PCI DSS v4.x Sample Templates to Support the Customized Approach

This document contains example templates for the controls matrix and a targeted risk analysis, to be documented by the entity as part of the customized approach. These templates are examples of formats that could be used.

Note: *While it is not required that entities follow the specific formats provided below, the entity's control matrix and targeted risk analysis must include all the information in these templates, as defined in PCI DSS v4.x Requirement 12.3.2.*

Customized Approach - Sample Controls Matrix Template

The following is a sample controls matrix template that an entity may use to document their customized implementation.

As described in *PCI DSS v4.x Appendix D: Customized Approach*, entities using the customized approach must complete a controls matrix to provide details for each implemented control that explain what is implemented, how the entity has determined that the controls meet the stated objective of a PCI DSS requirement, how the control provides at least the equivalent level of protection as would be achieved by meeting the defined requirement, and how the entity has assurance about the effectiveness of the control on an ongoing basis.

The assessor uses the information within each controls matrix to plan and prepare for the assessment.

This sample controls matrix template includes the minimum information to be documented by the entity and provided to the assessor for a customized validation. While it is not required that this specific template be used, it is required that the entity's customized approach documentation includes all information defined in this template, and that the entity provides this exact information to its assessor.

The controls matrix does not replace the need for the assessor to independently develop appropriate testing procedures for validating the implemented controls. The assessor must still perform the necessary testing to verify the controls meet the objective of the requirement, are effective, and are properly maintained. The controls matrix also does not replace the reporting requirements for customized validations as specified in the ROC Template.

The controls matrix must include at least the information in the following table.

Sample Controls Matrix Template for PCI DSS Requirements met via the Customized Approach To be completed by the entity being assessed		
Customized control name/identifier	<Entity defines how they want to refer to this control>	
PCI DSS Requirement(s) number and objective(s) that is met with this control(s)	Requirement #: Requirement #:	Objective: Objective:
Details of control(s)		
What is the implemented control(s)?	<Entity describes what the control is and what it does>	
Where is the control(s) implemented?	<Entity identifies locations of facilities and system components where control is implemented and managed>	
When is the control(s) performed?	<Entity details how frequently the control is performed – for example, runs continuously in real time or is scheduled to run at NN times and at XX intervals>	
Who has overall responsibility and accountability for the control(s)?	<Entity includes details of individual personnel/roles with responsibility and accountability for this control>	
Who is involved in managing, maintaining, and monitoring the control(s)?	<Entity includes details of individual personnel/roles and/or teams, as applicable, that manage, maintain, and monitor the control>	
If applicable, how is the control(s) an enhancement to any other PCI DSS control(s) already required for the item under review?	<Entity describes how this control is an enhancement to any other PCI DSS control(s) required for the item under review >	

Sample Controls Matrix Template for PCI DSS Requirements met via the Customized Approach To be completed by the entity being assessed	
For each **PCI DSS requirement for which the customized control(s) is used, the entity provides details of the following:**	
Entity describes how the implemented control(s) meets the stated ***Customized Approach Objective*** of the PCI DSS requirement.	<Entity describes how the control meets the stated customized approach objective of the PCI DSS requirement, and summarizes related results>
Entity describes testing **it performed** and the results of that testing that demonstrates the control(s) meets the objective of the applicable requirement.	<Entity describes the testing it performed to prove the control meets the stated objective of the PCI DSS requirement, and summarizes related results>
Entity briefly describes the results of the separate targeted risk analysis **it performed** that explains the control(s) implemented and describes how the results verify the control(s) provides at least an equivalent level of protection as the defined approach for the applicable PCI DSS requirement. *See the separate Customized Approach - SampleTargeted Risk Analysis Template for details on how to document this risk analysis.*	<Entity briefly describes the results of its risk analysis for this control, which is detailed separately in the Targeted Risk Analysis>
Entity describes the measures **it has implemented** to ensure the control(s) is maintained and its effectiveness is assured on an ongoing basis. *For example, how the entity monitors for control effectiveness, how control failures are detected and responded to, and the actions taken.*	<Entity describes how it ensures the control is maintained and how the control's effectiveness is assured.>

Customized Approach - Sample Targeted Risk Analysis Template

The following is a sample targeted risk analysis template an entity may use for their customized implementation. *While it is not required that an entity follow this specific format, its customized approach documentation must include all the information defined in this template.*

As described in PCI DSS v4.x *Appendix D: Customized Approach*, an entity using the customized approach must provide a detailed targeted risk analysis for each requirement the entity is meeting with the customized approach. The risk analysis defines the risk, describes how the entity has determined that the controls meet the Customized Approach Objective, and how the entity has determined that the controls provide at least an equivalent level of protection as the defined PCI DSS requirement.

The assessor uses the information in the targeted risk analysis to plan and prepare for the assessment.

In completing a targeted risk analysis for a customized approach, it is important to remember that:

- The asset being protected is the cardholder data that is stored, processed, or transmitted by the entity.
- The threat actor is highly motivated and capable. The motivation and capability of threat actors tends to increase in relation to the volume of cardholder data that a successful attack will realize.
- The likelihood that an entity will be targeted by threat actors increases as the entity stores, processes, or transmits greater volumes of cardholder data.
- The mischief is directly related to the objective. For example, if the objective is "malicious software cannot execute", the mischief is that malicious software executes; if the objective is "day-to-day responsibilities for performing all the activities are allocated", the mischief is that the responsibilities are not allocated.

