Payment Card Industry

3-D Secure (PCI 3DS)

Report on Compliance

Template for use with PCI 3DS Core Security Standard

Version 1.0, Revision 1.0

December 2017

Document Changes

Date	Version	Description
December 2017	PCI 3DS Core Security Standard v1.0, Revision1.0	To introduce the template for PCI 3DS Reports on Compliance. This document is intended for use with version 1.0 of the *PCI 3DS Security Requirements and Assessment Procedures for EMV® 3-D Secure Core Components: ACS, DS, and 3DS Server* (PCI 3DS Core Security Standard).

Table of Contents

Introduction to the PCI 3DS Reporting Template

This document, the *PCI 3DS Template for Report on Compliance for use with PCI 3DS Security Requirements and Assessment Procedures for EMV® 3-D Secure Core Components: ACS, DS, and 3DS Server* ("3DS ROC Reporting Template"), is the mandatory template for PCI 3DS Assessors completing an Assessment Report for assessments against the *PCI 3DS Security Requirements and Assessment Procedures for EMV® 3-D Secure Core Components: ACS, DS, and 3DS Server* (PCI 3DS Core Security Standard). The 3DS ROC Reporting Template provides reporting instructions and the reporting template for 3DS Assessors to use. This will help provide reasonable assurance that a consistent level of reporting against the PCI 3DS Core Security Standard is present among assessors.

Use of the 3DS ROC Reporting Template is mandatory. Do not delete any content from any place in this document, including this section and the versioning above. Addition of text or sections is applicable within reason, as noted within this document.

Tables have been included in this template to facilitate the reporting process for certain lists and other information as appropriate. The tables in this template may be modified to increase/decrease the number of rows, or to change column width. Additional appendices may be added if the assessor feels there is relevant information to be included that is not addressed in the current format. However, the assessor must not remove any details from the tables provided in this document. Personalization, such as the addition of company logos, is acceptable.

The 3DS Report on Compliance (3DS ROC) is produced during PCI 3DS assessments as part of a 3DS entity's assessment process. The 3DS ROC provides details about the entity's environment and assessment methodology, and documents the entity's compliance status for each PCI 3DS Requirement. A PCI 3DS compliance assessment involves thorough testing and assessment activities, from which the assessor will generate detailed work papers. These work papers contain comprehensive records of the assessment activities including observations, results of system testing, configuration data, file lists, interview notes, documentation excerpts, references, screenshots, and other evidence collected during the course of the assessment. The 3DS ROC is effectively a ***summary of evidence*** derived from the assessor's work papers to describe how the assessor performed the validation activities and how the resultant findings were reached. At a high level, the 3DS ROC provides a comprehensive ***summary of testing activities performed and information collected*** during the assessment against the PCI 3DS Core Security Standard. The information contained in a 3DS ROC must provide enough detail and coverage to verify that the assessed entity is compliant with all PCI 3DS Core Security Requirements.

Note: *The PCI 3DS Core Security Standard does not address how an entity would meet the requirements in the EMV® 3-D Secure Protocol and Core Functions Specification.*

Report Sections

The Report includes the following sections and appendices:

- Section 1: Contact Information and Report Summary
- Section 2: Description of Scope of Work and Approach Taken
- Section 3: Details about Reviewed Environment
- Section 4: Findings and Observations
  - Part 1: Baseline Security Requirements
  - Part 2: 3DS Security Requirements
- Appendix A: Compensating Controls Worksheet
- Appendix B: Explanation of Non-Applicability

All sections must be thoroughly and accurately completed. The Reporting Template includes tables with built-in reporting instructions to help assessors provide all required information throughout the document. Responses should be specific, but efficient. Details provided should focus on concise quality of detail rather than lengthy, repeated verbiage. Parroting the testing procedure within a description is discouraged, as it does not add any level of assurance to the narrative. Use of template language for summaries and descriptions is discouraged and details should be specifically relevant to the assessed entity.

Summary of Assessor Findings

This Reporting Template provides:

(1) At-a-glance overviews of assessment results for PCI 3DS Part 1 and Part 2 Requirements (located in Sections 4.1.1 and 4.2.1, respectively) with check boxes to indicate whether the assessment findings are "In Place," "In Place w/CCW," "N/A," or "Not in Place"; and

(2) Separate reporting space with instructions for assessors to document details of the testing that took place and subsequent results (located in Sections 4.1.2 and 4.2.2, respectively).

There are four results possible—In Place, In Place with CCW (Compensating Control Worksheet), Not in Place, and Not Applicable—and one selection only is to be made.

The following table is a helpful representation when considering which selection to make. Reporting details and results should be consistent throughout the Report on Compliance, as well as consistent with related reporting, such as the Attestation of Compliance (AOC).

Response	When to use this response:
In Place	The expected testing has been performed, and all elements of the requirement have been met as stated.
In Place w/CCW (Compensating Control Worksheet)	The expected testing has been performed, and the requirement has been met with the assistance of a compensating control. All responses in this column require completion of a Compensating Control Worksheet (CCW). Information on the use of compensating controls and guidance for completing the worksheet is provided in the PCI 3DS Standard.
Not in Place	Some or all elements of the requirement have not been met, are in the process of being implemented, or require further testing before it will be known whether they are in place.
N/A (Not Applicable)	The requirement does not apply to the organization's environment. All "not applicable" responses require reporting on testing performed to confirm the "not applicable" status. Note that a "Not Applicable" response still requires a detailed description explaining how it was determined that the requirement does not apply.

Dependence on another service provider's compliance

Generally, when reporting on a requirement where a third-party service provider is responsible for the tasks, an acceptable response for an "in place" finding may be something like:

> *Assessor verified this is the responsibility of Service Provider X, as verified through review of x/y contract (document). Assessor reviewed the AOC for Service Provider X, dated MM/DD/YYYY, and confirmed the service provider was found to be compliant against* ***standard/version*** *for all applicable requirements, and that it covers the scope of the services used by the assessed entity.*

That response could vary, but what's important is that the finding is noted as "in place" and that there has been a level of testing by the assessor to support the conclusion that this responsibility is verified and that the responsible party has been tested against the requirement and found to be compliant.

Do's and Don'ts: Reporting Expectations

DO:	*DON'T:*
▪ Use this Reporting Template when assessing against the PCI 3DS Core Security Standard. ▪ Complete all sections in the order specified. ▪ Read and understand the intent of each Requirement and Validation Method. ▪ Provide a response for every Validation Method. ▪ Provide sufficient detail and information to support the designated finding, but be concise. ▪ Describe *how* a Requirement was verified per the Reporting Instruction, not just that it *was* verified. ▪ Ensure all parts of the Validation Method and Reporting Instruction are addressed. ▪ Ensure the response covers all applicable system components. ▪ Perform an internal quality assurance review of the 3DS ROC for clarity, accuracy, and quality. ▪ Provide useful, meaningful diagrams, as directed.	▪ Don't report items as "In Place" unless they have been verified as being "in place" as stated. ▪ Don't include forward-looking statements or project plans in the "In Place" assessor response. ▪ Don't simply repeat or echo the Validation Method in the response. ▪ Don't copy responses from one Validation Method to another. ▪ Don't copy responses from previous assessments. ▪ Don't include information irrelevant to the assessment. ▪ Don't leave any spaces blank. If a section does not apply, annotate it as such.

Reporting Template for PCI 3DS Report on Compliance

This template is to be used for creating a PCI 3DS ROC. Content and format is defined as follows:

1. Contact Information and Report Summary

1.1 Contact information

Client	
▪ Company name:	
▪ Company address:	
▪ Company URL:	
▪ Company contact name:	
▪ Contact phone number:	
▪ Contact e-mail address:	
Assessor Company	
▪ Company name:	
▪ Company address:	
▪ Company website:	
Assessor	
▪ Assessor name:	
▪ Assessor PCI credentials: *(QSA, PA-QSA, etc.)*	
▪ Assessor phone number:	
▪ Assessor e-mail address:	
Assessor Quality Assurance (QA) Primary Reviewer for this specific report (not the general QA contact for the QSA)	
▪ QA reviewer name:	
▪ QA reviewer phone number:	
▪ QA reviewer e-mail address:	

1.2 Date and timeframe of assessment

• **Date of Report:** ***Note:*** *This date must be shown as the "3DS ROC Completion Date" in Part 3, PCI 3DS Validation, of the 3DS AOC.*	
• Timeframe of assessment *(start date to completion date):*	
• Identify date(s) spent onsite at the entity:	
• Describe the time spent onsite at the entity, time spent performing remote assessment activities, and time spent on validation of remediation activities.	

1.3 PCI 3DS Core Security Standard version

• Version of the 3DS Core Security Standard used for the assessment: ***Note:*** *Should be PCI 3DS v1.0.*	

1.4 Additional services provided by QSA Company

The PCI SSC Qualification Requirements for Qualified Security Assessors (QSA) includes content on "Independence," which specifies requirements for assessor disclosure of services and/or offerings that could reasonably be viewed to affect independence of assessment. Complete the below after review of relevant portions of the Qualification Requirements document(s) to ensure responses are consistent with documented obligations.

▪ Disclose all services offered to the assessed entity by the QSAC, including but not limited to whether the assessed entity uses any security-related devices or security-related applications that have been developed or manufactured by the QSA, or to which the QSA owns the rights or that the QSA has configured or manages:	
▪ Describe efforts made to ensure no conflict of interest resulted from the above mentioned services provided by the QSAC:	

2. Description of Scope of Work and Approach Taken

2.1 Description of how the entity performs or provides 3DS functions

Provide an overview of the entity's 3DS functions, including:

• Which 3DS functions are covered by this assessment? *(Check all that apply)*	☐ 3DS Server (3DSS) ☐ Access Control Server (ACS) ☐ Directory Server (DS)
• Describe the nature of the entity's business (what kind of work they do, etc.) ***Note:*** *This is not intended to be a cut-and-paste from the entity's website, but should be a tailored description that shows the assessor understands the business of the entity being assessed.*	
• Describe how the entity performs or provides 3DS functions. ***Note:*** *This is not intended to be a cut-and-paste from above, but should build on the understanding of the business and the impact this can have upon the security of the 3DS data environment (3DE) and 3DS data and processes.*	
• Identify the types of 3DS payment channels the entity serves—e.g., e-commerce, m-commerce, or both.	
• Other details, if applicable:	

2.2 Assessor's validation of defined 3DS environment (3DE) and scope accuracy

Document how the assessor validated the scope of the 3DS assessment.

• Describe the methods or processes (for example, types of tools, observations, feedback, scans, data flow analysis) used to verify that the PCI 3DS assessment scope is accurate and covers all system components, processes, and people in scope for the PCI 3DS assessment.	
• Provide the name of the assessor who attests that the defined 3DE and scope of 3DS assessment has been verified to be accurate, to the best of the assessor's ability and with all due diligence.	

2.3 Assessor's validation of applicability and alignment between PCI 3DS and PCI DSS

Document how the assessor validated the applicability of PCI DSS to the PCI 3DS assessment.

Where PCI DSS has been applied to the 3DS environment as described below, the implementation of additional controls may not be needed to meet the PCI 3DS Part 1 Requirements:

1. The 3DE is contained within a CDE, and all 3DS system components—including supporting infrastructure and systems—are included in scope for the applicable PCI DSS requirements, ***and***
2. The applicable PCI DSS requirements are confirmed to be "In Place" through a PCI DSS assessment performed no more than 12 months prior to the 3DS assessment.

A 3DS entity that has applied PCI DSS to protect its 3DE as described above may be able to leverage the results of its PCI DSS assessment to meet the PCI 3DS Part 1: Baseline Security Requirements. Refer to *Appendix B: Alignment between PCI 3DS and PCI DSS Requirements* of the PCI 3DS Core Security Standard for full details and requirements for this approach.

• Is the 3DS entity leveraging the results of their PCI DSS assessment to meet the PCI 3DS Part 1: Baseline Security Requirements?	☐ Yes ☐ No

If the answer to the above is:

- ***No: Go to Section 3***
- ***Yes: Complete the following***

• Provide the document name(s) and date of PCI DSS ROC and AOC being leveraged by the 3DS entity. ***Note:*** *The PCI DSS ROC and AOC must be dated no more than 12 months prior to the date of completion of the 3DS assessment.*	
• Describe how the 3DS Assessor verified that the PCI DSS assessment scope covered all systems components, processes, and people in scope for the PCI 3DS assessment.	

Note: Whether a 3DS entity is required to validate to PCI DSS, to the PCI 3DS Core Security Standard, or to both, is defined by individual payment brand compliance programs.

