Take the Chaos out of Compliance
Assess Smarter Not Harder

PCI Compliance & Sustainability

Payment Card Assessments, LLC

PCI DSS Report on Compliance Planner

AUGUST 2022
REVISED JANUARY 2023 TO INCLUDE THE CUSTOMIZED APPROACH IN PCI DSS V4.0

Table of Contents

Table of Contents	
3	Disclaimer
4	Welcome
6	Roles & Responsibilities
9	Report on Compliance Milestones
14	Scope Assessment
15	Customized Approach (new in PCI DSS v4.0 effective March 31, 2024)
18	Compensating Controls
21	Remediation Projects
23	Sample Agendas and Daily Calendar
26	The RoC Assessment Phase
30	Post RoC: Lessons Learned
33	More Resources

Who This Planner is For

This planner is for PCI-ISA's and PCI-P's and anyone tasked with delivering a PCI DSS Report on Compliance.

Disclaimer: (because we need to have one)

The intent of this planner is to help merchants plan, organize and execute a PCI DSS Report on Compliance assessment.

This planner does not guarantee that you will receive a report on compliance from your QSA.

This planner does not absolve any merchant from their contractual and legal obligations with the PCI SSC, card brands, and their acquirer(s).

No part of this planner may be copied or published by any entity without permission from Payment Card Assessments, LLC.

Welcome

You got this!

Welcome to the first day of your PCI Report on Compliance (RoC). Whether this your first RoC or you've done this more times than you'd like to count, this planner is designed to help you plan, organize, and execute on the activities critical to a successful RoC.

We want you to be able to deliver your Report on Compliance to your acquirer on time and on budget.

So let's get started, shall we?

Here's to your success,

Peggy & Lisa

START HERE

Commit to Your PCI Journey

THE CHOICE TO CHANGE

No one grows up thinking they're going to be doing PCI Compliance when they get older. No one. In fact, I still want to be an astronaut but there's this thing about training underwater and I just can't get past that.

In all seriousness, you're on the PCI compliance team or in charge of it and now it's on you to deliver.

I remember the stress and anxieity of my first Report on Compliance.

I muscled my way through it. I pushed, pulled, prodded, and begged other people along the way. I delivered a signed RoC on December 21, 2012 and took the rest of the year off. I spent 3 days on the couch watching reruns of Doctor Who. I struggled with going back. I thought about quitting. In the end, I went back with a strong resolve to create the best PCI DSS Compliance program in the universe.

So, let me ask you, are you ready for the next step?

Peggy

Roles & Responsibilities

Before you begin your Report on Compliance, it's important to review roles and responsibilities so everyone has a clear understanding of who is responsible for completing tasks and who needs to be kept informed.

Key Roles and Responsibilities

- QSA - Qualified Security Assessor -
  - responsible for assessing the merchant's security controls for their PCI DSS in scope assets, processes, and people.

- ISA - Internal Security Assessor -
  - Responsible for managing the Report on Compliance
  - Assigns tasks
  - Collects evidence
  - Assesses evidence to ensure accuracy
  - Assigns evidence to QSA for their assessment
  - Communicates status
  - Influences leadership and teams with PCI DSS responsibilities
  - Delivers the AoC to acquirers
  - MUST be kept informed and review all business and technical proposals that impact the security of the cardholder data environment (CDE).

- System Administrators, Security Architects, Software Developers
  - Responsible for maintaining security controls on the in-scope systems they "own."
  - Creates process documentation / standard operating procedures for their systems.
  - Provides evidence based on requirement frequencies.
  - Provides real time observations and responds to interview requirements.
  - Attends security training and provides training certificates as required.

Failure to plan is a plan to fail
~ Benjamin Franklin

Key RoC Milestones

Plan the Work

How do you eat an elephant?
---- one bite at a time.

Ready to plan your assessment? Let's start with the most critical milestone ~ the date your RoC is due to your acquirer:

Date Report on Compliance is due to merchant acquirer(s):

_____

Now let's work 6 months backward from this date to start your assessment:

Report on Compliance start date is:

_____

Key RoC Milestones

CREATE AN ACHIEVABLE TIMELINE

Use this milestone checklist to create a timeline for your organization.

