YourIT!
Your Logo Goes Here

PCI Assessment

PCI Risk Analysis

Prepared for:
Prospect or Customer
Prepared by:
Your Company Name

Table of Contents

1 - Overview

2 - Risk Score

3 - Issue Summary

Overview

Risk management, a component of the PCI assessment process, includes the implementation of security measures to reduce risk to reasonable and appropriate levels to, among other things, ensure the confidentiality, availability and integrity of PAN and PIN data and protect against any reasonably anticipated threats, hazards, or disclosures not permitted or required.

After a Risk Analysis the next step in the risk management process is to develop and implement a Risk Management Plan. The purpose of a Risk Management Plan is to provide structure for the evaluation, prioritization, and implementation of risk-reducing measures and controls.

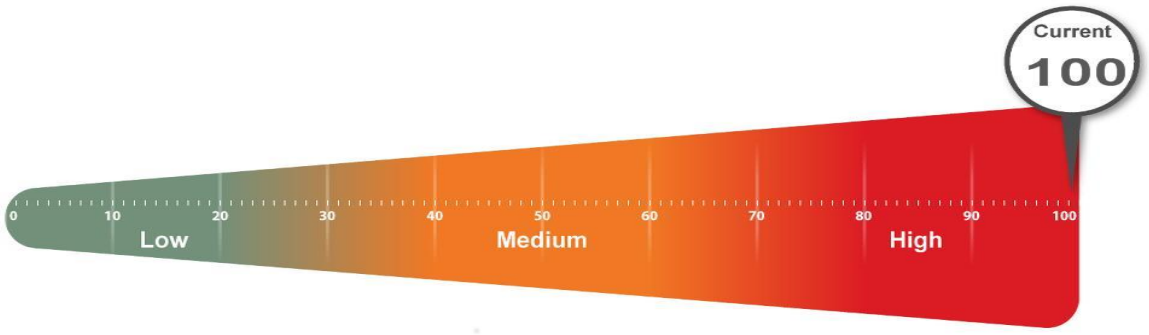
Risk prioritization and mitigation decisions will be determined by answering which controls and measures should be implemented and the priority in which they should be addressed based upon their "risk score." The implementation components of the plan include:

- Risk score (threat and vulnerability combinations) assigned to a particular issue being addressed;
- Recommendation(s) of measures and controls selected to reduce the risk of an issue;
- Ongoing evaluation and monitoring of the risk mitigation measures.

Risk analysis and risk management are not one-time activities. Risk analysis and risk management are dynamic processes that must be periodically reviewed and updated in response to changes in the environment. The risk analysis will identify new risks or update existing risk levels resulting from environmental or operational changes. The output of the updated risk analysis will be an input to the risk management process to reduce newly identified or updated risk levels to reasonable and appropriate levels.

Risk Score

The Risk Score is a value from 0 to 100, where 100 represents significant risk and potential issues.

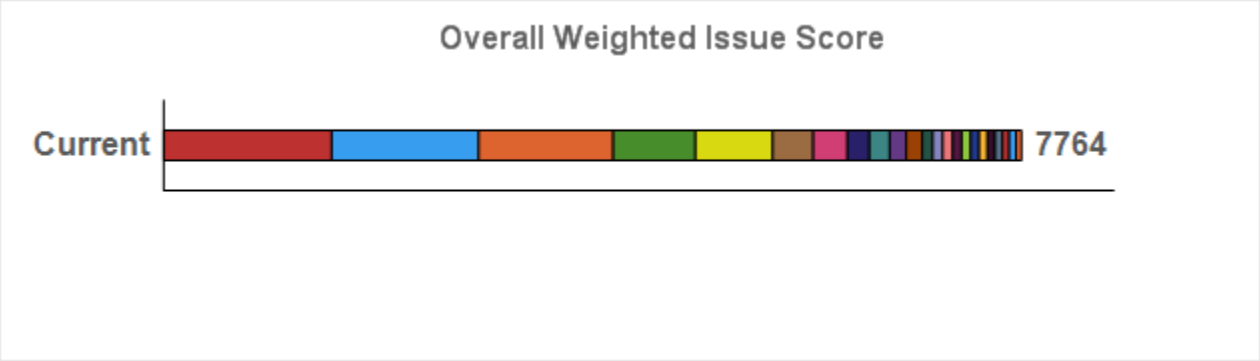


Several critical issues were identified. Identified issues should be investigated and addressed according to the Management Plan.