Details of PCI DSS Requirements leveraged to meet PCI 3DS Part 1: Baseline Security Requirements

For each 3DS Part 1 Baseline Requirement, select one of the following:

- **Full** – The corresponding PCI DSS requirement(s) and sub-requirements were ALL identified as "In Place" in the PCI DSS assessment.
- **Partial** – One or more of the corresponding PCI DSS requirements was identified as "Not Applicable" (N/A) in the PCI DSS assessment.

For all requirements identified as "Partial," provide details in the "Justification for all PCI DSS N/A Requirements" column, including:

- Details of specific PCI DSS requirements and sub-requirements that were marked as "Not Applicable" for the PCI DSS assessment
- The reason those requirements were identified as being Not Applicable for the PCI DSS assessment
- Details of how the 3DS assessor verified those PCI DSS requirements are also Not Applicable for this 3DS assessment

3DS Part 1 Baseline Requirement	Corresponding PCI DSS Requirements	PCI DSS Coverage		Justification for all PCI DSS N/A Requirements *(Required for all "Partial" responses)*
		Full – All PCI DSS Requirements identified as "In Place"	**Partial** – One or more PCI DSS requirements identified as "N/A"	
1. Maintain security policies for all personnel	• Requirement 12	☐	☐	
2. Secure network connectivity	• Requirement 1 • Requirement 10 • Requirement 11	☐	☐	
3. Develop and maintain secure systems	• Requirement 2 • Requirement 6	☐	☐	
4. Vulnerability management	• Requirement 5 • Requirement 6 • Requirement 11	☐	☐	
5. Manage access	• Requirement 7 • Requirement 8	☐	☐	
6. Physical security	• Requirement 9	☐	☐	
7. Incident response preparedness	• Requirement 10 • Requirement 12	☐	☐	

3. Details about Reviewed Environment

3.1 Detailed network diagram(s)

Provide one or more ***detailed diagrams*** to illustrate each communication/connection point between in scope networks/environments/facilities. Diagrams should include the following:

- Critical components within the 3DS data environment (3DE), including systems, databases, and web servers, as applicable
- All boundaries of the 3DS data environment
- Any network segmentation points which are used to reduce scope of the assessment
- Boundaries between trusted and untrusted networks
- Wireless and wired networks
- All other connection points applicable to the assessment
- Other necessary payment components, as applicable

Ensure the diagram(s) include enough detail to clearly understand how each communication point functions and is secured.

For example, the level of detail may include identifying the types of devices, device interfaces, network technologies, protocols, and security controls applicable to that communication point.

<Insert detailed diagram(s)>

3.2 Description of 3DS data flows

<Insert 3DS data flow diagram(s)>

3.3 Storage of 3DS Sensitive Data

Identify and list all databases, tables, and files storing 3DS sensitive data and provide the following details.

Note: *The list of files and tables that store cardholder data in the table below must be supported by an inventory created (or obtained from the client) and retained by the assessor in the work papers.*

Note: *Refer to the PCI 3DS Data Matrix for details of 3DS sensitive data and to understand which 3DS data elements are permitted to be stored by which 3DS entities (3DSS, ACS, DS).*

Data Store (database, etc.)	**File(s) and/or Table(s)**	**3DS sensitive data elements stored ***	**How data is secured ****	**How access to data stores is logged *****

* *For example, authentication value, issuer image, ACS HTML.*

** *For example, use of encryption, access controls, truncation, etc.*

*** *Description of logging mechanism used for logging access to data—for example, enterprise log-management solution, application-level logging, operating-system logging, etc.*

3.4 Critical hardware and software in use in the 3DS environment

Identify and list all types of hardware and critical software in the cardholder environment. Critical hardware includes network components, servers and other mainframes, devices performing security functions, end-user devices (such as laptops and workstations), virtualized devices (if applicable) and any other critical hardware—including homegrown components. Critical software includes e-commerce applications, software performing security functions or enforcing PCI DSS and 3DS controls, underlying operating systems that store, process, or transmit 3DS data, system-management software, virtualization-management software, and other critical software—including homegrown software/applications. For each item in the list, provide details for the hardware and software as indicated below. Add rows, as needed.

Critical Hardware			Critical Software		Role/Functionality
Type of Device (firewall, server, IDS, etc.)	**Vendor**	**Make/Model**	**Name of Software Product**	**Version or Release**	

3.5 Sampling

Identify whether sampling was used during the 3DS assessment.

• **If sampling is not used:**	
• Provide the name of the assessor who attests that every system component in the 3DE has been assessed.	
• **If sampling is used:**	
• Provide the name of the assessor who attests that all sample sets used for this assessment are represented in the below "Sample sets for reporting" table. *Examples may include, but are not limited to firewalls, application servers, retail locations, data centers, User IDs, people, etc.*	
• Describe the sampling rationale used for selecting sample sizes (for people, processes, technologies, devices, locations/sites, etc.).	
• If standardized 3DS security and operational processes/controls were used for selecting sample sizes, describe how they were validated by the assessor.	

3.6 Sample sets for reporting

Note: *If sampling is used, this section MUST be completed. When a reporting instruction asks to identify a sample, the 3DS Assessor may either refer to the Sample Set Reference Number (for example "Sample Set-1") OR list the sampled items individually in the response. Examples of sample sets may include, but are not limited to, firewalls, application servers, retail locations, data centers, User IDs, people, etc. Add rows as needed.*

Sample Set Reference Number	**Sample Type/ Description** (e.g., firewalls, datacenters, change records, User IDs, etc.)	**Listing of all items in the Sample Set** (devices, locations, change records, people, etc.)	**Make/Model of Components** (as applicable)	**Total Sampled**	**Total Population**
Sample Set-1					
Sample Set-2					
Sample Set-3					

3.7 Third-Party Service Providers and other third-party outsourcing that can impact 3DS functionality of the security of the 3DE

For each service provider or third party, provide:

Name of Third-Party Service Provider	**Purpose for sharing 3DS data ***	**Which PCI 3DS requirements are the responsibility of the service provider?**	**How the TPSP demonstrated compliance for the PCI 3DS requirements for which the TPSP is responsible ****

** For example, third-party storage, transaction processing, etc.*

*** For example, status of PCI 3DS Compliance with date of AOC and version #, or required evidence provided by the TPSP.*

3.8 Documentation reviewed

Note: *When a reporting instruction asks to identify a documented procedure or policy, the 3DS Assessor may either refer to the Documentation reviewed (for example "Doc-1") OR list the documentation reviewed individually in the response. Add rows as needed.*

Identify and list all reviewed documents. Include the following:

Reference Number *(optional)*	Document Name *(including version, if applicable)*	Brief description of document purpose	Document date *(latest version date)*
Doc-1			
Doc-2			
Doc-3			
Doc-4			
Doc-5			
Doc-6			
Doc-7			

3.9 Individuals interviewed

Note: *When a reporting instruction asks to identify an individual interviewed, the 3DS Assessor may either refer to the Individuals interviewed (for example "Int-1") OR list the individuals interviewed individually in the response. Add rows as needed.*

Identify and list the individuals interviewed. Include the following:

Reference Number *(optional)*	Employee Name	Role/Job Title	Organization	Purpose/topics covered in interview
Int-1				
Int-2				
Int-3				
Int-4				
Int-5				
Int-6				
Int-7				

3.10 Disclosure summary for "In Place with Compensating Control" responses

• Identify whether there were any responses indicated as "In Place with Compensating Control."	☐ Yes ☐ No
• *If "Yes," complete the table below:*	

List of all requirements/testing procedures with this result	**Summary of the issue** (legal obligation, etc.)

4. Findings and Observations

4.1 PCI 3DS Part 1: 3DS Baseline Security Requirements

• Is the 3DS entity leveraging the results of their PCI DSS assessment to meet the PCI 3DS Part 1: Baseline Security Requirements?	☐ Yes ☐ No
If Yes: *Select "In Place per PCI DSS" in the PCI 3DS Part 1: Summary of Assessment Findings table (Section 4.1.1). Do not complete the Detailed Findings and Observations for 3DS Part 1 Requirements (Section 4.1.2). Details of the PCI DSS assessment must be provided in Section 2.3.*	
If No: *Select an appropriate finding in the PCI 3DS Part 1: Summary of Assessment Findings table (Section 4.1.1) and complete the Detailed Findings and Observations for 3DS Part 1 Requirements (Section 4.1.2).*	

4.1.1 Summary of Findings for PCI 3DS Part 1 Requirements

Identify the appropriate assessment result for each high-level PCI 3DS requirement. Complete the table as follows:

- If the results of a PCI DSS assessment have been verified as meeting all the PCI 3DS Part 1 Requirements (as stated in Section 2.2):
    1. Select "In Place per PCI DSS" in the *PCI 3DS Part 1: Summary of Assessment Findings* table.
    2. Go to Section 4.2.
- If a PCI DSS assessment is not being leveraged to meet PCI 3DS Part 1 Requirements, select the appropriate finding for each high-level 3DS Part 1 Requirement. The information provided here must be supported by the detailed Findings and Observations (Section 4.1.2).

  When determining the appropriate finding for each high-level 3DS requirement, the following principles apply:

    1. If the finding for any requirement or sub-requirement is "Not in Place," select "Not in Place" for the high-level requirement.
    2. If the finding for any requirement or sub-requirement is "N/A" and all other requirements are "In Place," select "In Place" for the high-level requirement.
    3. If the finding for any requirement or sub-requirement is "In Place w/CCW" and all other requirements are "In Place," select "In Place w/CCW" for the high-level requirement.
    4. If the findings include one or more requirements or sub-requirements as "N/A," and one or more as "In Place w/CCW," and all other requirements are "In Place," select "In Place w/CCW" for the high-level requirement.
    5. If all requirements and sub-requirements are identified as "In Place," select "In Place" for the high-level requirement.

PCI 3DS Part 1: Summary of Assessment Findings

		In Place per PCI DSS		*In Place*	*In Place w/CCW*	*N/A*	*Not in Place*
Part 1: Baseline Security Requirements							
P1-1	Maintain security policies for all personnel			☐	☐	☐	☐
P1-2	Secure network connectivity			☐	☐	☐	☐
P1-3	Develop and maintain secure systems			☐	☐	☐	☐
P1-4	Vulnerability management	☐	***OR***	☐	☐	☐	☐
P1-5	Manage access			☐	☐	☐	☐
P1-6	Physical security			☐	☐	☐	☐
P1-7	Incident response preparedness			☐	☐	☐	☐

4.1.2 Detailed Findings and Observations for PCI 3DS Part 1 Requirements

Requirements		Validation Methods	Findings			
			In Place	In Place w/CCW	N/A	Not in Place
Requirement P1-1. Maintain security policies for all personnel						
P1–1.1 Maintain Security Policies						
P1	**1.1.1** An organizational security policy(s) is established and disseminated to all relevant personnel.	• Examine documented policies and procedures. • Interview personnel.	☐	☐	☐	☐
	• *Identify documented policies and procedures examined:*	*<Report Findings Here>*				
	• *Identify personnel interviewed and describe results of interviews:*	*<Report Findings Here>*				
	• *Additional assessor comments:*	*<Report Findings Here>*				
P1	**1.1.2** Security policies are reviewed and updated as needed to reflect changes to business objectives or the risk environment.	• Examine documented policies and procedures. • Interview personnel.	☐	☐	☐	☐
	• *Identify documented policies and procedures examined:*	*<Report Findings Here>*				
	• *Identify personnel interviewed and describe results of interviews:*	*<Report Findings Here>*				
	• *Additional assessor comments:*	*<Report Findings Here>*				
P1	**1.1.3** Policy updates are communicated to applicable personnel.	• Examine documented policies and procedures. • Interview personnel.	☐	☐	☐	☐
	• *Identify documented policies and procedures examined:*	*<Report Findings Here>*				
	• *Identify personnel interviewed and describe results of interviews:*	*<Report Findings Here>*				
	• *Additional assessor comments:*	*<Report Findings Here>*				
P1	**1.1.4** The security policy is approved by management	• Examine documented policies and procedures. • Interview personnel.	☐	☐	☐	☐
	• *Identify documented policies and procedures examined:*	*<Report Findings Here>*				
	• *Identify personnel interviewed and describe results of interviews:*	*<Report Findings Here>*				
	• *Additional assessor comments:*	*<Report Findings Here>*				

