completion of this examination, the penetration tester met with the Client to describe the preliminary results of the test and address any immediate concerns in advance of the report. The post-execution phase focused on analyzing the identified vulnerabilities to determine root causes, establish recommendations and/or remediation activities, and develop a final report where all vulnerabilities noted during the test were documented even though the vulnerabilities did not have an impact on the cardholder data environment.

The penetration test report was presented to the Client and it was discussed how the Client could remediate the vulnerabilities noted during the penetration test. It was noted that the denial-of-service attack and missing IPS, while serious issues for a retailer, were not PCI-relevant findings and would not be required in order to obtain a clean report.

The Client corrected all High and Medium-severity vulnerabilities within a 90-day window and the Pen Test Company provided documentation of successful remediation to the Client.

6.2 Hosting Provider Penetration Test Case Study

Case Introduction

PCIData Hosting is a hosting service provider. The only cardholder data environment that exists within PCIData Hosting belongs to its PCI DSS compliant customer, TechMerchant. TechMerchant is operating an e-commerce web environment on the PCIData hosting hardware. TechMerchant is solely responsible for the administration and maintenance of all the software and applications used to support its e-commerce

environment. PCIData Hosting is bound by contract with TechMerchant to maintain PCI Compliance. PCIData Hosting is required to maintain PCI Compliance by TechMerchant since PCIData Hosting provides critical security services to TechMerchant for its PCI DSS compliance. In addition, PCIData Hosting has a wish to extend this type of PCI DSS hosting service to more customers in the payment card industry.

PCIData Hosting is managing the systems in the cardholder data environment and is responsible for physical security, hardware, network, firewalls, and OS including updates, configuration etc.

Applications and databases are not the responsibility of PCIData Hosting.

Storing, processing, and transmitting cardholder data are in TechMerchant's scope and have been described and assessed in its own PCI DSS Assessment. PCIData Hosting has no type of cardholder data transactions in scope, and the only entity hosted from a PCI perspective is TechMerchant, for whom they only provide hardware hosting services and logical system management.

Description of Environment

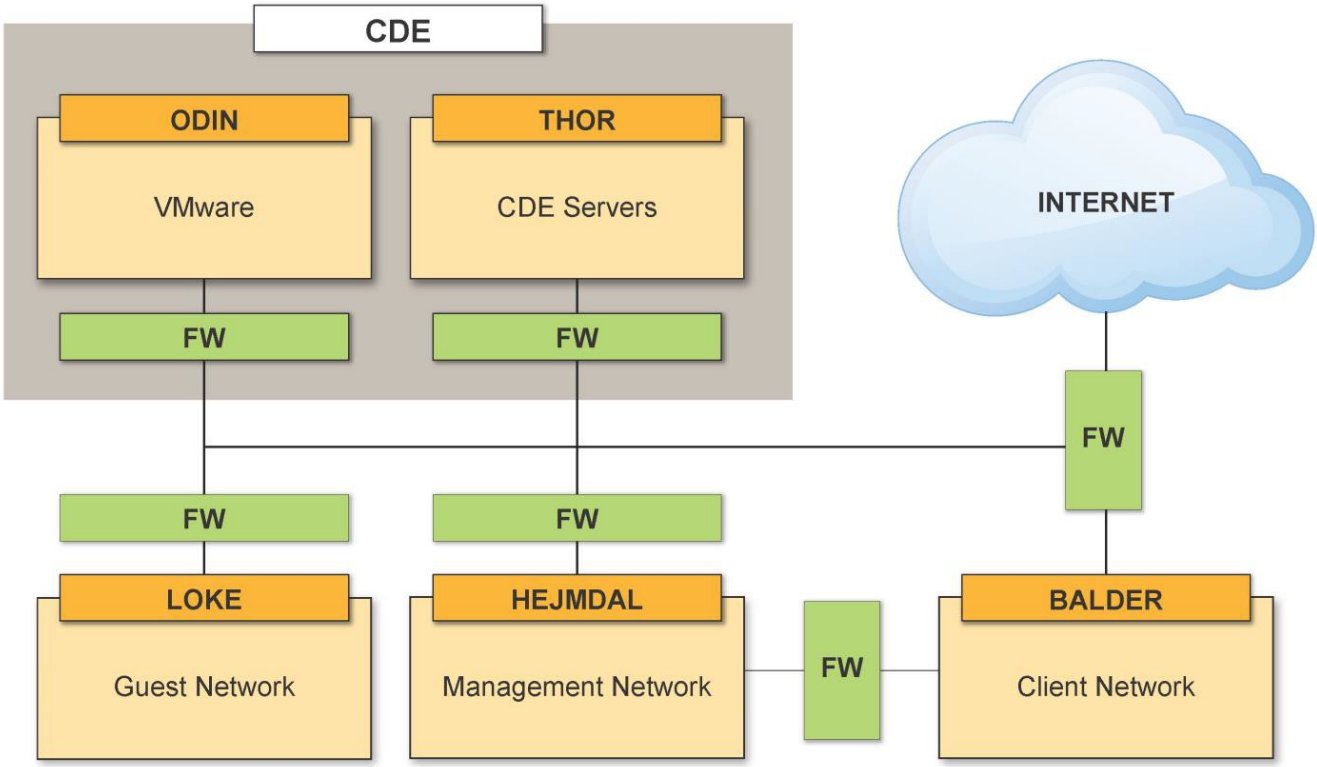
The environment at PCIData Hosting consists of five different networks:

- **ODIN Network Zone:** Only VMware Hypervisors used for the TechMerchant CDE servers and environment are hosted in this network segment. This network is not accessible from the THOR network.
- **THOR Network Zone:** This network is the CDE environment where TechMerchant has its virtual servers located; all servers located at this network are in PCI scope. The network is separated into smaller networks: DMZ, secure database zone, and an application zone. These networks are included in the penetration test performed at TechMerchant.
- **LOKE Network Zone:** Guest network used for external consultants, other guests, BYOD devices, etc. This is the only network that has wireless access points connected.

- **HEJMDAL Network Zone:** Management network from which PCIData Hosting manages the different client networks that do not fall into PCI scope. This network is only used to manage non-CDE servers.
- **BALDER:** All other clients are hosted on this network, including PCIData Hosting's own office network.

All networks are separated by firewalls, and access to ODIN and THOR network segments is restricted to two-factor authentication. The only wireless network is connected to LOKE (the guest network). The datacenter is located at PCIData Hosting's location and is also in scope for PCI compliance.

High-Level Network Diagram



***Success Criteria** – The success criteria for the penetration test is to gain access to the CDE.*

Resource List (CDE environment)

- **ODIN** – VMware servers
- **THOR** – UNIX-based servers including webservers; Oracle databases in a secure zone
- All employees at PCIData Hosting use Microsoft-based workstations to access the CDE environment.

Pre-Engagement Actives (Planning)

The methodology used for the penetration test was based on NIST SP800-115; the penetration test included the following phases: Planning, Discovery, Attack/Execution, Post-Execution and Reporting.

The planning phase was used to gather information needed for the assessment execution—such as the assets to be assessed, the threats of interest against the assets, and the security controls to be used to mitigate those threats—and to develop the assessment approach.

The networks ODIN (VMware) and THOR (CDE Servers) are the targets of the penetration test as these servers are those that store, process, and transmit cardholder data.

Scoping Discussion

It was discussed with PCIData Hosting how they managed their CDE environment, including servers and databases. The operating systems are administrated by PCIData Hosting; all applications and development are handled by TechMerchant. Both PCIData Hosting and TechMerchant administer databases. Encrypted information in the database is only accessible with the encryption keys that are held by TechMerchant. All access to ODIN and THOR are authenticated by a two-factor solution. This also applies when accessed from internal networks at PCIData Hosting.