If additional information is needed, please consult the Evidence of PCI Compliance.

Issues Summary

This section contains a summary of issues detected during the PCI Assessment process, and is based on industry-wide best practices for network health, performance, and security. The Overall Issue Score grades the level of issues in the environment. An Overall Issue score of zero (0) means no issues were detected in the environment. It may not always be possible to achieve a zero score in all environments due to specific circumstances.



Weighted Score: Risk Score x Number of Incidents = Total points: Total percent (%)

	Antivirus not enabled (95 pts each)
1520	***Current Score:*** 95 pts x 16 = 1520 : 19.58%
	Requirement: PCI DSS Requirement 5.1 - Deploy anti-virus software on all systems commonly affected by malicious software (particularly personal computers and servers).
	Issue: Antivirus is not enabled as required to fulfill PCI requirement 5.1.
	Recommendation: Enable antivirus on all computers commonly affected by malicious software.

	Antispyware not enabled (95 pts each)
1330	***Current Score:*** 95 pts x 14 = 1330 : 17.13%
	Requirement: PCI DSS Requirement 5.1 - Deploy anti-virus software on all systems commonly affected by malicious software (particularly personal computers and servers).
	Issue: Antispyware is not enabled as required to fulfill PCI requirement 5.1.
	Recommendation: Enable antispyware on all computers commonly affected by malicious software.

	Unrestricted web access from CDE (87 pts each)
1218	***Current Score:*** 87 pts x 14 = 1218 : 15.69%
	Requirement: PCI DSS Requirement 1.3.5 - Do not allow unauthorized outbound traffic from the cardholder data environment to the Internet.
	Issue: Web access should be restricted to what is necessary. Access to various sites were found to be unrestricted in the Cardholder Data Environment.
	Recommendation: Block web traffic to all sites not required by the CDE.

	Potential Former Employee and Former Vendors with Enabled Accounts (62 pts each)
744	***Current Score:*** 62 pts x 12 = 744 : 9.58%
	Requirement: PCI DSS Requirement 8.1.3 - Immediately revoke access for any terminated users.

	Issue: The following user accounts were found to not have user activity in the past 30 days and could be an indication of an account that should be disabled.
	Recommendation: Investigate and determine if the users are former employees or vendors.

	Potential Generic Accounts found (70 pts each)
700	***Current Score:*** 70 pts x 10 = 700 : 9.02%
	Requirement: PCI DSS Requirement 8.1.1 - Assign all users a unique ID before allowing them to access system components or cardholder data.
	Issue: Generic account logins were used on the following computers and should be investigated. The use of generic logins may prevent proper tracking and identification and is discouraged. There are legitimate uses for generic login, such as limited administrative access and use, as well as access to workstations where secondary logins are required to access the Cardholder Data Environment. If access is deemed inappropriate, further action should be taken to ensure the situation is remediated.
	Recommendation: Investigate and either disable or note compensating controls to ensure these potential generic accounts are not used inappropriately. Service accounts are excluded.

	Non-console access allowed through insecure remote-login commands (92 pts each)
368	***Current Score:*** 92 pts x 4 = 368 : 4.74%
	Requirement: PCI DSS Requirement 2.3.b - Review services and parameter files on systems to determine that Telnet and other insecure remote-login commands are not available for non-console access.
	Issue: Insecure remote-login commands, such as Telnet, are available for non-console access to computers in the CDE.
	Recommendation: Block or disable access to Telnet and other insecure remote-login commands for non-console access.

