PCI PA-DSS v3.2

What's New in PCI PA-DSS v3.2
Change Analysis Brief

CONTROL GAP

2016-07-26

Overview

Overview

We cover the following areas in this brief.

- What's new in PCI PA-DSS
  - Critical milestone dates
  - Changes to the PCI DSS and PA-DSS lifecycle
  - PA-DSS changes impact Implementers/Operators
- Some Key PCI DSS & PA-DSS Differences
- Our change analysis of PA-DSS v3.2
- Recommendations
- References

What's new in PCI PA-DSS

For vendors, implementers, and operators of validated applications.

Critical milestone dates

PCI PA-DSS v3.2

- PCI PA-DSS v3.2 has arrived!
- Published May 2016
- Effective June 1, 2016 - Now the current standard in force
- No future dated requirements
- Listed applications expire October 28, 2022
- No set retirement date

PCI PA-DSS v3.1

- DSS v3.1 is being retired
- Published May 2015
- Retires on August 31, 2016
- Listed applications expire October 28, 2019
- No impact and low impact changes accepted until applications expire

Changes to the PCI DSS & PA-DSS Lifecycle

In recent updates to assessor companies, the council shared:

- The DSS and PA-DSS have matured and maintenance will not require major changes
- Iterative changes will be made to address identified risks in the payment system
- Significant new DSS requirements will be future-dated to allow time for adoption

We believe this means:

- No more major DSS & PA-DSS updates on the current 36 month lifecycle
- Frequency of updates has not been formalized
- We may see frequent updates like we have seen annually with v3.1, v3.2
- Effective dates of the current version changes with the release of new versions
- PA-DSS may not see future dated requirements

PA-DSS changes impact Implementers/Operators

- PCI PA-DSS provides organizations with assurance that the application is securely developed, maintained, and does not impede DSS compliance
- Implementers/Operators (e.g. customers, integrator, resellers) of PA-DSS applications must follow vendor guidance to achieve DSS compliance
- Changes in PA-DSS 3.2 impact:
  - Implementation of the application and infrastructure
  - Patching and updating of the application
  - Administration of the application
  - Specific user roles

Some Key PCI DSS & PA-DSS Differences

While PCI PA-DSS aligns with and supports PCI DSS, there are significant differences where PA-DSS raises the bar:

- PA-DSS has never allowed compensating controls
- PA-DSS doesn't directly support disk level encryption as an alternative control (i.e. all encryption and key management requirements apply)
- The special cases for SSL and early TLS (i.e. migration/sunset and PTS exemptions) introduced in PCI DSS 3.1 were not carried over into PA-DSS

