PAYMENT CARD INDUSTRY DATA SECURITY STANDARD (PCI DSS) V4.0

Targeted Risk Analysis

TARGETED RISK ANALYSIS (TRA)

Requirement 12.2 in version 3.2.1 of the PCI Data Security Standards (PCI DSS) requires organizations to perform a risk assessment at least annually that identifies critical assets, threats, and vulnerabilities, and results in a formal, documented analysis of risk.

V4.0 of the PCI DSS removed requirement 12.2 and replaced this requirement with a new requirement: 12.3.1. The new requirement is to perform a TRA for any PCI DSS requirement that provides flexibility for how frequently it is performed. Resulting in a TRA to be performed for the following requirements: 5.2.3.1, 5.3.2.1, 7.2.5.1, 8.6.3, 9.5.1.2.1, 10.4.2.1, 11.3.1.1, 11.6.1, 12.3.1, 12.3.2, and 12.10.4.1.

DEFINITIONS

Targeted Risk Analysis: For PCI DSS purposes, a risk analysis that focuses on a specific PCI DSS requirement(s) of interest, either because the requirement allows flexibility (for example, as to frequency) or, for the Customized Approach, to explain how the entity assessed the risk and determined the customized control meets the objective of a PCI DSS requirement.

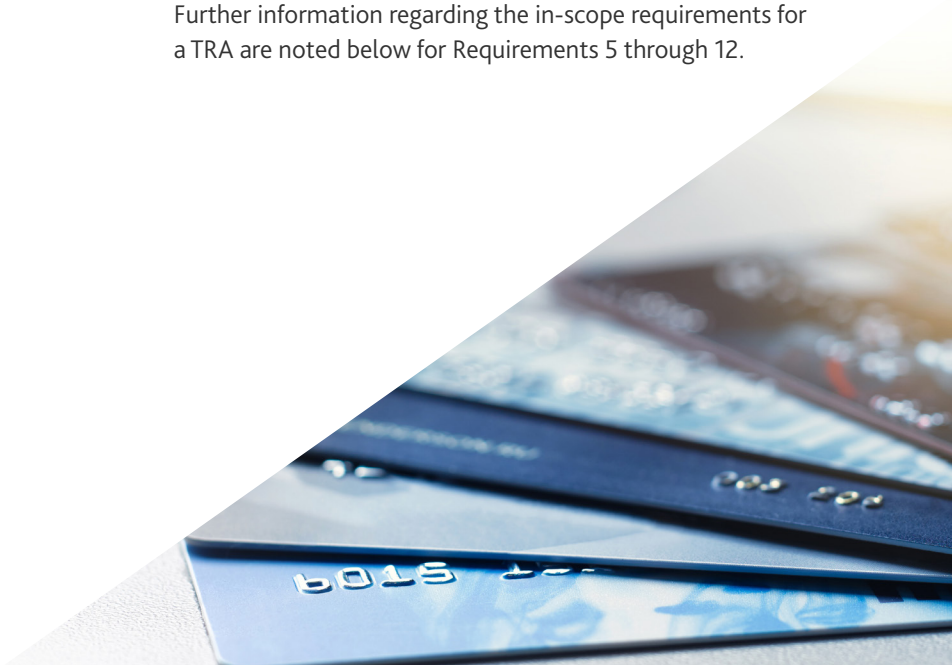
REQUIREMENT 12.3.1 – TARGETED RISK ANALYSIS

Each PCI DSS requirement that provides flexibility for how frequently it is performed (for example, requirements to be performed periodically) is supported by a TRA that is documented and includes:

- Identification of the assets being protected.
- Identification of the threat(s) that the requirement is protecting against.
- Identification of factors that contribute to the likelihood and/or impact of a threat being realized.
- Resulting analysis that determines, and includes justification for, how frequently the requirement must be performed to minimize the likelihood of the threat being realized.
- Review of each TRA at least once every 12 months to determine whether the results are still valid or if an updated risk analysis is needed.
- Performance of updated risk analyses when needed, as determined by the annual review.

Note: This requirement is a best practice until March 31 2025, after which it will be required and must be fully considered during a PCI DSS assessment.

Further information regarding the in-scope requirements for a TRA are noted below for Requirements 5 through 12.



REQUIREMENT 5

Protect All Systems and Networks from Malicious Software. Processes and mechanisms for protecting all systems and networks from malicious software are defined and understood.

NEW REQUIREMENT		APPLICABLE TO		EFFECTIVE DATE	
		All Entities	Service Providers Only	Immediately for all V4.0 Assessments	March 31, 2025
5.2.3.1	New requirement to define the frequency of periodic evaluations of system components not at risk for malware in the entity's targeted risk analysis.	X			X
5.3.2.1	New requirement to define the frequency of periodic malware scans in the entity's targeted risk analysis.	X			X

REQUIREMENT 7

Restrict Access to System Components and Cardholder Data by Business Need to Know. 7.1 Processes and mechanisms for restricting access to system components and cardholder data by business need to know are defined and understood.