- 6 months before Report on Compliance is due:
  - Set the start date of your assessment. For example, if your RoC is due August 30, your kickoff date is February 1.
  - Continue to collect evidence for all requirements with frequencies and for your critical controls that you need to continously monitor for effectiveness.
- 30 days before assessment starts:
  - Ensure SOW & NDA with QSA is in place.
  - Begin full scope assessment to include card data, network diagram, customized controls (new in v4.0) & comp control walk-throughs with network security architects, billing, finance, application developers, QSA.
    - Include remediation efforts that will directly or indirectly impact the assessment.
- 3 weeks before assessment starts:
  - Schedule mandatory annual PCI training for all in-scope personnel, include QSA, managers and directors as needed. This training *should* be completed before the assessment officially begins.
- 2 weeks before assessment starts:
  - Send out meeting invitations to all teams, leadership, and QSA for the RoC Kick-Off Meeting.
  - Complete scope assessment.
  - Send final in-scope asset inventory to QSA for sampling.
    - Note where automation is in place to ensure contionous complliance
  - Upload evidence (diagrams, card data flows, etc.) gathered during scope assessment to Polaris PCA.
  - Establish weekly status meeting for the duration of the assessment period.

Key RoC Milestones

CREATE AN ACHIEVABLE TIMELINE

- 1 week before assessment starts:
  - Complete mandatory PCI training.
  - QSA must return sample sets from in-scope inventory.
  - Schedule all physical site assessments.
  - Begin creating interview and observation schedule.
- Assessment start date:
  - Official meeting to kick-off Report on Compliance
  - Assign tasks in Polaris PCA
- 1 day after assessment kick-off
  - QSA begins assessing policies, standards, processes, evidence.
  - Assessing RoC evidence takes about 4 months depending on the size, scope, and complexity of your cardholder data environment.
- 1 week after start date
  - Schedule interview dry-runs as needed by your subject matter experts. Dry-runs benefit new system administrators as well as systems administrators who get nervous during interviews.
  - Confirm all physcial site assessments have been scheduled.
- 6 weeks before RoC is due to acquirer:
  - All documentation and evidence has been assessed and or reassessed if the QSA determined the requirement(s) was not in place.
  - Draft Report on Compliance is with the QSA's QA team. Allow 3-4 weeks for QA process
- 2 weeks before RoC is due to acquirer:
  - Merchant reviews draft of RoC. to ensure accuracy of entire document.
- 1 week before RoC is due to acquirer
  - Merchant and QSA co-sign merchant letter and Attestation of Compliance.

Key RoC Milestones

CREATE AN ACHIEVABLE TIMELINE

- On or before the RoC is due to acquirer
  - Submit RoC, AoC, and most current ASV scans to acquirer
- Within 1-3 days after RoC is sent to acquirer
  - Celebrate, Apprectiate, and Recognize your team
  - Conduct Retro or Lessons Learned
  - Determine what improvements can be made in the process
- Rinse and repeat
  - Continue monitoring key control activities
  - Continue gathering evidence for requirements with frequencies

Sample Milestone Checklist

REPORT ON COMPLIANCE

KEY MILESTONE CHECKLIST

Task	Date Completed
1. Establish start & end dates	
2. NDA in place	
3. SOW in place	
4. Cardholder data walk-throughs	
5. Network diagram walk-throughs	
6. Customized control walk-throughs	
7. Comp control walk-throughs	
8. Remediation walk-throughs	
9. Schedule mandatory PCI training	
10. On-board QSA's as needed	
11. Schedule kick-off meeting	
12. Complete scope assessment	
13. Send asset list to QSA	
14. QSA returns sample	
15. Upload evidence from walk-throughs	
16. Establish weekly status meeting	
17. Deliver mandatory PCI training	
18. Schedule physical site visits	

Sample Milestone Checklist

REPORT ON COMPLIANCE

KEY MILESTONE CHECKLIST

Task	Date Completed
18. Schedule interviews & observations	
19. Facilitate kick-off meeting	
20. Assign assessment tasks in Polaris	
21. QSA begins assessment	
22. Practice interviews for SMEs	
23. QSA completes site visits	
24. Complete interviews/observations	
25. QSA completes assessing evidence	
26. QSA firm completes QA of RoC	
27. Merchant / ISA completes QA of RoC	
28. Merchant & QSA sign AoC	
29. ISA submits RoC, AoC to acquirer(s)	
30. Celebration Time	
31. Hold lessons learned/retro	
32. Implement process improvement	
33. Establish due date for next RoC	
34. Continous compliance activities	

Creating and maintaining an accurate inventory of your in-scope PCI assets ensures an accurate RoC Executive Summary, a smoother assessment, and it improves your ability to sustain PCI DSS Compliance.