TechMerchant's last penetration test was reviewed to make sure that all perimeters, servers, etc. were covered by the tests. The application was tested as a part of the TechMerchant's annual PCI penetration test and is not considered in scope for PCIData Hosting's PCI penetration test, therefore the focus is network-layer testing.

The following documentation was reviewed before the assessment:

- A network diagram
- Results from quarterly external and internal vulnerability scans
- Results from the last penetration test
- The scope of the TechMerchant's last penetration test
- Security policies
- Review of PCIData Hosting's risk analysis.

The following tests were performed during the assessment:

- Internal penetration tests from LOKE (guest network), HEJMDAL (management network) and from the office network located in BALDER (Client).
- Social engineering against PCIData Hosting administrators of ODIN (VMware) and THOR (CDE servers) in form of phishing e-mails
- Physical security assessment as a part of the penetration test.
- External testing of PCIData Hosting of their external IP-addresses.

All servers, databases, employees with access to the CDE, etc. are considered in scope for the penetration test.

Pre-Test Preparations

A user account was created for the penetration tester following the regular procedures for granting access to new employees. Access credentials for the guest network were also granted to the tester.

Engagement Phase (Discovery and Attack/Execution)

Discovery was performed on the LOKE (guest), HEJMDAL (management) and BALDER (office) networks to identify targets (servers, network components, workstations, etc.) on the networks, and analyzing techniques were used to get an understanding of the environment. The objectives of this phase were to identify systems, ports, services, and potential vulnerabilities. This phase was performed both manually and via automated tools including network discovery and port and service detection.

When enough data was collected in the discovery phase, the penetration tester tried to gain access to the targets discovered. When access was gained to targets the tester tried to escalate privileges in order to gain complete control of the target. The access obtained was then used to gain more information about the environment, and a new discovery phase was started.

The primary goal for the discovery and attack/execution was gaining access to the CDE, including the VMware hosts. The techniques used included password cracking, vulnerability scanning, social engineering, and network-layer testing.

The above was completed for the following different perspectives during the assessment:

- External attacker without knowledge of the environment
- Internal attacker (guest, contractor, etc.)
- Internal attacker (employee without access to the CDE)

The following tests were performed during the assessment:

- **External attacker without knowledge of the environment**
  - External VPN connection was tested.
  - Phishing e-mails were sent to carefully selected victims who all are working with administrating the CDE environment.
  - Attempts to gain access to the data center without having notified the data center up front.

  Vulnerabilities related to the VPN connection were not found during the external test. Phishing e- mails were sent but the exploits were caught by PCIData Hosting's anti-virus installation. It was not possible to obtain access to the data center without first being authorized by PCIData Hosting.
- **Internal attacker**
  - Attacks from guest network were performed
  - Attacks from the management network were performed
  - Attacks from the office network were performed

Vulnerabilities were found on the different networks, and the tester was able to exploit these but was not able to use the vulnerabilities to gain access to ODIN or THOR.

Main vulnerabilities identified were:

- ***Man in the middle*** – It was possible to perform a man-in-the-middle attack using ARP poisoning but the tester was not able to extract any sensitive information that could provide information on how to gain access to ODIN or THOR.
- ***Weak password policy implemented*** – Weak password settings on local servers on the BALDER network were used to compromise accounts on this network. The tester was not able to use these accounts to gain access to ODIN or THOR. As these servers are not in PCI scope, the weak password policy was not considered to have an impact on compliance.
- ***Old user accounts were compromised*** – The tester was able to compromise user accounts that were created but had never been in use on the BALDER network. The compromised accounts did not grant access to ODIN or THOR.
- ***Others*** – Other vulnerabilities were noted as zone transfer, outdated software, unencrypted protocols used; these vulnerabilities were all related to LOKE or BALDER network and did not grant access to ODIN or THOR even when exploited.

Post-Engagement (Post-Execution phase)

The post-execution phase focused on analyzing the identified vulnerabilities to determine root causes, establish recommendations and/or remediation activities, and develop a final report where all vulnerabilities noted during the test were documented even though they did not have an impact on the cardholder data environment.