Requirements		Validation Methods	Findings			
			In Place	In Place w/CCW	N/A	Not in Place
P1	**1.1.5** Personnel acknowledge that they have read and understood the security policy, including updates to the policy.	• Examine evidence of acknowledgments. • Interview personnel.	☐	☐	☐	☐
	• *Identify evidence of acknowledgments examined:*	*<Report Findings Here>*				
	• *Identify personnel interviewed and describe results of interviews:*	*<Report Findings Here>*				
	• *Additional assessor comments:*	*<Report Findings Here>*				
P1–1.2 Evaluate Risk						
P1	**1.2.1** A risk-assessment process is documented.	• Examine documented policies and procedures. • Interview personnel responsible for risk-assessment process.	☐	☐	☐	☐
	• *Identify documented policies and procedures examined:*	*<Report Findings Here>*				
	• *Identify personnel interviewed and describe results of interviews:*	*<Report Findings Here>*				
	• *Additional assessor comments:*	*<Report Findings Here>*				
P1	**1.2.2** The documented risk-assessment process is performed at least annually and upon significant changes.	• Examine documented policies and procedures. • Interview personnel responsible for risk-assessment process.	☐	☐	☐	☐
	• *Identify documented policies and procedures examined:*	*<Report Findings Here>*				
	• *Identify personnel interviewed and describe results of interviews:*	*<Report Findings Here>*				
	• *Additional assessor comments:*	*<Report Findings Here>*				
P1–1.3 Educate personnel						
P1	**1.3.1** A security awareness program is implemented that provides awareness to all applicable personnel about security policy and procedures.	• Examine documented policies and procedures. • Examine security awareness materials.	☐	☐	☐	☐
	• *Identify documented policies and procedures examined:*	*<Report Findings Here>*				
	• *Describe the security awareness materials examined:*	*<Report Findings Here>*				
	• *Additional assessor comments:*	*<Report Findings Here>*				

Requirements		Validation Methods	Findings			
			In Place	In Place w/CCW	N/A	Not in Place
P1	**1.3.2** Personnel receive security awareness training at defined intervals, as appropriate for their job function.	• Examine records of attendance. • Interview personnel.	☐	☐	☐	☐
	• *Identify attendance records examined:*	*<Report Findings Here>*				
	• *Identify personnel interviewed and describe results of interviews:*	*<Report Findings Here>*				
	• *Additional assessor comments:*	*<Report Findings Here>*				
P1	**1.3.3** Personnel are aware of the security policy and responsibilities as applicable to their job function.	• Interview personnel.	☐	☐	☐	☐
	• *Identify personnel interviewed and describe results of interviews:*	*<Report Findings Here>*				
	• *Additional assessor comments:*	*<Report Findings Here>*				
P1–1.4 Screen personnel						
P1	**1.4.1** Personnel are screened (background checks) prior to being granted access to the 3DE.	• Examine documented policies and procedures. • Interview personnel. • Examine results of screening process.	☐	☐	☐	☐
	• *Identify documented policies and procedures examined:*	*<Report Findings Here>*				
	• *Describe the results of the screening process examined:*	*<Report Findings Here>*				
	• *Identify personnel interviewed and describe results of interviews:*	*<Report Findings Here>*				
	• *Additional assessor comments:*	*<Report Findings Here>*				
P1	**1.4.2** The screening process includes established criteria and a decision process for background check results.	• Examine documented policies and procedures. • Interview personnel. • Examine results of screening process.	☐	☐	☐	☐
	• *Identify documented policies and procedures examined:*	*<Report Findings Here>*				
	• *Describe the results of the screening process examined:*	*<Report Findings Here>*				
	• *Identify personnel interviewed and describe results of interviews:*	*<Report Findings Here>*				
	• *Additional assessor comments:*	*<Report Findings Here>*				

Requirements		Validation Methods	Findings			
			In Place	In Place w/CCW	N/A	Not in Place
Requirement P1-2. Secure network connectivity						
P1–2.1 Protect 3DS systems from untrusted systems and networks						
P1	**2.1.1** A security policy(s) and procedures for protection of 3DS environment boundaries are maintained and implemented.	• Examine documented policies and procedures. • Interview personnel.	☐	☐	☐	☐
	• *Identify documented policies and procedures examined:*	<Report Findings Here>				
	• *Identify personnel interviewed and describe results of interviews:*	<Report Findings Here>				
	• *Additional assessor comments:*	<Report Findings Here>				
P1	**2.1.2** Up-to-date network and data flow information is maintained for all 3DS communication paths.	• Examine network and data flow information. • Observe methods used to maintain up-to-date network and data flow information.	☐	☐	☐	☐
	• *Identify network and data flow information examined:*	<Report Findings Here>				
	• *Describe methods observed that are used to maintain up-to-date network and data flow information:*	<Report Findings Here>				
	• *Additional assessor comments:*	<Report Findings Here>				
P1	**2.1.3** Access between trusted and untrusted networks, systems, and applications is limited via physical and/or logical controls.	• Examine documentation describing controls. • Observe physical and/or logical controls.	☐	☐	☐	☐
	• *Identify documentation describing controls examined:*	<Report Findings Here>				
	• *Describe physical and/or logical controls observed:*	<Report Findings Here>				
	• *Additional assessor comments:*	<Report Findings Here>				
P1	**2.1.4** Traffic to/from 3DS systems is restricted to only that which is necessary, with all other traffic specifically denied.	• Examine documentation identifying necessary traffic. • Observe configurations of ingress and egress controls.	☐	☐	☐	☐
	• *Identify documentation examined:*	<Report Findings Here>				
	• *Describe configurations examined:*	<Report Findings Here>				

Requirements		Validation Methods	Findings			
			In Place	In Place w/CCW	N/A	Not in Place
	• *Additional assessor comments:*	*<Report Findings Here>*				
P1	**2.1.5** Network connectivity controls are monitored and/or periodically reviewed to confirm configurations are effective.	• Examine documented methods for monitoring and/or periodically reviewing network connectivity controls. • Observe implemented methods and processes.	☐	☐	☐	☐
	• *Identify documented methods examined:*	*<Report Findings Here>*				
	• *Describe implemented methods and processes observed:*	*<Report Findings Here>*				
	• *Additional assessor comments:*	*<Report Findings Here>*				
P1–2.2 Protect 3DS systems from network threats						
P1	**2.2.1** Controls are implemented to detect and/or block known and unknown network attacks.	• Examine documented controls/configuration standards. • Observe implemented controls.	☐	☐	☐	☐
	• *Identify documented controls/configuration standards examined:*	*<Report Findings Here>*				
	• *Describe implemented controls observed:*	*<Report Findings Here>*				
	• *Additional assessor comments:*	*<Report Findings Here>*				
P1	**2.2.2** Suspicious traffic is blocked or generates an alert that is investigated and responded to.	• Examine documented procedures. • Observe implemented controls and processes.	☐	☐	☐	☐
	• *Identify documented procedures examined:*	*<Report Findings Here>*				
	• *Describe implemented controls and processes observed:*	*<Report Findings Here>*				
	• *Additional assessor comments:*	*<Report Findings Here>*				
Requirement P1-3. Develop and maintain secure systems						
P1–3.1 Secure application development						
P1	**3.1.1** A security policy(s) and procedures for secure management of the Software Development Lifecycle (SDLC) is maintained and implemented.	• Examine documented policies and procedures. • Interview personnel.	☐	☐	☐	☐
	• *Identify documented policies and procedures examined:*	*<Report Findings Here>*				

Requirements		Validation Methods	Findings			
			In Place	In Place w/CCW	N/A	Not in Place
	• *Identify personnel interviewed and describe results of interviews:*	<*Report Findings Here*>				
	• *Additional assessor comments:*	<*Report Findings Here*>				
P1	**3.1.2** Personnel involved in software development are trained in secure software development practices.	• Examine evidence of training. • Interview developer personnel.	☐	☐	☐	☐
	• *Identify evidence of training examined:*	<*Report Findings Here*>				
	• *Identify developer personnel interviewed and describe results of interviews:*	<*Report Findings Here*>				
	• *Additional assessor comments:*	<*Report Findings Here*>				
P1	**3.1.3** Software development procedures include processes to address common coding vulnerabilities.	• Examine documented procedures. • Interview developer personnel.	☐	☐	☐	☐
	• *Identify documented procedures examined:*	<*Report Findings Here*>				
	• *Identify developer personnel interviewed and describe results of interviews:*	<*Report Findings Here*>				
	• *Additional assessor comments:*	<*Report Findings Here*>				
P1	**3.1.4** Software security testing is conducted during the software development lifecycle using methodologies documented in the SDLC processes.	• Examine documented software security testing procedures. • Examine results of software security testing. • Interview personnel.	☐	☐	☐	☐
	• *Identify documented software security testing procedures examined:*	<*Report Findings Here*>				
	• *Describe observations and outcomes:*	<*Report Findings Here*>				
	• *Identify personnel interviewed and describe results of interviews:*	<*Report Findings Here*>				
	• *Additional assessor comments:*	<*Report Findings Here*>				
P1	**3.1.5** The software security testing process identifies defects and security vulnerabilities.	• Examine documented software security testing procedures. • Examine results of software security testing. • Interview personnel.	☐	☐	☐	☐

	Requirements	Validation Methods	Findings			
			In Place	In Place w/CCW	N/A	Not in Place
	• *Identify documented software security testing procedures examined:*	*<Report Findings Here>*				
	• *Describe observations and outcomes:*	*<Report Findings Here>*				
	• *Identify personnel interviewed and describe results of interviews:*	*<Report Findings Here>*				
	• *Additional assessor comments:*	*<Report Findings Here>*				
P1	**3.1.6** Identified software defects and security vulnerabilities are addressed prior to release.	• Examine documented software security testing procedures. • Examine results of software security testing. • Interview personnel.	☐	☐	☐	☐
	• *Identify documented software security testing procedures examined:*	*<Report Findings Here>*				
	• *Describe observations and outcomes:*	*<Report Findings Here>*				
	• *Identify personnel interviewed and describe results of interviews:*	*<Report Findings Here>*				
	• *Additional assessor comments:*	*<Report Findings Here>*				
P1	**3.1.7** Results of software security testing are signed off by management prior to software release.	• Examine documented software security testing procedures. • Examine results of software security testing. • Interview personnel.	☐	☐	☐	☐
	• *Identify documented software security testing procedures examined:*	*<Report Findings Here>*				
	• *Describe observations and outcomes:*	*<Report Findings Here>*				
	• *Identify personnel interviewed and describe results of interviews:*	*<Report Findings Here>*				
	• *Additional assessor comments:*	*<Report Findings Here>*				
P1–3.2 Configuration standards						
P1	**3.2.1** A security policy(s) and procedures for system build and configuration management are maintained and implemented.	• Examine documented policies and procedures. • Interview personnel.	☐	☐	☐	☐

	Requirements	Validation Methods	Findings			
			In Place	In Place w/CCW	N/A	Not in Place
	• *Identify documented policies and procedures examined:*	<Report Findings Here>				
	• *Identify personnel interviewed and describe results of interviews:*	<Report Findings Here>				
	• *Additional assessor comments:*	<Report Findings Here>				
P1	**3.2.2** An up-to-date inventory of all 3DS system components is maintained.	• Examine system inventory. • Interview personnel.	☐	☐	☐	☐
	• *Describe the system inventory evidence examined:*	<Report Findings Here>				
	• *Identify personnel interviewed and describe results of interviews:*	<Report Findings Here>				
	• *Additional assessor comments:*	<Report Findings Here>				
P1	**3.2.3** Configuration standards are defined and implemented for all 3DS system types.	• Examine system configuration standards and build procedures for all system component types. • Examine system configurations • Interview personnel.	☐	☐	☐	☐
	• *Identify system configuration standards and build procedures examined:*	<Report Findings Here>				
	• *Describe the system configurations examined:*	<Report Findings Here>				
	• *Identify personnel interviewed and describe results of interviews:*	<Report Findings Here>				
	• *Additional assessor comments:*	<Report Findings Here>				
P1	**3.2.4** Configuration standards address all known security vulnerabilities and are based on industry-accepted system hardening standards.	• Examine system configuration standards and build procedures for all system component types. • Examine system configurations. • Interview personnel.	☐	☐	☐	☐
	• *Identify system configuration standards and build procedures examined:*	<Report Findings Here>				
	• *Describe the system configurations examined:*	<Report Findings Here>				
	• *Identify personnel interviewed and describe results of interviews:*	<Report Findings Here>				
	• *Additional assessor comments:*	<Report Findings Here>				

