



Azure Security Center

PCI DSS 3.2.1 Compliance Report

5/6/2021 9:51:58 PM UTC

Table of contents

- i. Executive summary
- ii. PCI DSS 3.2.1 sections summary
- iii. PCI DSS 3.2.1 controls status


Executive summary

Introduction

Azure Security Center executes a set of automated assessments on your Azure environment which can help provide evidence relevant to specific controls in a compliance framework or standard. This report summarizes the current status of those assessments on your environment, as they map to the associated controls. This report does not represent a complete compliance report for the standard, nor does it ensure compliance.

Compliance with PCI DSS 3.2.1 controls









Your environment is compliant with 43 of 43 supported PCI DSS 3.2.1 controls.







PCI DSS 3.2.1 sections summary

The following is a summary status for each of the sections of the PCI DSS 3.2.1. For each section, you will find the overall number of passing and failing controls, based on automated assessments run by Security Center.

A failing control indicates that at least one Security Center assessment associated with this control failed. A passing control indicates that all the Security Center assessments associated with this control passed. Note that status is shown only for supported controls, i.e. controls that have relevant Security Center assessments associated with them.

Area	Failed controls	Passed controls	
1. Install and maintain a firewall configuration to protect cardholder data	0	3	
2. Do not use vendor-supplied defaults for system passwords and other security parameters	0	4	
3. Protect stored cardholder data	0	2	
4. Encrypt transmission of cardholder data across open, public networks.	0	1	
5. Protect all systems against malware and regularly update anti-virus software or programs.	0	1	
6. Develop and maintain secure systems and applications	0	3	
7. Restrict access to cardholder data by business need to know	0	6	
8. Identify and authenticate access to system components	0	5	

10. Track and monitor all access to network resources and cardholder data	0	15	
11. Regularly test security systems and processes	0	1	
A2. Additional PCI DSS Requirements for Entities using SSL/Early TLS for Card-Present POS POI Terminal Connections	0	1	
A3. Designated Entities Supplemental Validation (DESV).	0	1	




PCI DSS 3.2.1 controls status

The following is a summary status for each supported control of the PCI DSS 3.2.1. For each control, you will find the overall number of passing, failing and skipped assessment associated with that control.





A failing assessment indicates a Security Center assessment that failed on at least one resource in your environment. A passing Security Center assessment indicates an assessment that passed on all resources. A skipped assessment indicates an assessment that was not run, whether because this assessment type is disabled or because there are no relevant resources in your environment.

Note that status is shown only for supported controls, i.e. controls that have relevant Security Center assessments associated with them.


1. Install and maintain a firewall configuration to protect cardholder data

Control	Failed assessments	Passed assessments	Skipped assessments	
1.2.1. Restrict inbound and outbound traffic to that which is necessary for the cardholder data environment, and specifically deny all other traffic.	0	124	0	
1.3.2. Limit inbound Internet traffic to IP addresses within the DMZ.	0	1	0	
1.3.4. Do not allow unauthorized outbound traffic from the cardholder data environment to the Internet.	0	1	0	

2. Do not use vendor-supplied defaults for system passwords and other security parameters

Control	Failed assessments	Passed assessments	Skipped assessments	
2.2.2. Enable only necessary services, protocols, daemons, etc., as required for the function of the system.	0	13	0	
2.2.3. Implement additional security features for any required services, protocols, or daemons that are considered to be insecure.	0	23	0	
2.2.4. Configure system security parameters to prevent misuse.	0	9	0	
2.3. Encrypt all non-console administrative access using strong cryptography.	0	21	0	

3. Protect stored cardholder data


Control	Failed assessments	Passed assessments	Skipped assessments	
3.2.*. Additional assessments for 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. It is permissible for issuers and companies that support issuing services to store sensitive authentication data if: <ul style="list-style-type: none"> - There is a business justification and - The data is stored securely. 	0	1	0	

3.4.*. Additional assessments for 3.4 - Render PAN unreadable anywhere it is stored (including on portable digital media, backup media, and in logs) by using any of the following approaches: <ul style="list-style-type: none"> - One-way hashes based on strong cryptography, (hash must be of the entire PAN) - Truncation (hashing cannot be used to replace the truncated segment of PAN) - Index tokens and pads (pads must be securely stored) - Strong cryptography with associated key-management processes and procedures. 	0	4	0	
--	---	---	---	--




4. Encrypt transmission of cardholder data across open, public networks.

Control	Failed assessments	Passed assessments	Skipped assessments	
4.1.*. Additional assessments for 4.1 - Use strong cryptography and security protocols to safeguard sensitive cardholder data during transmission over open, public networks, including the following: <ul style="list-style-type: none"> - Only trusted keys and certificates are accepted. - The protocol in use only supports secure versions or configurations. - The encryption strength is appropriate for the encryption methodology in use. 	0	26	0	







