INFORMATION SUPPLEMENT

PCI DSS v4.x: Targeted Risk Analysis Guidance

Date: November 2023
Author: PCI Security Standards Council

Contents

Introducing Targeted Risk Analyses

PCI DSS v4.0 introduced the concept of targeted risk analysis (TRA) and includes two different types of TRAs. A description of each, answers to frequently asked questions, and a table that lists the PCI DSS requirements that specify completion of TRAs to define how frequently to perform an activity are provided in this document.

For any PCI DSS requirement that specifies a TRA to define how frequently to perform an activity

The first type of TRA, specified in PCI DSS Requirement 12.3.1, focuses on those PCI DSS requirements that allow an entity flexibility about how frequently to perform a given control. This TRA provides a framework for the entity to define an appropriate frequency based on their assessment of the risk to their environment.

For these TRAs, entities will identify the specific assets—for example, log files, or credentials—that the related requirement is intended to protect, as well as the threat(s) or outcomes from which the requirement is protecting the assets—for example, malware, an undetected intruder, or misuse of credentials. Examples of factors that could contribute to likelihood and/or impact of a threat being realized include any that could increase the vulnerability of an asset to a threat—for example, exposure to untrusted networks, complexity of an environment, high staff turnover—as well as the criticality of the system components or the volume and/or sensitivity of the data being protected. The performance of a TRA that incorporates these factors ensures a robust, comprehensive, and consistent assessment of risks for each applicable asset.

All elements that must be included in a TRA for PCI DSS requirements that allow flexibility about how frequently to perform an activity are documented in *PCI DSS v4.x Sample Template: Targeted Risk Analysis for Activity Frequency,* which can be found in the PCI SSC Document Library. Entities documenting TRA(s) to define an activity's frequency, while required to include all elements specified in this template, are not required to use the template or follow the template's specific format.

For any PCI DSS requirement that an entity meets with a customized approach

The second type of TRA, specified in Requirement 12.3.2, is for any requirement that an entity meets with the customized approach. This TRA supports the implementation of a repeatable and robust risk analysis methodology specific to a customized approach and is one of several activities the entity will perform to show how it meets the Customized Approach Objective. The outcome of this type of TRA allows the entity to identify risks, evaluate the effect on security if the defined requirement is not met, and describe how the entity has determined that the controls meet the Customized Approach Objective and provide at least an equivalent level of protection as the defined PCI DSS requirement. The assessor uses the customized approach documentation provided by the entity, including in this TRA, to plan and prepare for the assessment.

All elements that must be included in a TRA for any PCI DSS requirements that an entity meets with the customized approach are documented in *PCI DSS v4.x Sample Templates to Support Customized Approach* (that includes sample templates for both Controls Matrix and Targeted Risk Analysis), which can be found in the PCI SSC Document Library.

Note: Entities documenting either type of TRA, while required to include all elements specified these templates, are not required to use either template or follow each template's specific format.

Frequently Asked Questions about TRAs

1. **How does an entity know when TRAs are required to determine frequency of an activity?**

   TRAs to determine the frequency of an activity are required only when explicitly stated in a requirement; each of these requirements specify that a TRA is to be "performed in accordance with all elements specified in Requirement 12.3.1."

   The list of requirements that specify a TRA to determine activity frequency is provided, along with recommended frequencies, at the end of this document.

2. **How often should an entity perform a TRA to determine the frequency of an activity?**

   The entity initially undertakes the risk analysis exercise and prepares the TRA to define how frequently to perform the activity based on the entity's risk. Then the entity performs the activity in accordance with the TRA. Annually thereafter, the entity reviews the TRA to determine if the results are still valid and updates the TRA as needed. Reviewing the results of these TRAs at least once every 12 months and upon changes that could impact the risk to the environment allows the organization to ensure that the risk analysis results remain current with organizational changes and evolving threats, trends, and technologies, and that the selected frequencies still adequately address the entity's risk.

3. **Is there a sample template for the TRA to define the frequency of a periodic activity, similar to the sample templates provided for the customized approach?**

   Yes. The *PCI DSS v4.x Sample Template: Targeted Risk Analysis for Activity Frequency* can be found in the PCI SSC Document Library, using the "PCI DSS" filter. Though the use of this template is not required, all elements included in this template, as described in Requirement 12.3.1, must be documented in TRAs that define the frequency of activity.

4. **How is the TRA at Requirement 12.3.1 in PCI DSS v4.0 different from the annual risk assessment, as required in PCI DSS v3.2.1, Requirement 12.2?**

   The intent of PCI DSS v4.0 Requirement 12.3.1 is to focus on certain targeted risk areas specific to PCI DSS requirements, whereas PCI DSS v3.2.1 required a general risk assessment, which many organizations were meeting with an enterprise-wide risk assessment that may not have been specific to payment account data.