Requirements		Validation Methods	Findings			
			In Place	In Place w/CCW	N/A	Not in Place
P1	**3.2.5** Configuration standards and build procedures include: • Changing all vendor-supplied default accounts and system settings. • Removing or disabling all unnecessary system or application functionality. • Preventing functions that require different security levels from co-existing on the same system component.	• Examine system configuration standards and build procedures for all system component types. • Examine system configurations. • Interview personnel.	☐	☐	☐	☐
	• *Identify system configuration standards and build procedures examined:*	*<Report Findings Here>*				
	• *Describe the system configurations examined:*	*<Report Findings Here>*				
	• *Identify personnel interviewed and describe results of interviews:*	*<Report Findings Here>*				
	• *Additional assessor comments:*	*<Report Findings Here>*				
P1–3.3 Change management						
P1	**3.3.1** Change-control procedures are defined and implemented for all changes to system components, including "emergency changes."	• Examine documented change-control procedures. • Examine records of changes and compare to system configurations. • Interview personnel.	☐	☐	☐	☐
	• *Identify documented change-control procedures examined:*	*<Report Findings Here>*				
	• *Identify records of changes examined:*	*<Report Findings Here>*				
	• *Describe observations and outcomes:*	*<Report Findings Here>*				
	• *Identify personnel interviewed and describe results of interviews:*	*<Report Findings Here>*				
	• *Additional assessor comments:*	*<Report Findings Here>*				
P1	**3.3.2** All changes are authorized and the security impact understood prior to implementing the change.	• Examine documented change-control procedures. • Examine records of changes and compare to system configurations. • Interview personnel.	☐	☐	☐	☐
	• *Identify documented change-control procedures examined:*	*<Report Findings Here>*				

	Requirements	Validation Methods	Findings			
			In Place	In Place w/CCW	N/A	Not in Place
	• *Identify records of changes examined:*	*<Report Findings Here>*				
	• *Describe observations and outcomes:*	*<Report Findings Here>*				
	• *Identify personnel interviewed and describe results of interviews:*	*<Report Findings Here>*				
	• *Additional assessor comments:*	*<Report Findings Here>*				
P1	**3.3.3** All changes are tested in a non-production environment.	• Examine documented change-control procedures. • Examine records of changes and compare to system configurations. • Interview personnel.	☐	☐	☐	☐
	• *Identify documented change-control procedures examined:*	*<Report Findings Here>*				
	• *Identify records of changes examined:*	*<Report Findings Here>*				
	• *Describe observations and outcomes:*	*<Report Findings Here>*				
	• *Identify personnel interviewed and describe results of interviews:*	*<Report Findings Here>*				
	• *Additional assessor comments:*	*<Report Findings Here>*				
P1	**3.3.4** Rollback procedures are prepared for all changes.	• Examine documented change-control procedures. • Examine records of changes and compare to system configurations. • Interview personnel.	☐	☐	☐	☐
	• *Identify documented change-control procedures examined:*	*<Report Findings Here>*				
	• *Identify records of changes examined:*	*<Report Findings Here>*				
	• *Describe observations and outcomes:*	*<Report Findings Here>*				
	• *Identify personnel interviewed and describe results of interviews:*	*<Report Findings Here>*				
	• *Additional assessor comments:*	*<Report Findings Here>*				
P1	**3.3.5** Unauthorized changes to system or application configurations are prevented and/or detected and addressed.	• Examine documentation of controls and/or processes. • Observe implemented controls. • Interview personnel.	☐	☐	☐	☐

Requirements		Validation Methods	Findings			
			In Place	In Place w/CCW	N/A	Not in Place
	• *Identify documented controls and/or processes examined:*	<Report Findings Here>				
	• *Describe observations and outcomes:*	<Report Findings Here>				
	• *Identify personnel interviewed and describe results of interviews:*	<Report Findings Here>				
	• *Additional assessor comments:*	<Report Findings Here>				
Requirement P1.4. Vulnerability management						
P1–4.1 Protect against malicious software						
P1	**4.1.1** A security policy(s) and procedures for protecting systems against malware are maintained and implemented.	• Examine documented policies and procedures. • Interview personnel.	☐	☐	☐	☐
	• *Identify documented policies and procedures examined:*	<Report Findings Here>				
	• *Identify personnel interviewed and describe results of interviews:*	<Report Findings Here>				
	• *Additional assessor comments:*	<Report Findings Here>				
P1	**4.1.2** Controls to prevent and/or detect and remove malicious software are implemented, active, and maintained.	• Examine documented controls/configurations. • Observe implemented controls and processes. • Examine evidence of malware prevention and/or detection and removal. • Interview personnel.	☐	☐	☐	☐
	• *Identify documented controls/configurations examined:*	<Report Findings Here>				
	• *Describe the evidence examined:*	<Report Findings Here>				
	• *Describe observations and outcomes:*	<Report Findings Here>				
	• *Identify personnel interviewed and describe results of interviews:*	<Report Findings Here>				
	• *Additional assessor comments:*	<Report Findings Here>				

Requirements		Validation Methods	Findings			
			In Place	In Place w/CCW	N/A	Not in Place
P1–4.2 Address vulnerabilities and security weaknesses						
P1	**4.2.1** A security policy(s) and procedures for identifying, ranking, and protecting against vulnerabilities are maintained and implemented.	• Examine documented policies and procedures. • Interview responsible personnel.	☐	☐	☐	☐
	• *Identify documented policies and procedures examined:*	<*Report Findings Here*>				
	• *Identify personnel interviewed and describe results of interviews:*	<*Report Findings Here*>				
	• *Additional assessor comments:*	<*Report Findings Here*>				
P1	**4.2.2** Vulnerability scans, both internal and external, are performed at least quarterly to identify and address vulnerabilities.	• Examine vulnerability scanning reports. • Interview personnel.	☐	☐	☐	☐
	• *Identify vulnerability scanning reports examined:*	<*Report Findings Here*>				
	• *Identify personnel interviewed and describe results of interviews:*	<*Report Findings Here*>				
	• *Additional assessor comments:*	<*Report Findings Here*>				
P1	**4.2.3** Vulnerability scans are performed by qualified personnel: • External scans are performed by a PCI SSC Approved Scanning Vendor (ASV). • Internal scans are performed by qualified personnel.	• Examine vulnerability scanning reports. • Interview personnel.	☐	☐	☐	☐
	• *Identify vulnerability scanning reports examined:*	<*Report Findings Here*>				
	• *Identify personnel interviewed and describe results of interviews:*	<*Report Findings Here*>				
	• *Additional assessor comments:*	<*Report Findings Here*>				
P1	**4.2.4** Identified vulnerabilities are ranked to determine the criticality of the vulnerability.	• Examine documented procedures for ranking vulnerabilities. • Interview personnel.	☐	☐	☐	☐
	• *Identify documented procedures for ranking vulnerabilities examined:*	<*Report Findings Here*>				
	• *Identify personnel interviewed and describe results of interviews:*	<*Report Findings Here*>				
	• *Additional assessor comments:*	<*Report Findings Here*>				
P1	**4.2.5** Penetration tests are performed at least annually.	• Examine penetration test reports. • Interview personnel.	☐	☐	☐	☐

Requirements		Validation Methods	Findings			
			In Place	In Place w/CCW	N/A	Not in Place
	• *Identify penetration test reports examined:*	<Report Findings Here>				
	• *Identify personnel interviewed and describe results of interviews:*	<Report Findings Here>				
	• *Additional assessor comments:*	<Report Findings Here>				
P1	**4.2.6** Penetration tests are performed by qualified personnel.	• Examine penetration test reports. • Interview personnel.	☐	☐	☐	☐
	• *Identify penetration test reports examined:*	<Report Findings Here>				
	• *Identify personnel interviewed and describe results of interviews:*	<Report Findings Here>				
	• *Notes and additional considerations:*	<Report Findings Here>				
P1	**4.2.7** Vulnerabilities and penetration testing findings considered as high risk are addressed within one month. All other vulnerabilities and identified security issues are addressed in a timely manner.	• Examine results of penetration tests and vulnerability scanning reports. • Examine evidence of remediation to address vulnerabilities and security issues. • Interview personnel.	☐	☐	☐	☐
	• *Identify penetration test reports and vulnerability scanning reports examined:*	<Report Findings Here>				
	• *Describe the evidence of remediation examined:*	<Report Findings Here>				
	• *Identify personnel interviewed and describe results of interviews:*	<Report Findings Here>				
	• *Additional assessor comments:*	<Report Findings Here>				
Requirement P1-5. Manage access						
P1–5.1 Access management						
P1	**5.1.1** A security policy(s) and procedures for assigning access are maintained and implemented.	• Examine documented policies and procedures. • Interview personnel.	☐	☐	☐	☐
	• *Identify documented policies and procedures examined:*	<Report Findings Here>				
	• *Identify personnel interviewed and describe results of interviews:*	<Report Findings Here>				
	• *Additional assessor comments:*	<Report Findings Here>				

Requirements		Validation Methods	Findings			
			In Place	In Place w/CCW	N/A	Not in Place
P1	**5.1.2** Roles and responsibilities are defined for groups and accounts with access to 3DS systems.	• Examine defined roles and responsibilities. • Interview personnel.	☐	☐	☐	☐
	• *Describe the evidence examined:*	*<Report Findings Here>*				
	• *Identify personnel interviewed and describe results of interviews:*	*<Report Findings Here>*				
	• *Additional assessor comments:*	*<Report Findings Here>*				
P1	**5.1.3** Least privileges are assigned based on individual job function and periodically reviewed.	• Observe assigned access privileges. • Examine evidence that access privileges are periodically reviewed. • Interview personnel.	☐	☐	☐	☐
	• *Describe the assigned access privileges examined:*	*<Report Findings Here>*				
	• *Describe the evidence examined:*	*<Report Findings Here>*				
	• *Identify personnel interviewed and describe results of interviews:*	*<Report Findings Here>*				
	• *Additional assessor comments:*	*<Report Findings Here>*				
P1–5.2 Account management						
P1	**5.2.1** A security policy(s) and procedures for managing accounts are maintained and implemented.	• Examine documented policies and procedures. • Interview personnel.	☐	☐	☐	☐
	• *Identify documented policies and procedures examined:*	*<Report Findings Here>*				
	• *Identify personnel interviewed and describe results of interviews:*	*<Report Findings Here>*				
	• *Additional assessor comments:*	*<Report Findings Here>*				
P1	**5.2.2** Individuals are assigned a unique account ID.	• Examine documented procedures. • Observe account settings.	☐	☐	☐	☐
	• *Identify documented procedures examined:*	*<Report Findings Here>*				
	• *Describe observations and outcomes:*	*<Report Findings Here>*				
	• *Additional assessor comments:*	*<Report Findings Here>*				

Requirements		Validation Methods	Findings			
			In Place	In Place w/CCW	N/A	Not in Place
P1	**5.2.3** Controls are implemented to protect the confidentiality and integrity of accounts and credentials.	• Examine documented procedures. • Observe implemented controls.	☐	☐	☐	☐
	• *Identify documented procedures examined:*	*<Report Findings Here>*				
	• *Describe observations and outcomes:*	*<Report Findings Here>*				
	• *Additional assessor comments:*	*<Report Findings Here>*				
P1	**5.2.4** Controls are implemented to prevent misuse of accounts.	• Examine documented procedures. • Observe implemented controls.	☐	☐	☐	☐
	• *Identify documented procedures examined:*	*<Report Findings Here>*				
	• *Describe observations and outcomes:*	*<Report Findings Here>*				
	• *Additional assessor comments:*	*<Report Findings Here>*				
P1	**5.2.5** Access for third parties is identified, controlled, and monitored.	• Examine documented procedures. • Observe implemented controls.	☐	☐	☐	☐
	• *Identify documented procedures examined:*	*<Report Findings Here>*				
	• *Describe observations and outcomes:*	*<Report Findings Here>*				
	• *Additional assessor comments:*	.				
P1– 5.3 Authentication						
P1	**5.3.1** All access to 3DS systems requires strong authentication prior to access being granted.	• Examine documented procedures. • Observe implemented controls.	☐	☐	☐	☐
	• *Identify documented procedures examined:*	*<Report Findings Here>*				
	• *Describe observations and outcomes:*	*<Report Findings Here>*				
	• *Additional assessor comments:*	*<Report Findings Here>*				
Requirement P1-6. Physical Security						
P1–6.1 Restrict physical access						
P1	**6.1.1** A security policy(s) and procedures for securing physical access to 3DS systems is maintained and implemented.	• Examine documented policies and procedures. • Interview personnel.	☐	☐	☐	☐