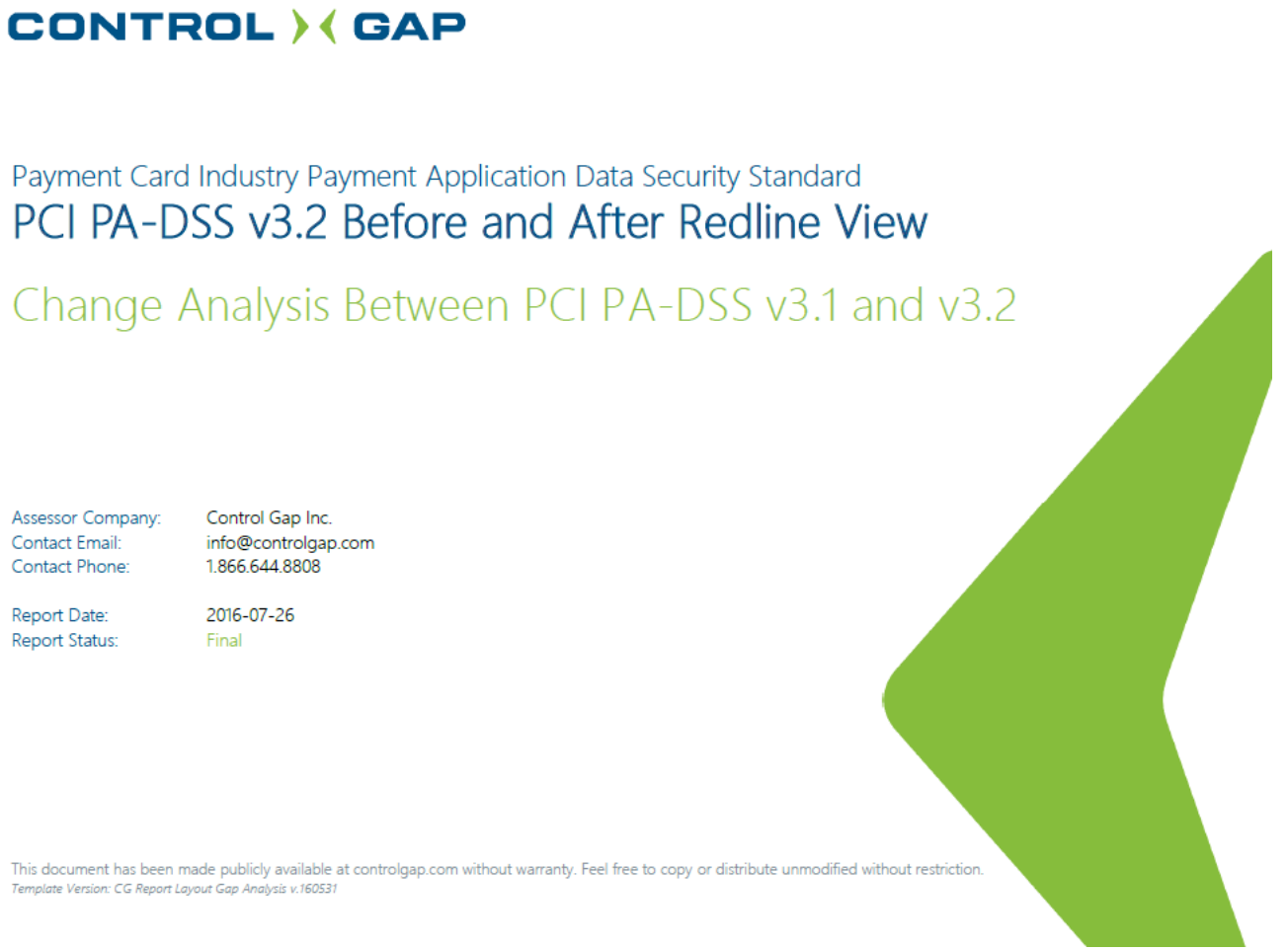
Our change analysis of PA-DSS v3.2

Control Gap PA-DSS v3.2 Change Analysis Companion Document

Want to know every word that changed in PCI PA-DSS v3.2?

See our detailed change analysis companion document.

PCI PA-DSS v3.2 Before & After Redline View.pdf



Our Impact Analysis Ratings

Our analysis estimated the impact of these changes based on:

- Our existing scoping and compliance validation process
- Our understanding and opinion of the original intent (of PA-DSS v3.1)
- The possible impact of the changes (of PA-DSS v3.2)

We analyzed and scored the potential impact of each changed item as follows:

- **None:** Negligible impact to compliance. Improvements in clarity and understanding of intent
- **Low:** Low impact/effort to compliance. A new incremental change potentially causing added or altered compliance efforts
- **High:** High impact/effort to compliance. A new requirement and/or potentially significant effort to achieve or sustain compliance

Note: Not all changes will be applicable to all applications. Each vendor must separately judge the actual severity of each impact.

Summary of PA-DSS v3.2 content changes

We found:

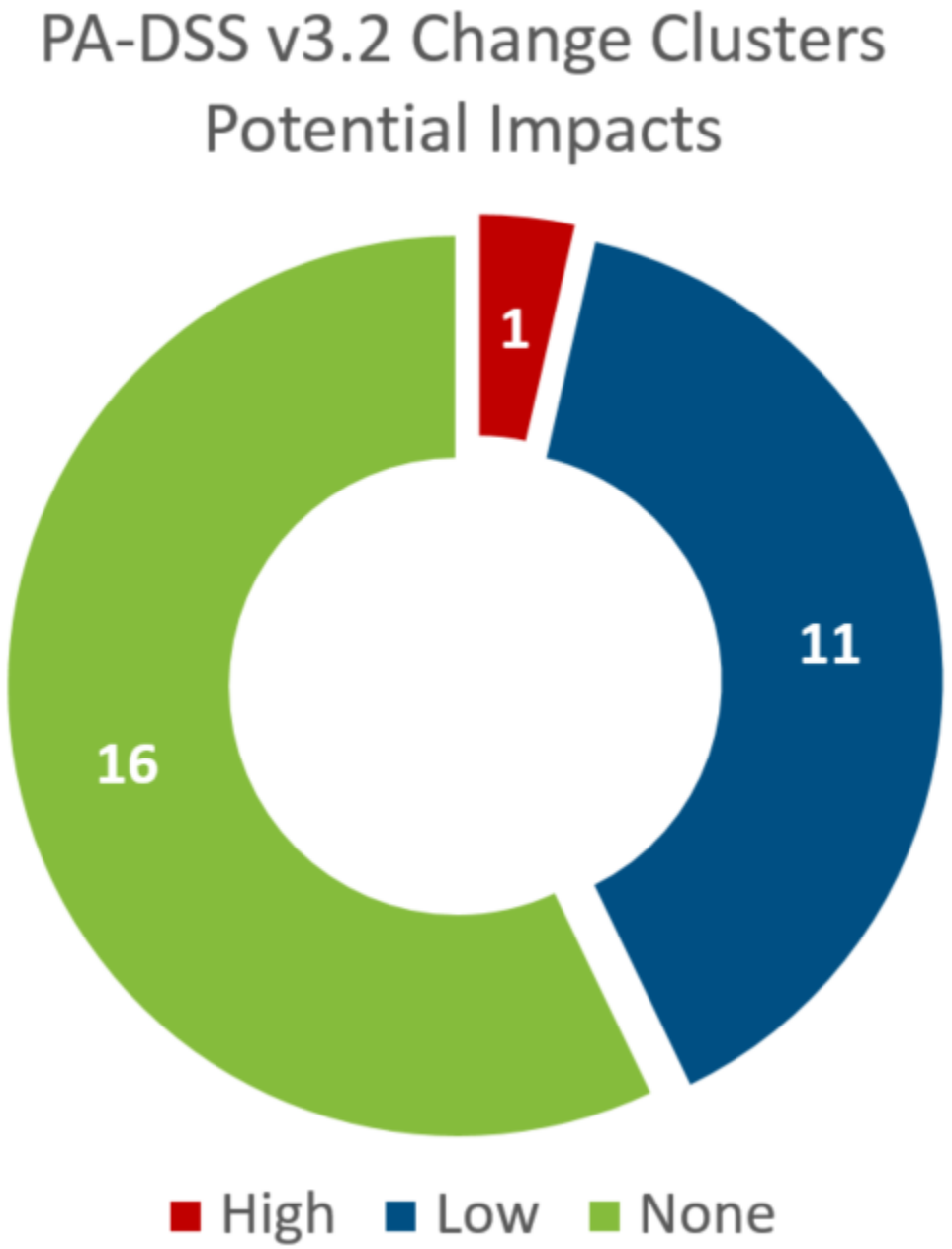
- Over a thousands words changed
- 28 total discrete change clusters
- 1 numbering change
- 2 new requirements
- 5 evolving (including new and changed) requirements

Significantly less changes when compared to DSS 3.2

Summary of PA-DSS v3.2 content changes

28 total discrete change clusters rated as:

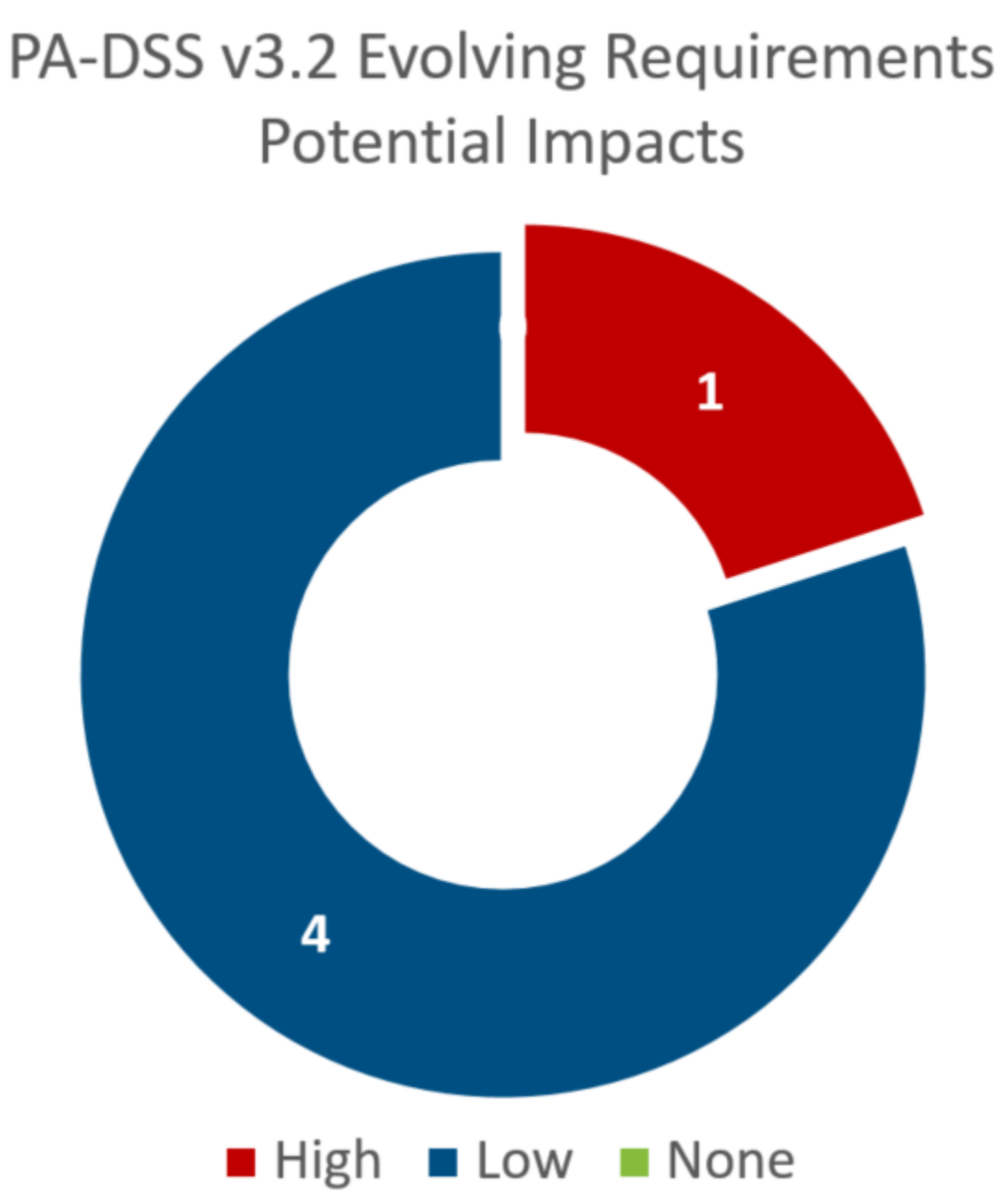
- 16 = None
- 11 = Low (#'s 3, 4, 5, 8, 9, 20, 21, 22, 23, 25, 28)
- 1 = High (# 18)