Scope Assessment

When discussing PCI Compliance, it's critical that we start with scope.

Why? Understanding and knowing your scope is where you begin to create, build, and maintain a continuous PCI DSS Compliance program.

If you don't have a firm grasp on what's in scope for assessment, being able to complete a self-assessment or, if you're a level 1 merchant, a mandatory Report on Compliance is next to impossible.

To complete an end-to-end scope assessment, please see our PCI DSS on demand Scope Assessment Workshop & Guide.

New in PCI DSS v4.0 - effective March 31, 2024

COMP CONTROLS

The Customized Approach

Per PCI DSS v4.0

"This approach is intended for entities that decide to meet a PCI DSS requirement's stated Customized Approach Objective in a way that does not strictly follow the defined requirement. The customized approach allows an entity to take a strategic approach to meeting a requirement's Customized Approach Objective, so it can determine and design the security controls needed to meet the objective in a manner unique for that organization."

Customized Approach

The Customized Approach is new with PCI DSS v4.0. It is not the same as a compensating control.

To implement a customized control to meet the objective of a requirement that meets the unique strategy of the organization, an entity must do the following:

Note: Refer to Appendix D & E in the PCI DSS

- Document and maintain evidence about each customized control, including all information specified in the Controls Matrix Template in Appendix E1.
- Perform and document a targeted risk analysis (PCI DSS Requirement 12.3.2) for **each** customized control, including all information specified in the Targeted Risk Analysis Template in Appendix E2.
- Perform testing of each customized control to prove effectiveness, and document testing performed, methods used, what was tested, when testing was performed, and results of testing in the controls matrix.
- Monitor and maintain evidence about the effectiveness of each customized control.
- Provide completed controls matrix(es), targeted risk analysis, testing evidence, and evidence of customized control effectiveness to its assessor.

Customized Approach

11 things to keep in mind when using the Customized Approach:

- Use custom controls sparingly
- Custom controls are not the same as compensating controls.
- Custom controls require effort above and beyond the defined approach
- Custom controls must be walked through when doing the scope assessment.
- Custom controls must be monitored on a regular cadence to ensure their effectiveness. This could be quarterly, monthly, or even daily.
- Custom controls may add confusion or complexity to the RoC
- Custom controls may not be sustainable
- Custom controls may not save time, effort, or money
- If you use a QSA to help design a custom control, he or she cannot assess that control.
- If you can meet the defined requirement without needing to customize anything, do that instead
- Likewise, if your custom approach for a specific requirement is more secure and better than the defined approach, follow the instructions in Appendix D & E and implement it.

As always, consult with your QSA and / or acquirer if you need to implement a compensating control or controls

Compensating Controls

Per PCI DSS v3.2.1 and v4.0:

"Compensating controls may be considered for most PCI DSS requirements when an entity cannot meet a requirement explicitly as stated, due to legitimate technical or documented business constraints, but has sufficiently mitigated the risk associated with the requirement through implementation of other, or compensating, controls."

Compensating Controls

Note: Refer to Appendix B in the PCI DSS Reporting Instructions

- Compensating controls, while permitted, should not be permanent.
- Compensating controls must go above and beyond the requirement in question.
- Compensating controls that were previously assessed in place must be assessed again if the merchant cannot meet the stated requirement.
- If the QSA feels that your compensating control does not meet the due diligence and rigor required, the only entity that can accept your risk is your acquirer.
  - You must meet with your acquirer to discuss the risk, what you've done to mitigate risk and proof of due diligence.
  - If your acquirer agrees to accept your risk, they must respond in writing (email is fine), and you must retain this as evidence for your Report on Compliance.

Compensating Controls:

- Comp controls are often manual and resource intensive
- Complicated and complex.
- Due to the ever changing threat landscape, comp controls are not sustainable.

Compensating Controls DO NOT:

- Save time, money or effort

Compensating Controls

Note: Refer to Appendix C in the PCI DSS Reporting Instructions for the comp control worksheet. You must fill out one worksheet for each requirement that is being met with a comp control.