Requirements		Validation Methods	Findings			
			In Place	In Place w/CCW	N/A	Not in Place
	• *Identify documented policies and procedures examined:*	*<Report Findings Here>*				
	• *Identify personnel interviewed and describe results of interviews:*	*<Report Findings Here>*				
	• *Additional assessor comments:*	*<Report Findings Here>*				
P1	**6.1.2** Facility entry controls are in place to limit and monitor physical access to systems in the 3DE.	• Observe physical access controls.	☐	☐	☐	☐
	• *Describe observations and outcomes:*	*<Report Findings Here>*				
	• *Additional assessor comments:*	*<Report Findings Here>*				
P1	**6.1.3** Physical access for personnel to 3DE is authorized and based on individual job function.	• Examine assigned access permissions. • Interview personnel. • Observe personnel access procedures.	☐	☐	☐	☐
	• *Identify assigned access permissions evidence examined:*	*<Report Findings Here>*				
	• *Describe observations and outcomes:*	*<Report Findings Here>*				
	• *Identify personnel interviewed and describe results of interviews:*	*<Report Findings Here>*				
	• *Additional assessor comments:*	*<Report Findings Here>*				
P1	**6.1.4** Personnel access is revoked immediately upon termination, and all physical access mechanisms, such as keys, access cards, etc., are returned or disabled.	• Examine documented procedures. • Examine evidence of access revocation and return of physical access mechanisms. • Interview personnel.	☐	☐	☐	☐
	• *Identify documented procedures examined:*	*<Report Findings Here>*				
	• *Describe the evidence examined:*	*<Report Findings Here>*				
	• *Identify personnel interviewed and describe results of interviews:*	*<Report Findings Here>*				
	• *Additional assessor comments:*	*<Report Findings Here>*				
P1–6.2 Secure media						
P1	**6.2.1** Strict control is maintained over the storage and accessibility of media.	• Observe implemented controls. • Interview personnel.	☐	☐	☐	☐
	• *Describe observations and outcomes:*	*<Report Findings Here>*				

Requirements		Validation Methods	Findings			
			In Place	In Place w/CCW	N/A	Not in Place
	• *Identify personnel interviewed and describe results of interviews:*	*<Report Findings Here>*				
	• *Additional assessor comments:*	*<Report Findings Here>*				
Requirement P1-7. Incident response preparedness						
P1–7.1 Incident response plan						
P1	**7.1.1** A security policy(s) and procedures for managing and responding to security incidents is maintained and implemented.	• Examine documented policies and procedures. • Interview personnel.	☐	☐	☐	☐
	• *Identify documented policies and procedures examined:*	*<Report Findings Here>*				
	• *Identify personnel interviewed and describe results of interviews:*	*<Report Findings Here>*				
	• *Additional assessor comments:*	*<Report Findings Here>*				
P1	**7.1.2** An incident response plan is in place that includes: • Roles and responsibilities • Communication and contact strategies • Specific incident response procedures • Business recovery and continuity procedures • Data back-up processes • Analysis of legal requirements for reporting compromises • Coverage and responses of all critical system components • Consideration of payment brands' response requirements	• Examine documented incident response plans and procedures. • Interview personnel.	☐	☐	☐	☐
	• *Identify documented incident response plans and procedures examined:*	*<Report Findings Here>*				
	• *Identify personnel interviewed and describe results of interviews:*	*<Report Findings Here>*				
	• *Additional assessor comments:*	*<Report Findings Here>*				
P1	**7.1.3** The plan is reviewed and tested at least annually.	• Examine documented procedures. • Examine evidence of reviews and testing. • Interview personnel.	☐	☐	☐	☐
	• *Identify documented procedures examined:*	*<Report Findings Here>*				
	• *Describe the evidence of reviews and testing examined:*	*<Report Findings Here>*				

Requirements		Validation Methods	Findings			
			In Place	In Place w/CCW	N/A	Not in Place
	• *Identify personnel interviewed and describe results of interviews:*	*<Report Findings Here>*				
	• *Additional assessor comments:*	*<Report Findings Here>*				
P1–7.2 Audit logs						
P1	**7.2.1** A security policy(s) and procedures for generating and managing audit logs is maintained and implemented.	• Examine documented policies and procedures. • Interview personnel.	☐	☐	☐	☐
	• *Identify documented policies and procedures examined:*	*<Report Findings Here>*				
	• *Identify personnel interviewed and describe results of interviews:*	*<Report Findings Here>*				
	• *Additional assessor comments:*	*<Report Findings Here>*				
P1	**7.2.2** Audit logs are implemented to: • Link all access to 3DS systems to an individual user. • Record security events.	• Examine system configurations. • Observe access attempts. • Examine audit log files.	☐	☐	☐	☐
	• *Identify system configurations examined:*	*<Report Findings Here>*				
	• *Describe observations and outcomes:*	*<Report Findings Here>*				
	• *Describe the audit log files examined:*	*<Report Findings Here>*				
	• *Additional assessor comments:*	*<Report Findings Here>*				
P1	**7.2.3** Time synchronization is implemented on 3DS systems to ensure system clocks are synchronized and have the correct and consistent time.	• Examine system configurations.	☐	☐	☐	☐
	• *Identify system configurations examined:*	*<Report Findings Here>*				
	• *Additional assessor comments:*	*<Report Findings Here>*				
P1	**7.2.4** Logs and security events are monitored and/or periodically reviewed for all 3DS systems to identify anomalies or suspicious activity.	• Examine evidence of reviews of logs and security events. • Interview personnel.	☐	☐	☐	☐
	• *Identify evidence of reviews of logs examined:*	*<Report Findings Here>*				
	• *Describe the security events examined:*	*<Report Findings Here>*				
	• *Identify personnel interviewed and describe results of interviews:*	*<Report Findings Here>*				

Requirements		Validation Methods	Findings			
			In Place	In Place w/CCW	N/A	Not in Place
	• *Additional assessor comments:*	*<Report Findings Here>*				
P1	**7.2.5** Audit Logs are secured so they cannot be altered.	• Examine controls/configurations. • Observe attempts to modify audit logs.	☐	☐	☐	☐
	• *Identify controls/configurations examined:*	*<Report Findings Here>*				
	• *Describe observations and outcomes:*	*<Report Findings Here>*				
	• *Additional assessor comments:*	*<Report Findings Here>*				
P1	**7.2.6** Audit and monitoring logs are retained for least one year, with a minimum of three months immediately available for analysis.	• Examine audit log files. • Interview personnel.	☐	☐	☐	☐
	• *Identify audit log files examined:*	*<Report Findings Here>*				
	• *Identify personnel interviewed and describe results of interviews:*	*<Report Findings Here>*				
	• *Additional assessor comments:*	*<Report Findings Here>*				

4.2 PCI 3DS Part 2: 3DS Security Requirements

4.2.1 Summary of Findings for PCI 3DS Part 2 Requirements

Identify the appropriate assessment result for each high-level PCI 3DS requirement. The information provided here must be supported by the detailed Findings and Observations (Section 4.2.2).

When determining the appropriate finding for each high-level requirement, the following principles apply:

1. If the finding for any requirement or sub-requirement is “Not in Place,” select “Not in Place” for the high-level requirement.
2. If the finding for any requirement or sub-requirement is “N/A” and all other requirements are “In Place,” select “In Place” for the high-level requirement.
3. If the finding for any requirement or sub-requirement is “In Place w/CCW” and all other requirements are “In Place,” select “In Place w/CCW” for the high-level requirement.
4. If the findings include one or more requirements or sub-requirements as “N/A,” and one or more as “In Place w/CCW,” and all other requirements are “In Place,” select “In Place w/CCW” for the high-level requirement.
5. If all requirements and sub-requirements are identified as “In Place,” select “In Place” for the high-level requirement.

PCI 3DS Part 2: Summary of Assessment Findings

		In Place	*In Place w/CCW*	*N/A*	*Not in Place*
Part 2: 3DS Security Requirements					
P2-1	Validate scope	☐	☐	☐	☐
P2-2	Security governance	☐	☐	☐	☐
P2-3	Protect 3DS systems and applications	☐	☐	☐	☐
P2-4	Secure logical access to 3DS systems	☐	☐	☐	☐
P2-5	Protect 3DS data	☐	☐	☐	☐
P2-6	Cryptography and key management	☐	☐	☐	☐
P2-7	Physically secure 3DS systems	☐	☐	☐	☐

4.2.2 Detailed Findings and Observations for PCI 3DS Part 2 Requirements

Requirements		Validation Methods	Findings			
			In Place	In Place w/CCW	N/A	Not in Place
Requirement P2-1. Validate scope						
P2–1.1 Scoping						
P2	**1.1.1** All networks and system components in-scope for these PCI 3DS security requirements are identified.	• Examine documented results of scope reviews. • Interview personnel.	☐	☐	☐	☐
	• *Identify documented results of scope reviews examined:*	*<Report Findings Here>*				
	• *Identify personnel interviewed and describe results of interviews:*	*<Report Findings Here>*				
	• *Additional assessor comments:*	*<Report Findings Here>*				
P2	**1.1.2** All out-of-scope networks are identified with justification for being out of scope and descriptions of segmentation controls implemented.	• Examine documented results of scope reviews. • Examine data flow and network diagrams. • Observe segmentation controls.	☐	☐	☐	☐
	• *Identify documented results of scope reviews examined:*	*<Report Findings Here>*				
	• *Identify the data flow and network diagrams examined:*	*<Report Findings Here>*				
	• *Describe observations and outcomes:*	*<Report Findings Here>*				
	• *Additional assessor comments:*	*<Report Findings Here>*				
P2	**1.1.3** All connected entities with access to the 3DS environments are identified.	• Examine documentation. • Interview personnel.	☐	☐	☐	☐
	• *Identify documentation examined:*	*<Report Findings Here>*				
	• *Identify personnel interviewed and describe results of interviews:*	*<Report Findings Here>*				
	• *Additional assessor comments:*	*<Report Findings Here>*				
Requirement P2-2. Security governance						
P2–2.1 Security governance						
P2	**2.1.1** Security objectives are aligned with business objectives.	• Examine documentation. • Interview personnel.	☐	☐	☐	☐

	Requirements	Validation Methods	Findings			
			In Place	In Place w/CCW	N/A	Not in Place
	• *Identify documentation examined:*	*<Report Findings Here>*				
	• *Identify personnel interviewed and describe results of interviews:*	*<Report Findings Here>*				
	• *Additional assessor comments:*	*<Report Findings Here>*				
P2	**2.1.2** Responsibilities and accountability for meeting security objectives are formally assigned, including responsibilities for the security of 3DS processes.	• Examine documentation. • Interview personnel.	☐	☐	☐	☐
	• *Identify documentation examined:*	*<Report Findings Here>*				
	• *Identify personnel interviewed and describe results of interviews:*	*<Report Findings Here>*				
	• *Additional assessor comments:*	*<Report Findings Here>*				
P2	**2.1.3** Responsibility for identifying and addressing evolving risks is assigned.	• Examine documentation. • Interview personnel.	☐	☐	☐	☐
	• *Identify documentation examined:*	*<Report Findings Here>*				
	• *Identify personnel interviewed and describe results of interviews:*	*<Report Findings Here>*				
	• *Additional assessor comments:*	*<Report Findings Here>*				
P2–2.2 Manage Risk						
P2	**2.2.1** A formal risk-management strategy is defined.	• Examine documentation. • Interview personnel.	☐	☐	☐	☐
	• *Identify documentation examined:*	*<Report Findings Here>*				
	• *Identify personnel interviewed and describe results of interviews:*	*<Report Findings Here>*				
	• *Additional assessor comments:*	*<Report Findings Here>*				
P2	**2.2.2** The risk-management strategy is approved by authorized personnel and updated as needed to address changing risk environment.	• Examine documentation. • Interview personnel.	☐	☐	☐	☐
	• *Identify documentation examined:*	*<Report Findings Here>*				
	• *Identify personnel interviewed and describe results of interviews:*	*<Report Findings Here>*				
	• *Additional assessor comments:*	*<Report Findings Here>*				

Requirements		Validation Methods	Findings			
			In Place	In Place w/CCW	N/A	Not in Place
P2–2.3 Business as usual (BAU)						
P2	**2.3.1** Review and/or monitoring is performed periodically to confirm personnel are following security policies and procedures.	• Examine evidence of reviews and/or ongoing monitoring. • Interview personnel.	☐	☐	☐	☐
	• *Describe the evidence of reviews and/or ongoing monitoring examined:*	*<Report Findings Here>*				
	• *Identify personnel interviewed and describe results of interviews:*	*<Report Findings Here>*				
	• *Additional assessor comments:*	*<Report Findings Here>*				
P2	**2.3.2** Processes to detect and respond to security control failures are defined and implemented	• Examine documented processes. • Observe implemented processes. • Interview personnel.	☐	☐	☐	☐
	• *Identify documented processes examined:*	*<Report Findings Here>*				
	• *Describe observations and outcomes:*	*<Report Findings Here>*				
	• *Identify personnel interviewed and describe results of interviews:*	*<Report Findings Here>*				
	• *Additional assessor comments:*	*<Report Findings Here>*				
P2–2.4 Manage third-party relationships						
P2	**2.4.1** Policies and procedures for managing third-party relationships are maintained and implemented.	• Examine documented policies/procedures. • Interview personnel.	☐	☐	☐	☐
	• *Identify documented policies and procedures examined:*	*<Report Findings Here>*				
	• *Identify personnel interviewed and describe results of interviews:*	*<Report Findings Here>*				
	• *Additional assessor comments:*	*<Report Findings Here>*				
P2	**2.4.2** Due diligence is performed prior to any engagement with a third party.	• Examine documented procedures. • Examine results of due diligence efforts. • Interview personnel.	☐	☐	☐	☐
	• *Identify documented procedures examined:*	*<Report Findings Here>*				
	• *Describe the results of due diligence efforts examined:*	*<Report Findings Here>*				