Note: *The term "mischief" as used in this targeted risk analysis (for example, in 1.3 in the table below) refers to an occurrence or event that negatively affects the security posture of the entity. Examples of this are the absence of a policy, the failure to conduct a vulnerability scan, or that malware executes in the entity's environment.*

This sample targeted risk analysis template includes the minimum information to be documented by the entity and provided to the assessor for a customized validation. While it is not required that this specific template be used, it is required that the entity's customized approach documentation include all information defined in this template, and that the entity provides this exact information to its assessor.

The targeted risk analysis must include at least the information in the following table.

Sample Targeted Risk Analysis for PCI DSS Requirements met via the Customized Approach To be completed by the entity being assessed	
Item	**Details**
1. Identify the requirement	
1.1 Identify the PCI DSS requirement as written.	<Entity identifies the requirement>
1.2 Identify the objective of the PCI DSS requirement as written.	<Entity identifies the objective of the requirement>
1.3 Describe the mischief that the requirement was designed to prevent	<Entity describes the mischief> <Entity describes the effect on its security if the objective is not successfully met by the entity.> <Entity describes which security fundamentals would not be in place, or what a threat actor may be able to do if the objective is not successfully met by the entity.>
2. Describe the proposed solution	
2.1 Customized control name/identifier	<Entity identifies the customized control as documented in the Controls Matrix.>
2.2 What parts of the requirement as written will change in the proposed solution?	<Entity identifies what elements of the requirement will not be met by the defined approach and so will be covered by customized approach. This could be as small as changing the periodicity of a requirement, or the implementation of a completely different set of controls to meet the objective.>
2.3 How will the proposed solution prevent the mischief?	<Entity describes how the controls detailed in the Controls Matrix will prevent the mischief identified in 1.3.>

Sample Targeted Risk Analysis for PCI DSS Requirements met via the Customized Approach To be completed by the entity being assessed						
Item	**Details**					
3. Analyze any changes to the LIKELIHOOD of the mischief occurring, leading to a breach in confidentiality of cardholder data						
3.1 Describe the factors detailed in the Control Matrix that affect the likelihood of the mischief occurring.	Entity describes: • How successful the controls will be at preventing the mischief • How the controls detailed in the Control Matrix reduce the likelihood of the mischief occurring					
3.2 Describe the reasons the mischief may still occur after the application of the customized control.	Entity describes: • The typical reasons for the control to fail, the likelihood of this, and how could it be prevented • How resilient the entity's processes and systems are for detecting that the control(s) are not operating normally? • How a threat actor could bypass this control – what steps would they need to take, how hard is it, would the threat actor be detected before the control failed? How has this been determined?					
3.3 To what extent do the controls detailed in the customized approach represent a change in the likelihood of the mischief occurring when compared with the defined approach requirement?	Mischief more likely to occur	☐	No change	☐	Mischief less likely to occur	☐
3.4 Provide the reasoning for your assessment of the change in likelihood that the mischief occurs once the customized controls are in place.	Entity provides: • The justification for the assessment documented at 3.3. • The criteria and values used for the assessment documented at 3.3.					

Sample Targeted Risk Analysis for PCI DSS Requirements met via the Customized Approach To be completed by the entity being assessed				
Item	**Details**			
4. Analyze any changes to the IMPACT of unauthorized access to PANs				
4.1 For the scope of system components that this solution covers what volume of PANs would be at risk of unauthorized access if the solution failed?	**4.1.1** Number of stored PANs	*Maximum at any one time*	**4.1.2** Number of PANs processed or transmitted over a 12-month period	*Total*
4.2 Description of how the customized controls will directly: • Reduce the number of individual PANs compromised if a threat actor is successful, and/or • Allow quicker notification of the PANs compromised to the card brands.	Impact to the payment ecosystem is directly related to the number of accounts compromised and how quickly any compromised PANs can be blocked by the card issuer. Entity describes how the customized controls achieve the following if any of the customized controls: • Reduce the volume of cardholder data that is stored, processed, or transmitted and therefore reduce what is available to a successful threat actor, and/or • Decrease the time to detection, notification of compromised accounts, and containment of the threat actor.			
5. Risk approval and review				
5.1 I have reviewed the above risk analysis and I agree that the use of the proposed customized approach as detailed provides at least an equivalent level of protection as the defined approach for the applicable PCI DSS requirement.	A member of executive management must review and agree to the proposed customized approach. <Member of entity's executive management signs that it reviewed and agreed to the customized approach documented herein.>			
5.2 This risk analysis must be reviewed and updated no later than:	The risk analysis should be reviewed at least every twelve months and more frequently if the customized approach itself is time limited (for example, because there is a planned change in technology) or if other factors dictate a needed change. In the event of an unscheduled risk review, detail the reason the review occurred. <Entity indicates date the targeted risk analysis was reviewed and updated.>			