The penetration test report was presented to the Client and it was discussed how the Client could remediate the vulnerabilities noted during the penetration test. It was confirmed that none of the vulnerabilities had an effect on the cardholder data environment.

As no significant vulnerabilities related to the CDE environment were discovered and access to the CDE environment was not obtained, remediation testing was not performed.

6.3 Retail Merchant Penetration Test Case Study

Case Introduction

In this example, the business is a retail clothing company called Green Clothing. Cardholder data is collected as a card-present transaction by swiping or keying the card into a POS terminal. The information is then sent to a local server at each store before being sent out to the processor. No cardholder data is transmitted between stores or back to corporate. After receiving a confirmation from the processor, cardholder data is purged from the POS server. The POS server runs a PA-DSS point-of-sale application.

Corporate has a persistent VPN connection into each of the store locations to allow for administration of networked resources, accessing CCTV recordings, and checking inventory.

Description of Environment

The environment at Green Clothing consists of six store locations and one corporate office.

All stores were determined to be identically configured and have been segmented into two networks:

- POS Network – Cardholder Data Environment (CDE)
  - 2 POS devices
  - 1 POS server
- General Store Network (Non-CDE)
  - 1 manager workstation
  - 1 CCTV server

Corporate is made up of two network segments:

- Corporate General User Network (Non-CDE)
  - 4 workstations
  - 1 wireless access point
- Corporate IT Management Network (Non-CDE)
  - 3 workstations used to manage CDE servers

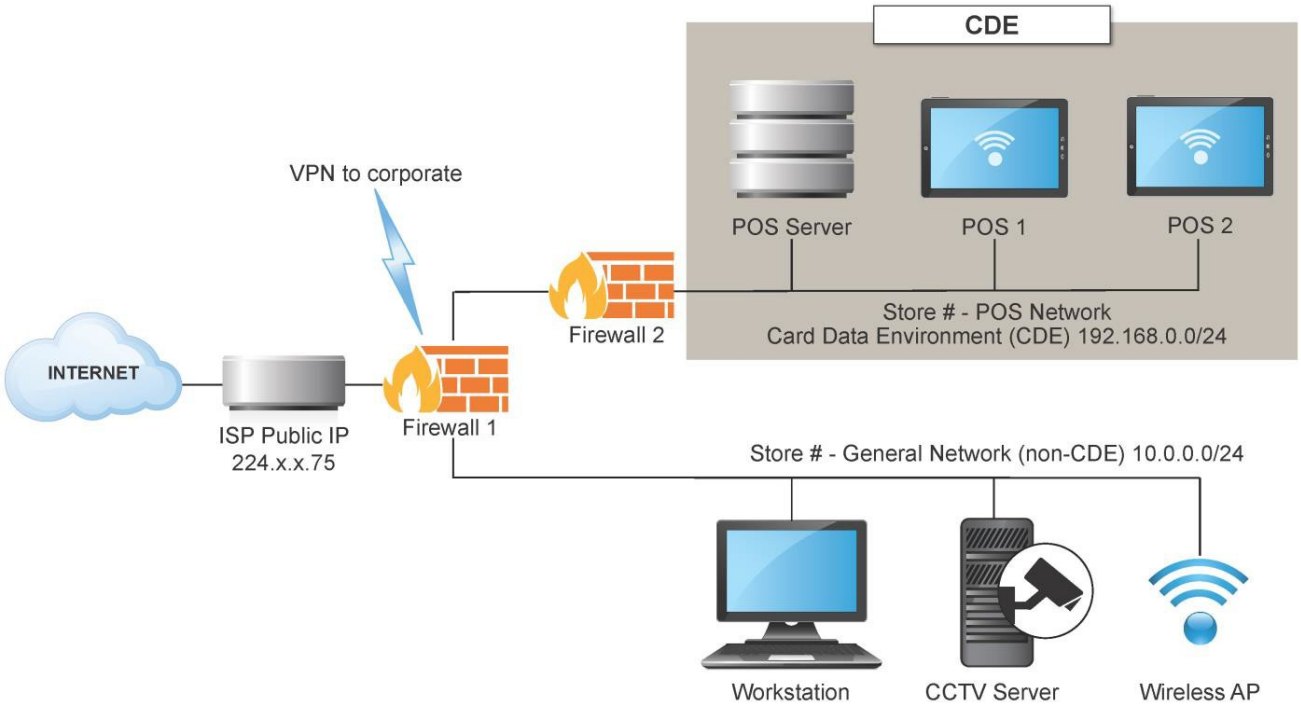
IPR2025-01085
Orca Security EX1041 Page 36