Requirements		Validation Methods	Findings			
			In Place	In Place w/CCW	N/A	Not in Place
	• *Identify personnel interviewed and describe results of interviews:*	<Report Findings Here>				
	• *Additional assessor comments:*	<Report Findings Here>				
P2	**2.4.3** Security responsibilities are clearly defined for each third-party engagement.	• Examine documentation. • Interview personnel.	☐	☐	☐	☐
	• *Identify documentation examined:*	<Report Findings Here>				
	• *Identify personnel interviewed and describe results of interviews:*	<Report Findings Here>				
	• *Additional assessor comments:*	<Report Findings Here>				
P2	**2.4.4** The 3DS entity periodically verifies that the agreed-upon responsibilities are being met.	• Examine results of periodic verification. • Interview personnel.	☐	☐	☐	☐
	• *Describe the results of periodic verification examined:*	<Report Findings Here>				
	• *Identify personnel interviewed and describe results of interviews:*	<Report Findings Here>				
	• *Additional assessor comments:*	<Report Findings Here>				
P2	**2.4.5** Written agreements are maintained.	• Examine documentation. • Interview personnel.	☐	☐	☐	☐
	• *Identify documentation examined:*	<Report Findings Here>				
	• *Identify personnel interviewed and describe results of interviews:*	<Report Findings Here>				
	• *Additional assessor comments:*	<Report Findings Here>				
Requirement P2-3. Protect 3DS systems and applications						
P2–3.1 Protect boundaries						
P2	**3.1.1** Traffic to and from ACS and DS is restricted to only that which is relevant to the 3DS functions.	• Examine log files. • Observe implemented controls.	☐	☐	☐	☐
	• *Identify log files examined:*	<Report Findings Here>				
	• *Describe observations and outcomes:*	<Report Findings Here>				
	• *Additional assessor comments:*	<Report Findings Here>				

Requirements		Validation Methods	Findings			
			In Place	In Place w/CCW	N/A	Not in Place
P2	**3.1.2** Traffic to and from ACS and DS is permitted only via approved interfaces.	• Examine log files. • Observe implemented controls.	☐	☐	☐	☐
	• *Identify log files examined:*	<*Report Findings Here*>				
	• *Describe observations and outcomes:*	<*Report Findings Here*>				
	• *Additional assessor comments:*	<*Report Findings Here*>				
P2–3.2 Protect baseline configurations						
P2	**3.2.1** Controls are implemented to protect the confidentiality and integrity of system configurations and documentation that support security settings.	• Examine log files. • Observe implemented controls.	☐	☐	☐	☐
	• *Identify log files examined:*	<*Report Findings Here*>				
	• *Describe observations and outcomes:*	<*Report Findings Here*>				
	• *Additional assessor comments:*	<*Report Findings Here*>				
P2–3.3 Protect applications and application interfaces						
P2	**3.3.1** Applications and programs are protected from unauthorized changes once in a production state.	• Examine log files. • Observe implemented controls.				
	• *Identify log files examined:*	<*Report Findings Here*>				
	• *Describe observations and outcomes:*	<*Report Findings Here*>				
	• *Additional assessor comments:*	<*Report Findings Here*>				
P2	**3.3.2** The mechanisms to protect applications and programs from unauthorized changes are monitored and maintained to confirm effectiveness.	• Observe implemented controls for monitoring and maintaining protection mechanisms. • Interview personnel.	☐	☐	☐	☐
	• *Describe observations and outcomes:*	<*Report Findings Here*>				
	• *Identify personnel interviewed and describe results of interviews:*	<*Report Findings Here*>				
	• *Additional assessor comments:*	<*Report Findings Here*>				

Requirements		Validation Methods	Findings			
			In Place	In Place w/CCW	N/A	Not in Place
P2	**3.3.3** All APIs that interface with the 3DS environment are identified, defined, and tested to verify they perform as expected.	• Examine network and data-flow diagrams. • Observe implemented controls. • Examine results of testing. • Interview personnel.	☐	☐	☐	☐
	• *Identify network and data-flow diagrams examined:*	*<Report Findings Here>*				
	• *Describe observations and outcomes:*	*<Report Findings Here>*				
	• *Describe results of testing examined:*	*<Report Findings Here>*				
	• *Identify personnel interviewed and describe results of interviews:*	*<Report Findings Here>*				
	• *Additional assessor comments:*	*<Report Findings Here>*				
P2	**3.3.4** Controls are implemented to protect APIs exposed to untrusted networks.	• Examine network and data-flow diagrams • Observe implemented controls. • Examine results of testing • Interview personnel.	☐	☐	☐	☐
	• *Identify network and data-flow diagrams examined:*	*<Report Findings Here>*				
	• *Describe observations and outcomes:*	*<Report Findings Here>*				
	• *Describe results of testing examined:*	*<Report Findings Here>*				
	• *Identify personnel interviewed and describe results of interviews:*	*<Report Findings Here>*				
	• *Additional assessor comments:*	*<Report Findings Here>*				
P2–3.4 Secure web configurations						
P2	**3.4.1** Only those HTTP request methods required for system operation are accepted. All unused methods are explicitly blocked.	• Examine log files. • Observe implemented controls. • Interview personnel	☐	☐	☐	☐
	• *Identify log files examined:*	*<Report Findings Here>*				
	• *Describe observations and outcomes:*	*<Report Findings Here>*				
	• *Identify personnel interviewed and describe results of interviews:*	*<Report Findings Here>*				

	Requirements	Validation Methods	Findings			
			In Place	In Place w/CCW	N/A	Not in Place
	• *Additional assessor comments:*	*<Report Findings Here>*				
P2	**3.4.2** The use of HTTPS is enforced across all application pages/resources and all communications are prevented from being sent over insecure channels (e.g., HTTP).	• Examine log files. • Observe implemented controls. • Interview personnel.	☐	☐	☐	☐
	• *Identify log files examined:*	*<Report Findings Here>*				
	• *Describe observations and outcomes:*	*<Report Findings Here>*				
	• *Identify personnel interviewed and describe results of interviews:*	*<Report Findings Here>*				
	• *Additional assessor comments:*	*<Report Findings Here>*				
P2	**3.4.3** Applications (or the underlying systems) are configured to reject content provided by external sources by default. Exceptions are explicitly authorized	• Examine documented controls. • Observe implemented controls. • Interview personnel.	☐	☐	☐	☐
	• *Identify documented controls examined:*	*<Report Findings Here>*				
	• *Describe observations and outcomes:*	*<Report Findings Here>*				
	• *Identify personnel interviewed and describe results of interviews:*	*<Report Findings Here>*				
	• *Additional assessor comments:*	*<Report Findings Here>*				
P2	**3.4.4** Applications are configured to prevent content from being embedded into untrusted third-party sites/applications. Exceptions are explicitly authorized.	• Examine documented controls. • Observe implemented controls. • Interview personnel.	☐	☐	☐	☐
	• *Identify documented controls examined:*	*<Report Findings Here>*				
	• *Describe observations and outcomes:*	*<Report Findings Here>*				
	• *Identify personnel interviewed and describe results of interviews:*	*<Report Findings Here>*				
	• *Additional assessor comments:*	*<Report Findings Here>*				
P2	**3.4.5** Security features native to the development framework and/or application platform are enabled (where feasible) to protect against common client-side attacks (such as XSS, Injection, etc.)	• Examine documented controls. • Observe implemented controls. • Interview personnel.	☐	☐	☐	☐
	• *Identify documented controls examined:*	*<Report Findings Here>*				

Requirements		Validation Methods	Findings			
			In Place	In Place w/CCW	N/A	Not in Place
	• *Describe observations and outcomes:*	<Report Findings Here>				
	• *Identify personnel interviewed and describe results of interviews:*	<Report Findings Here>				
	• *Additional assessor comments:*	<Report Findings Here>				
P2–3.5 Maintain availability of 3DS operations						
P2	**3.5.1** Availability mechanisms are implemented to protect against loss of processing capability within the 3DS infrastructure.	• Examine documented controls. • Observe implemented controls.	☐	☐	☐	☐
	• *Identify documented controls examined:*	<Report Findings Here>				
	• *Describe observations and outcomes:*	<Report Findings Here>				
	• *Additional assessor comments:*	<Report Findings Here>				
P2	**3.5.2** The availability mechanisms implemented are monitored and maintained to confirm effectiveness.	• Observe implemented controls for monitoring and maintaining the availability mechanisms. • Interview personnel.	☐	☐	☐	☐
	• *Identify controls for monitoring and maintaining availability mechanisms examined:*	<Report Findings Here>				
	• *Describe observations and outcomes:*	<Report Findings Here>				
	• *Identify personnel interviewed and describe results of interviews:*	<Report Findings Here>				
	• *Additional assessor comments:*	<Report Findings Here>				
Requirement P2-4. Secure access to 3DS systems						
P2–4.1 Secure connections for issuer and merchant customers						
P2	**4.1.1** Access by issuer and merchant users to their assigned issuer and merchant interfaces—for example, via API or web portal—for purposes of managing only their own account, is restricted to authorized personnel and requires a unique user ID with strong password and another form of strong authentication.	• Examine documented procedures. • Observe implemented controls.	☐	☐	☐	☐
	• *Identify documented procedures examined:*	<Report Findings Here>				
	• *Describe observations and outcomes:*	<Report Findings Here>				
	• *Additional assessor comments:*	<Report Findings Here>				

Requirements		Validation Methods	Findings			
			In Place	In Place w/CCW	N/A	Not in Place
P2-4.2 Secure internal network connections						
P2	**4.2.1** Multi-factor authentication is required for all personnel with non-console access to ACS, DS and 3DSS.	• Examine documented procedures. • Observe implemented controls.	☐	☐	☐	☐
	• *Identify documented procedures examined:*	*<Report Findings Here>*				
	• *Describe observations and outcomes:*	*<Report Findings Here>*				
	• *Additional assessor comments:*	*<Report Findings Here>*				
P2–4.3 Secure remote access						
P2	**4.3.1** Multi-factor authentication is required for all remote access originating from outside the entity's network that provides access into the 3DE.	• Examine documented procedures. • Observe implemented controls.	☐	☐	☐	☐
	• *Identify documented procedures examined:*	*<Report Findings Here>*				
	• *Describe observations and outcomes:*	*<Report Findings Here>*				
	• *Additional assessor comments:*	*<Report Findings Here>*				
P2	**4.3.2** Remote access to the 3DE is controlled and documented, including: • System components for which remote access is permitted • The location(s) from which remote access is permitted • The conditions under which remote access is acceptable • Individuals with remote access permission • The access privileges applicable to each authorized use	• Examine policies and procedures. • Observe remote access controls. • Interview personnel.	☐	☐	☐	☐
	• *Identify documented policies and procedures examined:*	*<Report Findings Here>*				
	• *Describe observations and outcomes:*	*<Report Findings Here>*				
	• *Identify personnel interviewed and describe results of interviews:*	*<Report Findings Here>*				
	• *Additional assessor comments:*	*<Report Findings Here>*				