NEW REQUIREMENT		APPLICABLE TO		EFFECTIVE DATE	
		All Entities	Service Providers Only	Immediately for all V4.0 Assessments	March 31, 2025
7.2.5.1	New requirement for review of all access by application and system accounts and related access privileges. ▶ Periodically (at the frequency defined in the entity's targeted risk analysis, which is performed according to all elements specified in Requirement 12.3.1).	X			X

REQUIREMENT 8

Identify Users and Authenticate Access to System Components. Processes and mechanisms for identifying users and authenticating access to system components are defined and understood.

	NEW REQUIREMENT	APPLICABLE TO		EFFECTIVE DATE	
		All Entities	Service Providers Only	Immediately for all V4.0 Assessments	March 31, 2025
8.6.3	New requirement for protecting passwords/ passphrases for application and system accounts against misuse. ▶ Passwords/passphrases are changed periodically (at the frequency defined in the entity's targeted risk analysis, which is performed according to all elements specified in Requirement 12.3.1) and upon suspicion or confirmation of compromise	X			X

REQUIREMENT 9

Restrict Physical Access to Cardholder Data. Processes and mechanisms for restricting physical access to cardholder data are defined and understood.

	NEW REQUIREMENT	APPLICABLE TO		EFFECTIVE DATE	
		All Entities	Service Providers Only	Immediately for all V4.0 Assessments	March 31, 2025
9.5.1.2.1	New requirement to define the frequency of periodic POI device inspections based on the entity's targeted risk analysis.	X			X

REQUIREMENT 10

Log and Monitor All Access to System Components and Cardholder Data. Processes and mechanisms for logging and monitoring all access to system components and cardholder data are defined and documented.

	NEW REQUIREMENT	APPLICABLE TO		EFFECTIVE DATE	
		All Entities	Service Providers Only	Immediately for all V4.0 Assessments	March 31, 2025
10.4.2.1	New requirement for a targeted risk analysis to define the frequency of periodic log reviews for all other system components (not defined in Requirement 10.4.1).	X			X

REQUIREMENT 11

Test Security of Systems and Networks Regularly. Processes and mechanisms for regularly testing security of systems and networks are defined and understood.

	NEW REQUIREMENT	APPLICABLE TO		EFFECTIVE DATE	
		All Entities	Service Providers Only	Immediately for all V4.0 Assessments	March 31, 2025
11.3.1.1	New requirement to manage all other applicable vulnerabilities (those not ranked as high-risk or critical) found during internal vulnerability scans. ▶ Addressed based on the risk defined in the entity's targeted risk analysis, which is performed according to all elements specified in Requirement 12.3.1	X			X
11.6.1	New requirement to deploy a change- and-tamper-detection mechanism to alert for unauthorized modifications to the HTTP headers and contents of payment pages as received by the consumer browser. The mechanism functions are performed as follows: ▶ At least once every seven days **OR** ▶ Periodically (at the frequency defined in the entity's targeted risk analysis, which is performed according to all elements specified in Requirement 12.3.1).	X			X

REQUIREMENT 12

Support Information Security with Organizational Policies and Programs. A comprehensive information security policy that governs and provides direction for protection of the entity's information assets is known and current.

	NEW REQUIREMENT	APPLICABLE TO		EFFECTIVE DATE	
		All Entities	Service Providers Only	Immediately for all V4.0 Assessments	March 31, 2025
12.3.1	New requirement to perform a targeted risk analysis for any PCI DSS requirement that provides flexibility for how frequently it is performed.	X			X
12.3.2	New requirement for entities using a Customized Approach to perform a targeted risk analysis for each PCI DSS requirement that the entity meets with the customized approach.	X		X	
12.10.4.1	New requirement to perform a targeted risk analysis to define the frequency of periodic training for incident response personnel.	X			X

APPENDIX E – TARGETED RISK ANALYSIS TEMPLATE

PCI DSS requirement 12.3.2 requires entity's using a customized approach to perform a TRA for each PCI DSS requirement that the entity meets with the customized approach. Appendix E1 and E2 provides entities with a template that the entity can use to document the customized approach and targeted risk.

RESPONSIBILITIES

The entity has the responsibility to document the TRA. They may document their TRA using any form or format the entity chooses as long as they include the requirements of 12.3.1. The TRA is to be completed prior to the assessor being onsite to start the assessment.

The assessor is responsible for reviewing the entity's TRA to determine if the TRA is completed correctly.

BDO USA Can Help

As a Qualified Security Assessor Company (QSAC), BDO USA has experienced QSAs who can assist your organization in understanding and transitioning to the new PCI V4.0 standards.

HAVE QUESTIONS OR WANT TO LEARN MORE? CONTACT US!

GREG SCHU
Cybersecurity, Compliance, and Assessments Services Principal
gschu@bdo.com

BRIAN HILL
Cybersecurity, Compliance, and Assessments Services Managing Director
bhill@bdo.com

FRED BRANTNER
Cybersecurity, Compliance, and Assessments Services Director
fbrantner@bdo.com

JAMES ROMAN
Cybersecurity, Compliance, and Assessments Services Senior Manager
james.roman@bdo.com