Description of Access

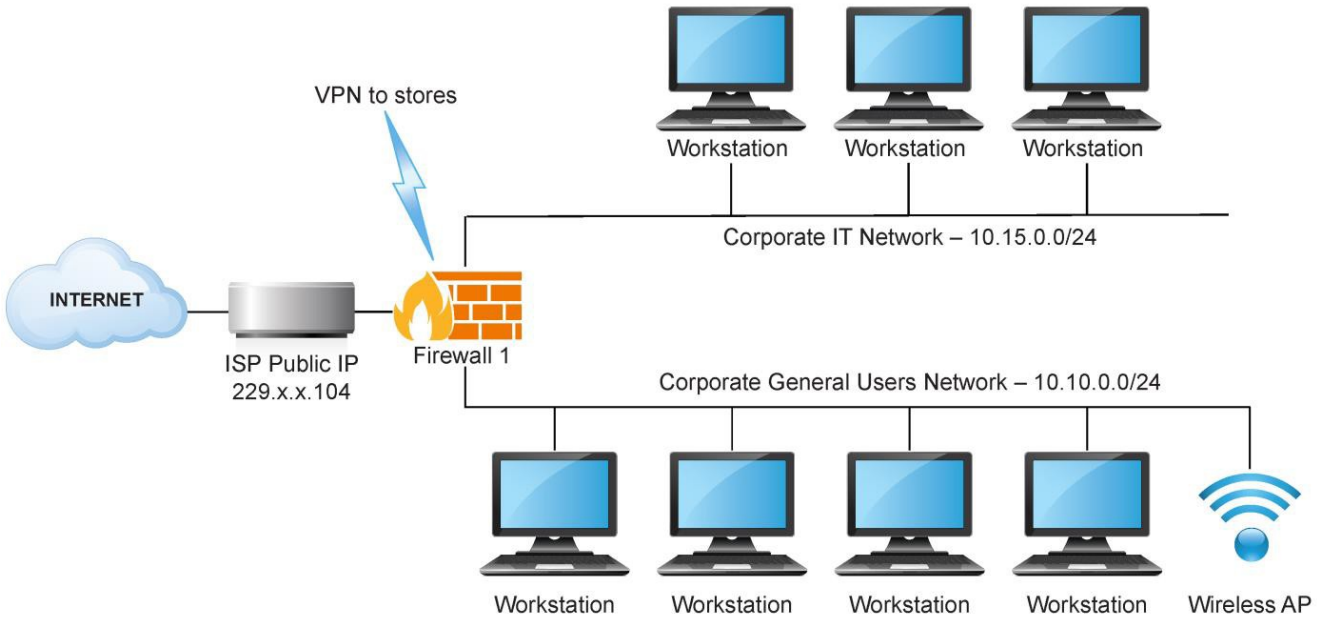
The table below outlines the access from all non-CDE networks into the CDE. This access definition will help in determining what types of testing should be conducted and from where.

Source Network (Non CDE)	Destination Network (CDE)	Access
Corporate General User Network	Store POS Network	None – Segmented
Corporate IT Management Network	Store POS Network	SSH to POS server
Store General Network	Store POS Network	None – Segmented

Example Store Network Diagram



Example Corporate Network Diagram



Pre-Engagement Activities

The POS networks at each store location are considered the cardholder data environment and are the target of the penetration test. The servers within this network at each store are the servers that store, process, and transmit cardholder data.