Requirements		Validation Methods	Findings			
			In Place	In Place w/CCW	N/A	Not in Place
P2	**4.3.3** Where remote access using personally owned devices is permitted, strict requirements for their use are defined and implemented to include: • Device security controls are implemented and maintained as equivalent to corporate-owned devices. • Each device is explicitly approved by management.	• Examine policies and procedures. • Observe remote access controls. • Interview personnel.	☐	☐	☐	☐
	• *Identify documented policies and procedures examined:*	*<Report Findings Here>*				
	• *Describe observations and outcomes:*	*<Report Findings Here>*				
	• *Identify personnel interviewed and describe results of interviews:*	*<Report Findings Here>*				
	• *Additional assessor comments:*	*<Report Findings Here>*				
P2	**4.3.4** Remote access privileges are monitored and/or reviewed at least quarterly by an authorized individual to confirm access is still required.	• Examine documented processes. • Examine evidence of monitoring and/or reviews. • Interview personnel.	☐	☐	☐	☐
	• *Identify documented processes examined:*	*<Report Findings Here>*				
	• *Describe the evidence of monitoring and/or reviews examined:*	*<Report Findings Here>*				
	• *Describe observations and outcomes:*	*<Report Findings Here>*				
	• *Identify personnel interviewed and describe results of interviews:*	*<Report Findings Here>*				
	• *Additional assessor comments:*	*<Report Findings Here>*				
P2–4.4 Restrict Wireless Exposure						
P2	**4.4.1** 3DS components (ACS, DS, 3DSS) do not use or connect to any wireless network.	• Examine network diagrams. • Observe implemented controls. • Interview personnel.	☐	☐	☐	☐
	• *Identify network diagrams examined:*	*<Report Findings Here>*				
	• *Describe observations and outcomes:*	*<Report Findings Here>*				
	• *Identify personnel interviewed and describe results of interviews:*	*<Report Findings Here>*				
	• *Additional assessor comments:*	*<Report Findings Here>*				

Requirements		Validation Methods	Findings			
			In Place	In Place w/CCW	N/A	Not in Place
P2–4.5 Secure VPNs						
P2	**4.5.1** All VPNs that provide access to 3DE are properly configured to provide strong security communications and protect against eavesdropping, replay attacks, and man-in-the-middle attacks.	• Examine configuration standards. • Observe VPN controls. • Interview personnel.	☐	☐	☐	☐
	• *Identify configuration standards examined:*	*<Report Findings Here>*				
	• *Describe observations and outcomes:*	*<Report Findings Here>*				
	• *Identify personnel interviewed and describe results of interviews:*	*<Report Findings Here>*				
	• *Additional assessor comments:*	*<Report Findings Here>*				
Requirement P2-5. Protect 3DS data						
P2–5.1 Data lifecycle						
P2	**5.1.1** Policies and procedures for usage, flow, retention, and disposal of 3DS data are maintained and implemented.	• Examine documented policies. • Examine evidence of data usage, flow, retention and disposal. • Interview personnel.	☐	☐	☐	☐
	• *Identify documented policies examined:*	*<Report Findings Here>*				
	• *Describe the evidence of data usage, flow, retention, and disposal examined:*	*<Report Findings Here>*				
	• *Describe observations and outcomes:*	*<Report Findings Here>*				
	• *Identify personnel interviewed and describe results of interviews:*	*<Report Findings Here>*				
	• *Additional assessor comments:*	*<Report Findings Here>*				
P2	**5.1.2** 3DS data is retained only as necessary and securely purged when no longer needed.	• Examine data retention schedule and data disposal process. • Interview personnel. • Observe data storage.	☐	☐	☐	☐
	• *Describe the data retention schedule and data disposal process examined:*	*<Report Findings Here>*				
	• *Describe data storage locations observed:*	*<Report Findings Here>*				

Requirements		Validation Methods	Findings			
			In Place	In Place w/CCW	N/A	Not in Place
	• *Describe observations and outcomes:*	<*Report Findings Here*>				
	• *Identify personnel interviewed and describe results of interviews:*	<*Report Findings Here*>				
	• *Additional assessor comments:*	<*Report Findings Here*>				
P2–5.2 Data transmission						
P2	**5.2.1** Strong cryptography and security protocols are used to safeguard 3DS sensitive data during transmission.	• Examine documentation describing methods for encrypting data. • Examine configuration standards. • Observe implemented controls.	☐	☐	☐	☐
	• *Identify documented methodology examined:*	<*Report Findings Here*>				
	• *Describe the configuration standards examined:*	<*Report Findings Here*>				
	• *Describe observations and outcomes:*	<*Report Findings Here*>				
	• *Additional assessor comments:*	<*Report Findings Here*>				
P2	**5.2.2** Fallback to insecure cryptographic protocols and configurations is not permitted.	• Examine documentation describing methods for encrypting data. • Examine configuration standards. • Observe implemented controls.	☐	☐	☐	☐
	• *Identify documented methodology examined:*	<*Report Findings Here*>				
	• *Describe the configuration standards examined:*	<*Report Findings Here*>				
	• *Describe observations and outcomes:*	<*Report Findings Here*>				
	• *Additional assessor comments:*	<*Report Findings Here*>				
P2–5.3 TLS configuration						
P2	**5.3.1** All TLS communications between ACS, DS and 3DSS for purposes of 3DS transmissions use only allowed cipher suites, as defined in the *EMV® 3DS Protocol and Core Functions Specification.*	• Examine configuration standards and TLS configurations. • Observe TLS communications.	☐	☐	☐	☐
	• *Describe configuration standards examined:*	<*Report Findings Here*>				
	• *Describe TLS configurations examined:*	<*Report Findings Here*>				

	Requirements	Validation Methods	Findings			
			In Place	In Place w/CCW	N/A	Not in Place
	• *Describe observations and outcomes:*	*<Report Findings Here>*				
	• *Additional assessor comments:*	*<Report Findings Here>*				
	• *Additional assessor comments:*	*<Report Findings Here>*				
P2	**5.3.2** 3DS components (ACS, DS, and 3DSS) do not offer or support any cipher suite that identified as "not supported" in the *EMV® 3DS Protocol and Core Functions Specification*.	• Examine configuration standards and TLS configurations. • Observe TLS communications.	☐	☐	☐	☐
	• *Describe configuration standards examined:*	*<Report Findings Here>*				
	• *Describe TLS configurations examined:*	*<Report Findings Here>*				
	• *Describe observations and outcomes:*	*<Report Findings Here>*				
	• *Additional assessor comments:*	*<Report Findings Here>*				
P2	**5.3.3** TLS configurations do not support rollback to unapproved algorithms, key sizes, or implementations.	• Examine configuration standards and TLS configurations. • Observe TLS communications.	☐	☐	☐	☐
	• *Describe configuration standards examined:*	*<Report Findings Here>*				
	• *Describe TLS configurations examined:*	*<Report Findings Here>*				
	• *Describe observations and outcomes:*	*<Report Findings Here>*				
	• *Additional assessor comments:*	*<Report Findings Here>*				
P2	**5.3.4** Controls are in place to monitor TLS configurations to identify configuration changes and to ensure secure TLS configuration is maintained.	• Observe implemented controls for monitoring and maintaining TLS configurations. • Interview personnel.	☐	☐	☐	☐
	• *Describe observations and outcomes::*	*<Report Findings Here>*				
	• *Identify personnel interviewed and describe results of interviews:*	*<Report Findings Here>*				
	• *Additional assessor comments:*	*<Report Findings Here>*				

Requirements		Validation Methods	Findings			
			In Place	In Place w/CCW	N/A	Not in Place
P2–5.4 Data Storage						
P2	**5.4.1** Storage of 3DS sensitive data is limited to only permitted data elements.	• Examine data flows and 3DS transaction processes. • Observe data storage.	☐	☐	☐	☐
	• *Identify data flows and 3DS transaction processes examined:*	*<Report Findings Here>*				
	• *Identify data storage examined:*	*<Report Findings Here>*				
	• *Describe observations and outcomes:*	*<Report Findings Here>*				
	• *Additional assessor comments:*	*<Report Findings Here>*				
P2	**5.4.2** Strong cryptography is used to protect any permitted storage of 3DS sensitive data.	• Examine documentation describing methods for protecting stored data. • Observe implemented controls and configurations.	☐	☐	☐	☐
	• *Identify documented methodology examined:*	*<Report Findings Here>*				
	• *Describe observations and outcomes:*	*<Report Findings Here>*				
	• *Additional assessor comments:*	*<Report Findings Here>*				
P2–5.5 Monitor 3DS transactions						
P2	**5.5.1** 3DS transactions are monitored to identify, log, and alert upon anomalous activity.	• Examine documented procedures and configuration standards. • Examine log files. • Observe implemented controls. • Interview personnel.	☐	☐	☐	☐
	• *Identify documented procedures and configuration standards examined:*	*<Report Findings Here>*				
	• *Identify log files examined:*	*<Report Findings Here>*				
	• *Describe observations and outcomes:*	*<Report Findings Here>*				
	• *Identify personnel interviewed and describe results of interviews:*	*<Report Findings Here>*				
	• *Additional assessor comments:*	*<Report Findings Here>*				

Requirements		Validation Methods	Findings			
			In Place	In Place w/CCW	N/A	Not in Place
P2	**5.5.2** Anomalous or suspicious transaction activity is investigated and addressed in a timely manner.	• Examine documented procedures and configuration standards. • Examine log files. • Observe implemented controls. • Interview personnel.	☐	☐	☐	☐
	• *Identify documented procedures and configuration standards examined:*	*<Report Findings Here>*				
	• *Identify log files examined:*	*<Report Findings Here>*				
	• *Describe observations and outcomes:*	*<Report Findings Here>*				
	• *Identify personnel interviewed and describe results of interviews:*	*<Report Findings Here>*				
	• *Additional assessor comments:*	*<Report Findings Here>*				
Requirement P2-6. Cryptography and Key Management						
P2–6.1 Key management						
P2	**6.1.1** Policies and procedures for managing cryptographic processes and keys are maintained and implemented.	• Examine documented policies and procedures. • Interview personnel.	☐	☐	☐	☐
	• *Identify documented policies and procedures examined:*	*<Report Findings Here>*				
	• *Identify personnel interviewed and describe results of interviews:*	*<Report Findings Here>*				
	• *Additional assessor comments:*	*<Report Findings Here>*				
P2	**6.1.2** ***For ACS and DS only:*** All key management activity for specified cryptographic keys (as defined in the *PCI 3DS Data Matrix*) is performed using an HSM that is either: • FIPS 140-2 Level 3 (overall) or higher certified, or • PCI PTS HSM approved.	• Examine documented key-management procedures. • Interview personnel.	☐	☐	☐	☐
	• *Identify whether the HSM is FIPS 140-2 Level 3 (overall) or higher certified or PCI PTS HSM approved:*	*<Report Findings Here>*				
	• *Identify documented key-management procedures examined:*	*<Report Findings Here>*				
	• *Identify personnel interviewed and describe results of interviews:*	*<Report Findings Here>*				

Requirements		Validation Methods	Findings			
			In Place	In Place w/CCW	N/A	Not in Place
	• *Additional assessor comments:*	*<Report Findings Here>*				
P2	**6.1.3** ***For ACS and DS only:*** The HSM is deployed securely, in accordance with the security policy, as follows: • If FIPS-approved HSMs are used, the HSM uses the FIPS-approved cryptographic primitives, data-protection mechanisms, and key-management processes for account data decryption and related processes. • If PCI PTS-approved HSMs are used, the HSM is configured to operate in accordance with the security policy that was included in the PTS HSM approval, for all operations (including algorithms, data protection, key management, etc.).	• Examine HSM approval documentation / security policy (as applicable). • Observe HSM configurations.	☐	☐	☐	☐
	• *Identify HSM approval documentation/security policy examined:*	*<Report Findings Here>*				
	• *Describe observations and outcomes:*	*<Report Findings Here>*				
	• *Additional assessor comments:*	*<Report Findings Here>*				
P2	**6.1.4** A documented description of the cryptographic architecture exists that includes: • Description of the usage for all keys • Details of all keys used by each HSM (if applicable)	• Examine documented description of the cryptographic architecture. • Interview personnel. • Examine HSM approval documentation.	☐	☐	☐	☐
	• *Identify documented description of the cryptographic architecture examined:*	*<Report Findings Here>*				
	• *Identify HSM approval documentation examined:*	*<Report Findings Here>*				
	• *Identify personnel interviewed and describe results of interviews:*	*<Report Findings Here>*				
	• *Additional assessor comments:*	*<Report Findings Here>*				

Requirements		Validation Methods	Findings			
			In Place	In Place w/CCW	N/A	Not in Place
P2	**6.1.5** Cryptographic keys are securely managed throughout the cryptographic lifecycle including: • Generation • Distribution/conveyance • Storage • Established crypto periods • Replacement/rotation when the crypto period is reached • Escrow/backup • Key compromise and recovery • Emergency procedures to destroy and replace keys • Accountability and audit	• Examine documented key-management procedures. • Observe key-management activities. • Interview personnel.	☐	☐	☐	☐
	• *Identify documented key-management procedures examined:*	*<Report Findings Here>*				
	• *Describe observations and outcomes:*	*<Report Findings Here>*				
	• *Identify personnel interviewed and describe results of interviews:*	*<Report Findings Here>*				
	• *Additional assessor comments:*	*<Report Findings Here>*				
P2	**6.1.6** Cryptographic key-management processes conform to recognized national or international key-management standards.	• Examine documented key-management procedures. • Observe key-management activities. • Interview personnel.	☐	☐	☐	☐
	• *Identify documented key-management procedures examined:*	*<Report Findings Here>*				
	• *Describe observations and outcomes:*	*<Report Findings Here>*				
	• *Identify personnel interviewed and describe results of interviews:*	*<Report Findings Here>*				
	• *Additional assessor comments:*	*<Report Findings Here>*				