5. Protect all systems against malware and regularly update anti-virus software or programs.

Control	Failed assessments	Passed assessments	Skipped assessments	
5.1.*. Additional assessments for 5.1 - Deploy anti-virus software on all systems commonly affected by malicious software (particularly personal computers and servers).	0	1	0	


6. Develop and maintain secure systems and applications





Control	Failed assessments	Passed assessments	Skipped assessments	
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.	0	2	0	
6.5.3. Insecure cryptographic storage	0	4	0	
6.6. For public-facing web applications, address new threats and vulnerabilities on an ongoing basis and ensure these applications are protected against known attacks by either of the following methods: - Reviewing public-facing web applications via manual or automated application vulnerability security assessment tools or methods, at least annually and after any changes - Installing an automated technical solution that detects and prevents web-based attacks (for example, a web-application firewall) in front of public-facing web applications, to continually check all traffic.	0	1	0	

7. Restrict access to cardholder data by business need to know



Control	Failed assessments	Passed assessments	Skipped assessments	
7.1.1. Define access needs for each role, including: - System components and data resources that each role needs to access for their job function - Level of privilege required (for example, user, administrator, etc.) for accessing resources.	0	2	0	
7.1.2. Restrict access to privileged user IDs to least privileges necessary to perform job responsibilities.	0	42	0	
7.1.3. Assign access based on individual personnel's job classification and function.	0	42	0	
7.2.1. Coverage of all system components	0	1	0	
7.2.2. Assignment of privileges to individuals based on job classification and function.	0	40	0	
7.2.3. Default 'deny-all' setting.	0	3	0	













8. Identify and authenticate access to system components

Control	Failed assessments	Passed assessments	Skipped assessments	
8.1.2. Control addition, deletion, and modification of user IDs, credentials, and other identifier objects.	0	3	0	

8.1.3. Immediately revoke access for any terminated users.	0	1	0	
8.1.5. Manage IDs used by third parties to access, support, or maintain system components via remote access as follows: - Enabled only during the time period needed and disabled when not in use. - Monitored when in use.	0	3	0	
8.2.3. Passwords/passphrases must meet the following: - Require a minimum length of at least seven characters. - Contain both numeric and alphabetic characters. Alternatively, the passwords/passphrases must have complexity and strength at least equivalent to the parameters specified above.	0	2	0	
8.3.1. Incorporate multi-factor authentication for all non-console access into the CDE for personnel with administrative access, Enable MFA for accounts with admin privileges on your subscription	0	4	0	


10. Track and monitor all access to network resources and cardholder data

Control	Failed assessments	Passed assessments	Skipped assessments	
10.1. Implement audit trails to link all access to system components to each individual user.	0	66	0	
10.2.2. All actions taken by any individual with root or administrative privileges	0	66	0	


10.2.3. Access to all audit trails	0	66	0	
10.2.4. Invalid logical access attempts	0	66	0	
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	0	66	0	
10.2.6. Initialization, stopping, or pausing of the audit logs	0	66	0	
10.2.7. Creation and deletion of system-level objects	0	66	0	
10.3.1. User identification	0	66	0	
10.3.2. Type of event	0	66	0	
10.3.3. Date and time	0	66	0	
10.3.4. Success or failure indication	0	66	0	
10.3.5. Origination of event	0	66	0	
10.3.6. Identity or name of affected data, system component, or resource.	0	66	0	
10.3.*. Additional assessments for 10.3 - Record at least the following audit trail entries for all system components for each event	0	11	0	

10.5.4. Write logs for external-facing technologies onto a secure, centralized, internal log server or media device.	0	11	0	
--	---	----	---	---

11. Regularly test security systems and processes

Control	Failed assessments	Passed assessments	Skipped assessments	
11.2.1. Perform quarterly internal vulnerability scans. Address vulnerabilities and perform rescans to verify all 'high risk' vulnerabilities are resolved in accordance with the entity's vulnerability ranking (per Requirement 6.1). Scans must be performed by qualified personnel.	0	2	0	

A2. Additional PCI DSS Requirements for Entities using SSL/Early TLS for Card-Present POS POI Terminal Connections

Control	Failed assessments	Passed assessments	Skipped assessments	
A2.1. Where POS POI terminals (at the merchant or payment acceptance location) use SSL and/or early TLS, the entity must confirm the devices are not susceptible to any known exploits for those protocols.	0	21	0	

A3. Designated Entities Supplemental Validation (DESV).

Control	Failed assessments	Passed assessments	Skipped assessments	
---------	--------------------	--------------------	---------------------	--

A3.4.1. Review user accounts and access privileges to in-scope system components at least every six months to ensure user accounts and access remain appropriate based on job function, and authorized.

0

40

0