Include the following:

- Requirement number and description.
- Describe the business and / or legal constraints that are preventing your organization from meeting the defined PCI DSS requirement.
- Describe the objective of the original control; identify the objective met by the compensating control.
- Identify any risk associated with not meeting the control as defined in the PCI DSS.
- Define the comp control, the objective of the comp control, and how the comp control mitigates any risk associated with not meeting the original requirement.
- Describe how the comp control was validated and tested.
- Describe the process/procedure of the comp control and describe how the comp control will be maintained and monitored for effectiveness.

REMEMBER: Compensating Controls DO NOT:

- Save time, money or effort

REMEMBER: Review your comp controls during the scope assessment with your QSA.

If you start a RoC assessment with one or more remediation efforts, the remediation project must be completed and all evidence turned in 2 weeks before the RoC goes into QA

Remediation Efforts

Upgrades happen.

Vulnerabilities show up when you least expect them.

Someone will accidentally decommission a server that 30 other servers rely on for logging.

Outages happen.

The remediation effort to transition from one logging tool to a better one is still ongoing as you start your annual RoC.

During the scope assessment, disclose any ongoing remediation efforts that directly or indirectly impact your cardholder data enviroment.

Current Remediation Efforts

In a perfect world, nothing would break. Servers wouldn't drift out of configuration standards, security flaws wouldn't need patching, and operating systems would never reach end of life. While it's not ideal to begin a RoC with an ongoing remediation effort or multiple efforts, it's not unheard of. Any and all remediation efforts in play for the assessment must complete and turn in all evidence by the final due date for all evidence .

REMEDIATION PROJECT #1

Problem

Est completion date:_____

Solution

POC

REMEDIATION PROJECT #2

Problem

Est completion date:_____

Solution

POC

REMEDIATION PROJECT #3

Problem

Est completion date:_____

Solution

POC

Merchants are legally and contractually obligated to maintain PCI DSS Compliance.

Sample Agendas & Daily Calendar

- Mandatory Training Agenda
- Kick-Off Agenda
- Status Meeting Agenda.
- For those who love to write their to-do lists, print out the daily calendar.

Sample Agendas & Topics

- Sample Mandatory PCI Training Agenda
  - Welcome & Introduction
  - Overview of PCI DSS purpose & objectives
  - Overview of PCI DSS high level requirements
  - Overview of merchant's processes and safeguards for handling cardholder data
  - Report on Compliance assessment timeline
  - Overview of merchant's assessment process
  - Open forum for Q&A

- Sample Kick-off Meeting Agenda
  - Welcome & Introduction
  - Opening remarks from CISO or CIO
  - Overview of PCI DSS purpose & objectives
  - Overview of scope
  - Report on Compliance assessment timeline
  - Overview of merchant's assessment process
  - What to expect during the assessment
  - Interviews, observations, evidence
  - Overview of merchant's current PCI DSS compliance status
  - Review merchant's remediation projects if any
  - Review frequency requirements that must be met during assessment
  - Open forum for Q&A

- Sample Status Meeting Agenda
  - Status of requirements in place, in progress, not in place
  - Blockers and at risk requirements
  - Status of remediation projects, if any
  - Due dates and deadlines
  - Open forum for Q&A

- Daily Standup with QSA
  - What requirements are "In place."
  - What requirements are "in progress."
  - What requirements are "not in place" and what the QSA needs to mark them "in place."

Date: _____

"PCI is everyone's responsibility" - Peggy Nolan

PCI DSS ASSESSMENT

SCHEDULE	TOP PRIORITIES
7:00	
8:00	
9:00	
10:00	
11:00	
12:00	NOTES
1:00	
2:00	
3:00	
4:00	
5:00	FOR TOMORROW
6:00	**1.**
7:00	**2.**
8:00	**3.**

Work the plan

Assessment Phase

- Have an understanding of the PCI DSS Requirements
  - Requirements have frequencies
  - Requirements are interconnected
- Automate your workflow
- Assign tasks
- Documentation (policies, standards, processes) must be current and have an annual review frequency
- Review evidence from system administrators
- Self-collect evidence whenever you can
- Consolidate interveiws with real-time observations
- Create a feedback loop for evidence that the ISA and / or QSA has assessed "not in place."