Requirements		Validation Methods	Findings			
			In Place	In Place w/CCW	N/A	Not in Place
P2	**6.1.7** Cryptographic keys are used only for their intended purpose, and keys used for 3DS functions are not used for non-3DS purposes.	• Examine documented key-management procedures. • Interview personnel.	☐	☐	☐	☐
	• *Identify documented key-management procedures examined:*	*<Report Findings Here>*				
	• *Identify personnel interviewed and describe results of interviews:*	*<Report Findings Here>*				
	• *Additional assessor comments:*	*<Report Findings Here>*				
P2	**6.1.8** A trusted Certificate Authority is used to issue all digital certificates used for 3DS operations between 3DSS, ACS, and DS components.	• Examine documented evidence of Certificate Authority validation (e.g., security assessments, certifications). • Observe implemented digital certificates.	☐	☐	☐	☐
	• *Identify documented evidence of Certificate Authority validation examined:*	*<Report Findings Here>*				
	• *Describe observations and outcomes:*	*<Report Findings Here>*				
	• *Additional assessor comments:*	*<Report Findings Here>*				
P2	**6.1.9** Audit logs are maintained for all key-management activities and all activities involving clear-text key components. The audit log includes: • Unique identification of the individual that performed each function • Date and time • Function being performed • Purpose • Success or Failure of activity	• Examine documented key-management procedures. • Examine audit logs. • Interview personnel.	☐	☐	☐	☐
	• *Identify documented key-management procedures examined:*	*<Report Findings Here>*				
	• *Identify audit logs examined:*	*<Report Findings Here>*				
	• *Describe observations and outcomes:*	*<Report Findings Here>*				
	• *Identify personnel interviewed and describe results of interviews:*	*<Report Findings Here>*				
	• *Additional assessor comments:*	*<Report Findings Here>*				

Requirements		Validation Methods	Findings			
			In Place	In Place w/CCW	N/A	Not in Place
P2	**6.1.10** Incident response procedures include activities for reporting and responding to suspicious or confirmed key-related issues.	• Examine documented incident response procedures. • Interview personnel.	☐	☐	☐	☐
	• *Identify documented incident response procedures examined:*	*<Report Findings Here>*				
	• *Identify personnel interviewed and describe results of interviews:*	*<Report Findings Here>*				
	• *Additional assessor comments:*	*<Report Findings Here>*				
P2–6.2 Secure Logical Access to HSMs (*For ACS and DS only*)						
P2	**6.2.1** Personnel with logical access to HSMs must be either at the HSM console or using an HSM non-console access solution that has been evaluated by an independent laboratory to comply with the following sections of the current version of ISO 13491: • Annex A – Section A.2.2: Logical security characteristics. • Annex D – Section D.2: Logical security characteristics. *(**Note:** The use of single DEA message authentication codes is not permitted.)* • Annex E – Section E.2.1: Physical security characteristics, and Section E.2.2 Logical security characteristics. *(**Note:** Only random number generators meeting the requirements of SP 800-90A are allowed.)* • Annex F – Section F.2.1: Physical security characteristics, and Section F.2.2 Logical security characteristics. • If digital signature functionality is provided: Annex G – Section G.2.1 General considerations, and Section G.2.2 Device management for digital signature verification.	• Examine systems configurations. If non-console access is used: • Examine documented evidence (e.g., lab certification letters, solution technical documentation, or vendor attestation) that the solution has been validated to applicable ISO requirements. • Observe implemented solution.	☐	☐	☐	☐
	• *Describe system configurations examined:*	*<Report Findings Here>*				
	• *Identify whether non-console access is used:*	*<Report Findings Here>*				
	• *If non-console access is used, identify documented evidence of solution validation to applicable ISO requirements examined:*	*<Report Findings Here>*				
	• *Describe observations and outcomes:*	*<Report Findings Here>*				
	• *Additional assessor comments:*	*<Report Findings Here>*				

Requirements		Validation Methods	Findings			
			In Place	In Place w/CCW	N/A	Not in Place
P2	**6.2.2** All non-console access to HSMs originates from a 3DE network(s).	• Examine network and system configuration settings.	☐	☐	☐	☐
	• *Identify network and system configurations examined:*	*<Report Findings Here>*				
	• *Describe observations and outcomes:*	*<Report Findings Here>*				
	• *Additional assessor comments:*	*<Report Findings Here>*				
P2	**6.2.3** Devices used to provide personnel with non-console access to HSMs are secured as follows: • Located in a designated secure area or room that is monitored at all times. • Locked in room/rack/cabinet/ drawer/safe when not in use. • Physical access is restricted to authorized personnel and managed under dual control. • Authentication mechanisms (e.g., smart cards, dongles etc.) for devices with non-console access are physically secured when not in use. • Operation of the device requires dual-control and multifactor authentication. • Devices have only applications and software installed that is necessary. • Devices are verified as having up-to-date security configurations. • Devices cannot be connected to other networks while connected to the HSM. • Devices are cryptographically authenticated prior to the connection being granted access to HSM functions.	• Observe locations of devices used for non-console access to HSMs. • Observe device configurations. • Observe HSM authentication mechanisms	☐	☐	☐	☐
	• *Identify locations of devices used for non-console access to HSMs observed:*	*<Report Findings Here>*				
	• *Describe device configurations observations and outcomes:*	*<Report Findings Here>*				
	• *Describe HSM authentication mechanism observations and outcomes:*	*<Report Findings Here>*				
	• *Additional assessor comments:*	*<Report Findings Here>*				

Requirements		Validation Methods	Findings			
			In Place	In Place w/CCW	N/A	Not in Place
P2	**6.2.4** The loading and exporting of clear-text cryptographic keys, key components and/or key shares to/from the HSM is not performed over a non-console connection.	• Examine device configurations.	☐	☐	☐	☐
	• *Identify device configurations examined:*	*<Report Findings Here>*				
	• *Additional assessor comments:*	*<Report Findings Here>*				
P2	**6.2.5** Activities performed via non-console access adhere to all other HSM and key-management requirements.	• Examine policies and procedures. • Interview personnel. • Examine HSM configurations and observe connection processes.	☐	☐	☐	☐
	• *Identify documented policies and procedures examined:*	*<Report Findings Here>*				
	• *Identify HSM configurations examined:*	*<Report Findings Here>*				
	• *Describe observations and outcomes:*	*<Report Findings Here>*				
	• *Identify personnel interviewed and describe results of interviews:*	*<Report Findings Here>*				
	• *Additional assessor comments:*	*<Report Findings Here>*				
	P2–6.3 Secure Physical Access to HSMs *(For ACS and DS only)*					
P2	**6.3.1** HSMs are stored in a dedicated area(s).	• Examine 3DS device inventory. • Observe physical locations of HSMs.	☐	☐	☐	☐
	• *Describe 3DS device inventory examined:*	*<Report Findings Here>*				
	• *Describe observations and outcomes:*	*<Report Findings Here>*				
	• *Additional assessor comments:*	*<Report Findings Here>*				
P2	**6.3.2** Physical access to the HSMs is restricted to authorized personnel and managed under dual control.	• Examine documented procedures. • Observe access controls.	☐	☐	☐	☐
	• *Identify documented procedures examined:*	*<Report Findings Here>*				
	• *Describe observations and outcomes:*	*<Report Findings Here>*				
	• *Additional assessor comments:*	*<Report Findings Here>*				

Requirements		Validation Methods	Findings			
			In Place	In Place w/CCW	N/A	Not in Place
Requirement P2-7. Physically secure 3DS systems						
P2	**7.1.1** ACS and DS systems are hosted in data center environments.	• Observe ACS/DS locations.	☐	☐	☐	☐
	• *Identify ACS/DS locations observed:*	<*Report Findings Here*>				
	• *Describe observations and outcomes:*	<*Report Findings Here*>				
	• *Additional assessor comments:*	<*Report Findings Here*>				
P2	**7.1.2** Data centers supporting ACS and DS are equipped with a positively controlled single-entry portal (e.g., mantrap), that: • Requires positive authentication prior to granting entry; and • Grants entry to a single person for each positive authentication.	• Observe data center entry points.	☐	☐	☐	☐
	• *Describe observations and outcomes:*	<*Report Findings Here*>				
	• *Additional assessor comments:*	<*Report Findings Here*>				
P2	**7.1.3** Doors to areas within the data center that contain 3DS systems are fitted with an electronic access control system (e.g., card reader, biometric scanner) that controls and records all entry and exit activities.	• Observe all entrances to the 3DE. • Examine audit logs and/or other access records.	☐	☐	☐	☐
	• *Describe observations and outcomes:*	<*Report Findings Here*>				
	• *Identify audit logs and/or other access records examined:*	<*Report Findings Here*>				
	• *Additional assessor comments:*	<*Report Findings Here*>				
P2	**7.1.4** Multi-factor authentication is required for entry to telecommunications rooms that are not located within a secure data center.	• Examine access controls. • Observe access events.	☐	☐	☐	☐
	• *Identify access controls examined:*	<*Report Findings Here*>				
	• *Describe access event observations and outcomes:*	<*Report Findings Here*>				
	• *Additional assessor comments:*	<*Report Findings Here*>				

Requirements		Validation Methods	Findings			
			In Place	In Place w/CCW	N/A	Not in Place
P2	**7.1.5** Entry controls prevent piggy-backing by granting access to a single person at a time, with each person being identified and authenticated before access is granted.	• Observe personnel entering the data center.	☐	☐	☐	☐
	• *Describe observations and outcomes:*	<Report Findings Here>				
	• *Additional assessor comments:*	<Report Findings Here>				
P2	**7.1.6** A physical intrusion-detection system that is connected to the alarm system is in place.	• Interview personnel. • Observe intrusion-detection controls.	☐	☐	☐	☐
	• *Describe observations and outcomes:*	<Report Findings Here>				
	• *Identify personnel interviewed and describe results of interviews:*	<Report Findings Here>				
	• *Additional assessor comments:*	<Report Findings Here>				
P2	**7.1.7** Physical connection points leading into the 3DE are controlled at all times.	• Observe physical connection points.	☐	☐	☐	☐
	• *Describe observations and outcomes:*	<Report Findings Here>				
	• *Additional assessor comments:*	<Report Findings Here>				
	P2–7.2 CCTV					
P2	**7.2.1** CCTV cameras are located at all entrances and emergency exit points and capture identifiable images, at all times of the day and night.	• Observe all entrances and emergency exit points. • Examine CCTV footage.	☐	☐	☐	☐
	• *Identify ACS locations observed:*	<Report Findings Here>				
	• *Identify DS locations observed:*	<Report Findings Here>				
	• *Describe observations and outcomes:*	<Report Findings Here>				
	• *Additional assessor comments:*	<Report Findings Here>				
P2	**7.2.2** CCTV recordings are time stamped.	• Examine CCTV records.	☐	☐	☐	☐
	• *Identify CCTV records examined:*	<Report Findings Here>				
	• *Additional assessor comments:*	<Report Findings Here>				

Appendix A: Compensating Controls Worksheet

If a compensating control(s) is used to meet any PCI 3DS requirement, complete a Compensating Controls Worksheet (CCW) for each requirement.

Refer to Appendix A-1: Compensating Controls in the PCI 3DS Core Security Standard for details on the use of compensating controls.

Note: *Only companies that have undertaken a risk analysis and have legitimate technological or documented business constraints can consider the use of compensating controls to achieve compliance.*

3DS Requirement Number and Description:	

Information Required	Description	Explanation
1. Constraints	List constraints precluding compliance with the original requirement.	
2. Objective	Define the objective of the original requirement; identify the objective met by the compensating control.	
3. Identified Risk	Identify any additional risk posed by the lack of the original control.	
4. Definition of Compensating Controls	Define the compensating controls and explain how they address the objectives of the original control and the increased risk, if any.	
5. Validation of Compensating Controls	Define how the compensating controls were validated and tested.	
6. Maintenance	Define processes and controls in place to monitor and maintain the effectiveness of the compensating controls.	

Appendix B: Explanation of Non-Applicability

If "N/A" (Not Applicable) was selected for any requirement, explain why the requirement is not applicable to the 3DS entity.

Requirement	Reason Requirement is Not Applicable
Example: P2-6.1.2	The entity is being assessed only for 3DSS—it is not involved in ACS or DS functions.