	Missing additional security features for inherently insecure protocols (77 pts each)
308	***Current Score:*** 77 pts x 4 = 308 : 3.97%
	Requirement: PCI DSS Requirement 2.2.3 - Implement additional security features for any required services, protocols, or daemons that are considered to be insecure—for example, use secured technologies such as SSH, S-FTP, SSL, or IPSec VPN to protect insecure services such as NetBIOS, file-sharing, Telnet, FTP, etc.
	Issue: Additional security features should be implemented for protocols that are typically considered insecure.
	Recommendation: Implement additional security features for any required services, protocols, or daemons that are considered to be insecure.

	Primary Account Numbers found (100 pts each)
200	***Current Score:*** 100 pts x 2 = 200 : 2.58%
	Requirement: PCI DSS Requirement 3.2 - Do not store sensitive authentication data after authorization (even if encrypted). If sensitive authentication data is received, render all data unrecoverable upon completion of the authorization process.
	Issue: Although the environment is believed to not store Cardholder Data on the file system, Primary Account Numbers (PAN) were found during a file system scan.
	Recommendation: Identify and remove the source resulting in storage of Primary Account Numbers (PAN) in the file system.

	Antivirus definitions not current (92 pts each)
184	***Current Score:*** 92 pts x 2 = 184 : 2.37%

Requirement: PCI DSS Requirement 5.1 - Deploy anti-virus software on all systems commonly affected by malicious software (particularly personal computers and servers).
Issue: Antivirus definitions are not up to date and may not protect against the latest threats.
Recommendation: Update antivirus definitions to ensure protection against the latest threats.

	FEW Security patches missing on computers. (75 pts each)
150	***Current Score:*** 75 pts x 2 = 150 : 1.93% ***Requirement:*** PCI DSS Requirement 6.2 - Ensure that all system components and software are protected from known vulnerabilities by installing applicable vendor-supplied security patches. Install critical security patches within one month of release. ***Issue:*** Security patches are missing on computers. Maintaining proper security patch levels helps prevent unauthorized access and the spread of malicious software. Few is defined as missing 3 or less patches. ***Recommendation:*** Address patching on computers with missing security patches.

	Former Employee with Enabled Accounts (72 pts each)
144	***Current Score:*** 72 pts x 2 = 144 : 1.85% ***Requirement:*** PCI DSS Requirement 8.1.3 - Immediately revoke access for any terminated users. ***Issue:*** Terminated employees should have their accounts disabled to prevent potential unauthorized access to Cardholder Data. The following active accounts designated as former employees were identified. These accounts should be disabled or removed. ***Recommendation:*** Disable or remove accounts for former employees and vendors.

	Security features not documented (94 pts each)
94	***Current Score:*** 94 pts x 1 = 94 : 1.21% ***Requirement:*** PCI DSS Requirement 1.1.6 - Documentation and business justification for use of all services, protocols, and ports allowed, including documentation of security features implemented for those protocols considered to be insecure. ***Issue:*** Security features for external ports using inherently insecure protocols not documented. ***Recommendation:*** Close or unpublish external facing ports using inherently insecure protocols or provide additional security features and documentation.

	Antispyware definitions not current (92 pts each)
92	***Current Score:*** 92 pts x 1 = 92 : 1.18% ***Requirement:*** PCI DSS Requirement 5.1 - Deploy anti-virus software on all systems commonly affected by malicious software (particularly personal computers and servers). ***Issue:*** Antispyware definitions are not up to date and may not protect against the latest threats. ***Recommendation:*** Update antispyware definitions to ensure protection against the latest threats.

	Administrative account auditing adequately enabled (89 pts each)
89	***Current Score:*** 89 pts x 1 = 89 : 1.15% ***Requirement:*** PCI DSS Requirement 10.2.2 - All actions taken by any individual with root or administrative privileges. ***Issue:*** Accounts with increased privileges, such as the “administrator” or “root” account, have the potential to greatly impact the security or operational functionality of a system. Without a log of the activities performed, an organization is unable to trace any issues resulting from an administrative mistake or misuse of privilege back to the specific action and individual.

Recommendation: Enable auditing of all actions taken by any individual with root or administrative privileges.