REMEDIATION EFFORTS

PCI DSS Requirement Basics

- If you're being assessed for the full PCI DSS, there are hundreds of requirements and sub-requirements that you must be in compliance with to pass your annual Report on Compliance.

- Not all of these requirements may apply to your environment. You will need to work with your QSA to determine what is "not applicable."

- Each main requirement may have one or many sub-requirements that may have one or many testing procedures that may have one or many burdens of proof.

- Some requirements are repetitive, contradictory, and / or no longer seen as a best security practice (v3.2.1).

- Requirements have frequencies, which means that compliance is ongoing and must be continuous for merchants to remain in good standing with their legal and contractual obligations.

- Some requirements loop together, which means that if you fail one, you may be failing all the requirements that loop together.

- If you can't comply with a requirement there are only two ways to handle it:
  - Your acquirer accepts the risk.
  - You implement a defensible compensating control that meets the rigor of compensating controls.

PCI DSS Requirement Basics

- Think of the DSS as the skeleton or the structure of your PCI Compliance program. The requirements tell you what you need to comply with.

- The testing procedures make up part of the connective tissue surrounding the structure of the requirements. The testing procedures tell you how to comply with the requirement. Be careful here as the testing procedures don't always match up with the proof you need to fully satisfy your compliance.

- The intent of the requirements is more connective tissue that connect the requirements and testing procedures. The intent tells you why you must comply. The PCI DSS includes this with the requirements to help explain the rationale and better educate merchants about securing their payment card environments.

- The proof required to validate your compliance is not in the PCI DSS. It's in the Requirements and Security Assessment Procedures. Types of proof:
  - Standards, policies, documented processes
  - Sample sets
  - Configuration settings
  - Real time observations
  - Interviews

Assessment Best Practices

- Use Polaris PCA for your PCI Report on Compliance assessment and sustainability program.
  - Automated workflow
  - Built in knowledge base withPCI DSS authoritative sources
  - Best practices to help you save thousands of dollars in outside assessment fees
  - Best practices to help you save hundreds of hours in internal work effort
  - Learn more by emailing Payment Card Assessments at support@paymentcardassessments.com

- Use the PCA Scope Assessment Guide Book

- Use the PCA Consolidated Interview and Observation Schedule
  - Practice interviews with system administrators before they are interviewed by the QSA
  - Schedule and attend every interview & real time observation

- Create an effective communication plan using the templates provided in this planner

- Remember to assess documentation for annual reviews and current dates.

- Self collect evidence whenever and wherever possible.

- Coordinate and schedule all physical site visits at the beginning of the assessment phase
  - Ensure you've communicated expectations, requirements, and the real time observations the QSA will be making at each location

- Schedule a daily stand-up meeting with your QSA (meeting cadence may vary) to review
  - What requirements are "In place."
  - What requirements are "in progress."
  - What requirements are "not in place" and what the QSA needs to mark them "in place."

The past is where you learn the lesson. The future is where you apply the lesson.
~ unk

Lessons Learned

Within two weeks of completing and submitting your Report on Compliance to your acquirer, it's time to host a RoC retrospective or Lessons Learned session.

- Invite someone outside of the PCI Compliance team to facilitate the retro/lessons learned session
- Invite system administrators, security architects, QSA, developers, mangers, and anyone else who has PCI responsibilities to attend the session.
- Use a free online retro tool to allow people to submit their responses

Lessons Learned List

In the space below, list the lessons learned from your most recent Report on Compliance.

WHAT WORKED WELL?

WHAT DIDN'T WORK WELL?

WHAT NEEDS TO CHANGE?

SHOUT OUTS

Prioritized Process Improvements

In the spaces below, describe the prioritized process improvements you're making for your next Report on Compliance

PROCESS IMPROVEMENT #1

PROCESS IMPROVEMENT #2

PROCESS IMPROVEMENT #3

PROCESS IMPROVEMENT #4

Additional Resources

- PCI DSS: https://pcissc.org

- Payment Card Assessments
  - Workshops
  - Coaching
  - Gap assessments: email support@paymentcardassessments.com
  - Automate your next RoC or SAQ with Polaris PCA: email support@paymentcardassessments.com

TAKE THE CHAOS OUT OF COMPLIANCE

...

ASSESS SMARTER NOT HARDER