Scoping Discussion

It was discussed with Green Clothing company how they managed their CDE-environment, specifically how servers and databases are administrated. All administration is conducted from the IT network at corporate over the VPN connection.

The following documentation was reviewed before the assessment:

- A network diagram
- Results from quarterly external and internal vulnerability scans
- Results from the last penetration test
- The scope of the Green Clothing's last penetration test
- Security policies
- Review of Green Clothing's risk analysis

Final Scope Definition

After review of all provided materials, Green Clothing and the penetration tester came to an agreement of the following scope definition.

External Penetration Test

Testing included evaluation of the following Internet-facing resources:

- Six store public IPs

Internal Penetration Testing

Based on information that all stores are configured identically, internal testing was performed against two stores. Any vulnerabilities identified are assumed to exist in all stores. Testing included evaluation of the following unique testing perspectives targeting two store POS networks:

Table x: Network-layer penetration testing scope

Perspective network	Targeted Network
Corporate IT Network	Store # 1 – POS Network
Corporate IT Network	Store # 2 – POS Network

Table y: Segmentation testing scope

Perspective network	Targeted Network
Corporate general user network	Store # 1 – POS Network
Store 1 – general network	Store # 1 – POS Network
Corporate general user network	Store # 2 – POS Network
Store 2 – general network	Store # 2 – POS Network

Pre-Test Preparations

The penetration tester was given a network level access in each of the defined testing perspectives.

- Corporate IT Network
- Corporate General User Network
- Store 1 General Network
- Store 2 General Network

The penetration tester was also provided with the internal IP information for the POS network at the sample target store. No other network access or user credentials were provided.

Engagement Phase

The success criteria for the penetration test were defined as getting access to the CDE environment and accessing cardholder data.

Based on the defined scope, the following different attack scenarios were evaluated:

- External attacker without knowledge of the environment
- Internal attacker with no CDE access (guest, contractor, etc.) in either the store general network, or the corporate general network
- Internal attacker gaining unauthorized access to the corporate IT management network segment and pivoting to attack stores as an administrator

Reporting Phase

The penetration tester reported the following items after completing the test.

External Penetration Test

No notable items reported. It was determined that the only publicly reachable services were the VPN connection points, which were vetted and determined to be secure.

Internal Penetration Test

Outlined below are the vulnerabilities identified during the internal penetration test.

- ***Vulnerability #1 – Segmentation failure***
  Summary: It was found that firewall #2 (CDE firewall) was configured to allow unrestricted access (all ports and services) from the store General Network (10.0.0.0/24) into the store POS Network (192.168.0.0/24).
- ***Vulnerability #2 – Default user credentials on POS server***
  Summary: Default credentials were enabled on the third-party application running on the POS server. Using these credentials, the penetration tester was able to obtain administrative-level access to the POS server.

Post-Engagement

Green Clothing reviewed the penetration test report and implemented fixes for each identified item.

The penetration tester conducted additional testing to validate that the remediation activities sufficiently resolved the reported items. An updated report was provided that showed the items as remediated.

Appendix A: Quick-Reference Table to Guidance on PCI DSS Penetration Testing Requirements

PCI DSS 11.3.x Requirement	Informational Supplement Section(s) Containing Guidance
11.3 Penetration test methodology sub-bullets:	
- Based on industry-accepted approaches	3.1, 4.4, 5.1.1, 5.1.2, 5.2
- Coverage for CDE and critical systems	2.2, 2.2.4, 4.1.1
- Includes external and internal testing	2.2.1, 2.2.2
- Test to validate segmentation controls	2.2.3, 4.2.3
- Application-layer testing	2.3, 4.2.1
- Network-layer tests for network and OS	2.3, 4.2.2

IPR2025-01085
Orca Security EX1041 Page 41

Acknowledgements

PCI SSC would like to acknowledge the contribution of the Penetration Testing Guidance Special Interest Group (SIG) in the preparation of the original document published in 2015. The Penetration Testing Guidance SIG consisted of representatives from the following organizations:

Accuvant, Inc
Agio, LLC
Alaska Airlines
A-lign Security and Compliance Services
Allstate Insurance
Aperia Solutions
AT&T Consulting Solutions
atsec (Beijing) Information Technology Co., Ltd
Bally Total Fitness
Bank Of New Zealand
Bashas' Inc.
BB&T Corporation
Board of Trustees of the University of Arkansas
Bridge Point Communications
The Brick Group
BrightLine CPAs & Associates, Inc.
British Airways PLC
BT PLC
Canadian Tire Financial Services
CBIZ Security & Advisory Services, LLC
CDG Commerce
CenturyLink
Cisco Systems, Inc.
Citigroup Inc.
Clydesdale Bank PLC
Coalfire Systems, Inc.
Compass IT Compliance, LLC
Computer Services, Inc.
Comsec
ControlScan Inc.
Convergys Corp
CradlePoint
Crosskey Banking Solutions
Crowe Horwath LLP
DataFlight Europe AS
Delhaize America Shared Services Group, LLC
Dell, Inc.
Deluxe Corp.
Diamond Resorts Corp.
Digital Defense, Inc.
Domino's Pizza, Inc.
DST Output
Enterprise Holdings, Inc.
EVO Payments International
EVRY A/S
Experian Information Services
Exxon Mobil Corporation
Fiscal Systems, Inc.
Fiserv Solutions, Inc.
FishNet Security
Foregenix
Foresight IT Consulting Pty Ltd.
FortConsult A-S
Games Workshop Ltd
Gap Inc.
Global Payments Direct, Inc.
Grant Thornton
Groupement Interbancaire Monetique de L'uemoa (GIM-UEMOA)
GuidePoint Security, LLC

IPR2025-01085
Orca Security EX1041 Page 42

Hewlett-Packard
Hitachi-Omron Terminal Solutions, Corp.
IBM Corporation
Internet Security Auditors
IQ Information Quality
Isis Mobile Commerce
Jet Infosystems
Liverpool Victoria Friendly Society
Lloyds Banking Group
MegaPath Inc.
MobileIron, Inc.
Módulo Security Solutions S.A.
MTI Technology, Ltd.
National Australia Bank
Nettitude, Ltd.
NIC Inc
Novacoast
NRI Secure Technologies
NTA Monitor Ltd.
NTT Security Ltd.
Online Enterprises
Outerwall
Payment Software Company (PSC)
PayPal, Inc.
Pier1 Imports
Princeton Payment Solutions LLC
Progressive Casualty Insurance Company
Promocion y Operacion SA de CV
Rapid7 LLC
RBC Royal Bank
RBS
Right Time Limited
Secured Net Solutions Inc.
SecureNet
SecurityMetrics, Inc.
Sense of Security Pty Ltd.
Sikich LLP
SISA
SIX Payment Services Ltd
Solutionary, Inc.
Starwood Hotels & Resorts Worldwide, Inc.
State Farm Mutual Automobile Insurance Company
StoreFinancial Services
Structured Communication Systems, Inc.
Sword & Shield Enterprise Security, Inc.
Symantec Corporation
Sysnet Limited
Telstra
Tesco Stores Ltd.
Tieto Latvia SIA
TIVIT (Terceirizacao de Tecnologiae Servicios S/A)
Trustwave Holdings, Inc.
TSYS
TUI Travel PLC
U.S. Bancorp
U.S. Cellular
UL Transaction Security PTY Ltd.
University of Oklahoma
UPS (United Parcel Service)
usd AG
Verizon Wireless
VigiTrust Ltd.
Vodat International Ltd.
The Walt Disney Company
Westpac Banking Corporation
Xpient Solutions LLC

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 Financial Services, JCB International, Mastercard, and Visa Inc., the Council has more than 700 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.

IPR2025-01085
Orca Security EX1041 Page 44