	Password complexity not enforced (83 pts each)
83	***Current Score:*** 83 pts x 1 = 83 : 1.07%
	Requirement: PCI DSS Requirement 8.2.3 - Passwords/phrases must meet the following: * Require a minimum length of at least seven characters. * Contain both numeric and alphabetic characters. Alternatively, the passwords/phrases must have complexity and strength at least equivalent to the parameters specified above.
	Issue: Passwords/phrases must require a minimum length of at least seven characters and contain both numeric and alphabetic characters.
	Recommendation: Enforce password complexity of at least 7 characters and contain both numeric and alphabetic characters.

	Password repeat policy not enforced. (81 pts each)
81	***Current Score:*** 81 pts x 1 = 81 : 1.04%
	Requirement: PCI DSS Requirement 8.2.5 - Do not allow an individual to submit a new password/phrase that is the same as any of the last four passwords/phrases he or she has used.
	Issue: Passwords/phrases must not be the same as the last four passwords/phrases.
	Recommendation: Do not allow an individual to submit a new password/phrase that is the same as any of the last four passwords/phrases he or she has used.

	Password attempt lockout not enforced (77 pts each)
77	***Current Score:*** 77 pts x 1 = 77 : 0.99%
	Requirement: PCI DSS Requirement 8.1.6 - Limit repeated access attempts by locking out the user ID after not more than six attempts.
	Issue: Limit repeated access attempts by locking out the user ID after not more than six attempts.
	Recommendation: Ensure password lockout is enforced after more than six attempts.

	Inadequate password lockout duration (74 pts each)
74	***Current Score:*** 74 pts x 1 = 74 : 0.95%
	Requirement: PCI DSS Requirement 8.1.7 - Set the lockout duration to a minimum of 30 minutes or until an administrator enables the user ID.
	Issue: Account lockout duration not set to a minimum of 30 minutes or until an administrator enables the user ID.
	Recommendation: Set the lockout duration to a minimum of 30 minutes or until an administrator enables the user ID.

	Auditing for account changes required (69 pts each)
69	***Current Score:*** 69 pts x 1 = 69 : 0.89%
	Requirement: PCI DSS Requirement 10.2.5 - Use of and changes to identification and authentication mechanisms—including but not limited to creation of new accounts and elevation of privileges—and all changes, additions, or deletions to accounts with root or administrative privileges.
	Issue: Auditing use of and changes to identification and authentication mechanisms—including but not limited to creation of new accounts and elevation of privileges—and all changes, additions, or deletions to accounts with root or administrative privileges is required.

Recommendation: Enable auditing of changes to account identification and authentication mechanisms.

	Vendor access should be disabled when not in use (67 pts each)
67	***Current Score:*** 67 pts x 1 = 67 : 0.86%
	Requirement: PCI DSS Requirement 8.1.5 - Manage IDs used by vendors to access, support, or maintain system components via remote access
	Issue: Vendor user accounts with access rights to the Cardholder Data Environment and/or system components must be disabled when not in use.
	Recommendation: Disable vendor accounts when not in use.

	Potential Former Vendors with Enabled Accounts (62 pts each)
62	***Current Score:*** 62 pts x 1 = 62 : 0.8%
	Requirement: PCI DSS Requirement 8.1.5 - Manage IDs used by vendors to access, support, or maintain system components via remote access
	Issue: The following user accounts were found to not have user activity in the past 30 days and could be an indication of an account that should be disabled.
	Recommendation: Disable or remove accounts for former employees and vendors.

	Network diagram not consistent with firewall configuration standard (60 pts each)
60	***Current Score:*** 60 pts x 1 = 60 : 0.77%
	Requirement: PCI DSS Requirement 1.1.4.b - Verify that the current network diagram is consistent with the firewall configuration standards.
	Issue: The current network diagram is not consistent with the firewall configuration standards.
	Recommendation: Updated the network diagram to be consistent with the requirement to deploy a firewall at each Internet connection or note in the CCW any exceptions.

	Developer training required (50 pts each)
50	***Current Score:*** 50 pts x 1 = 50 : 0.64%
	Requirement: PCI DSS Requirement 6.5 - Address common coding vulnerabilities in software-development processes
	Issue: Developers have not received training in developing applications based on secure coding guidelines to protect applications
	Recommendation: Establish a program to train developers on secure coding guidelines to protect applications.