An enterprise-wide risk assessment process may be established as part of an entity's overarching risk management program and information from that risk assessment could provide input into TRA processes. Note that an enterprise-wide risk assessment is recommended but is not required for PCI DSS v4.0. Examples of risk-assessment methodologies for enterprise-wide risk assessments include, but are not limited to, ISO 27005 and NIST SP 800-30.

5. **Can an entity complete a *Targeted Risk Analysis for Activity Frequency* if they want to perform an activity *less* frequently than stated in a PCI DSS requirement**?

   No. This type of TRA cannot be used for this purpose. If a requirement states that an activity must be performed at a specific frequency, an organization must perform the activity at least at the defined frequency to meet the requirement as stated. If an organization performs an activity less frequently than the requirement states, they are not meeting that PCI DSS requirement.

   Alternatively, the organization can choose to meet the requirement's Customized Approach Objective, providing that the entity designs, implements, tests, and documents a customized control that meets the Customized Approach Objective for that requirement. Note that a TRA is required for the customized approach, and completion of a TRA for the customized approach is one of several activities the entity will perform to show how it meets the Customized Approach Objective. Refer to PCI DSS v4.0 Appendix D for details about the customized approach.

6. **Should an entity complete a *Targeted Risk Analysis for Activity Frequency* if they want to perform an activity *more* frequently than stated in a PCI DSS requirement?**

   No. If an organization would like to perform an activity more frequently than a requirement states, they can do so without performing a TRA.

7. **If an entity has a legitimate technical or business constraint that prevents it from meeting the frequency as stated in a PCI DSS requirement, is a TRA required?**

   No. If there is a documented business or technical constraint preventing the organization from meeting the requirement's specified frequency, a compensating control can be documented and put in place to mitigate the risk associated with not meeting the PCI DSS requirement as stated.

8. **What is the assessor's role in reviewing an entity's TRA to determine the frequency of an activity?**

   The assessor's role is to make sure that all the elements specified in Requirement 12.3.1 are documented in the entity's TRA, including that the entity justified how frequently the activity must be performed and how this frequency addresses the entity's risk.

PCI DSS v4.x TRA Requirements and Frequency Recommendations

The table below lists all PCI DSS requirements that specify completion of a TRA to define how frequently an activity is performed, along with guidance on recommended frequencies for the related activities.

Note that even where the Suggested Frequency in the table below is followed, a TRA will be required to document and support the frequency selected. All required components must be included in the TRA, as specified in PCI DSS v4.0 Requirement 12.3.1.

PCI DSS v4.0 Requirement[1]	Suggested Frequency[2]
5.2.3.1 The frequency for periodic evaluations for system components identified as not at risk for malware is defined in the entity's targeted risk analysis.	At least once every six months
5.3.2.1 If periodic malware scans are performed to meet Requirement 5.3.2, the frequency of scans is defined in the entity's targeted risk analysis.	At least once a day/daily
7.2.5.1 All access by application & system accounts and related access privileges are reviewed periodically (at the frequency defined in the entity's targeted risk analysis).	At least once every six months
8.6.3 Passwords/passphrases for application and system accounts are changed periodically (at the frequency defined in the entity's targeted risk analysis).	At least once every three months
9.5.1.2.1 The frequency of periodic POI device inspections and the type of inspections performed is defined in the entity's targeted risk analysis.	At least once every month/monthly
10.4.2.1 The frequency of periodic log reviews for all other system components (not defined in Requirement 10.4.1) is defined in the entity's targeted risk analysis.	At least once every seven days/Weekly
11.3.1.1 All other applicable vulnerabilities (those not ranked as high-risk or critical per the entity's vulnerability risk rankings defined at Requirement 6.3.1) are addressed based on the risk defined in the entity's targeted risk analysis.	Medium: Within three months Low: Within six months Informational: Monitor regularly
11.6.1 A change- and tamper-detection mechanism is deployed to detect unauthorized modifications to HTTP headers and contents of payment pages, with the mechanism functions performed at least once every seven days OR periodically at the frequency defined in the entity's targeted risk analysis.	At least once every seven days
12.10.4.1 The frequency of periodic training for incident response personnel is defined in the entity's targeted risk analysis.	At least once a year and at the start of employment

[1] This column represents summarized extracts of the requirements to focus on the TRA elements of each. Refer to PCI DSS v4.0 for the full requirements.

[2] The Suggested Frequency column includes baseline recommendations that entities may wish to consider as input to their decision-making process when assessing risk and determining an appropriate activity frequency for their environment. Each entity should use their specific TRA results to determine the minimum frequencies needed to address the entity's risk and best protect the entity's environment.