Summary of DSS v3.2 content changes

5 evolving requirements

- 3 existing requirements changed
  - (#'s 3, 4, 5)
- 2 new requirements added
  - (#'s 9, 18)



#3 – PA-DSS Req. 2.2

Potential Impact: Low

PCI SSC Evolving Requirement

Changed Requirement

PCI SSC Change Comments:

- Updated requirement to clarify that any displays of PAN greater than the first six/last four digits of the PAN requires a legitimate business need. Added guidance on common masking scenarios

This means:

- Only authorized personnel can see more than the first six and last four digits of the PAN
- This was previously to authorize views of "full" PAN
- Vendor's PCI Implementation Guide may not provide current instructions to configure access to unmasked partial PAN
- Delays to remediate if this is found in an ROV
- Potential impact and delays to Implementer/Operator ROC

#4 – PA-DSS Req. 2.3.a

Potential Impact: Low

PCI SSC Evolving Requirement

Changed Requirement

PCI SSC Change Comments:

- Updated testing procedure for the PA-DSS Implementation Guide to include instruction that if debugging logs are ever enabled (for example, for troubleshooting purposes), and include PAN, the logs must be protected in accordance with PCI DSS, disabled as soon as troubleshooting is complete, and securely deleted when no longer needed.

This means:

- Clear guidance must be provided to fully protect cardholder data even when stored temporarily such as for troubleshooting
- Vendor's PCI Implementation Guide may not provide current instructions to configure access to protect stored PAN
- Delays to remediate if this is found in an ROV
- Potential impact and delays to Implementer/Operator ROC

#5 – PA-DSS Req. 3.1.a

Potential Impact: Low

PCI SSC Evolving Requirement

Changed Requirement

PCI SSC Change Comments:

- Updated testing procedure for the PA-DSS Implementation Guide to include identification of all roles and default accounts within the application with administrative access.

This means:

- All applications and roles within the application must be clearly documented
- Vendor's PCI Implementation Guide may not provide current instructions to securely configure administrators and default accounts
- Delays to remediate if this is found in an ROV
- Potential impact and delays to Implementer/Operator ROC

#8 – PA-DSS Req. 5.1.7

Potential Impact: Low

PCI SSC Clarification

Changed Requirement

PCI SSC Change Comments:

- Clarified that training for developers must be up to date and occur at least annually

This means:

- Vendors must train developers regularly (with a minimum of annually) using up-to-date secure coding techniques
- Delays to remediate if this is found in an ROV

#9 – PA-DSS Req. 5.1.7

Potential Impact: Low

PCI SSC Evolving Requirement

New Requirement

PCI SSC Change Comments:

- Added requirement for the PA-DSS Implementation Guide to include instructions about secure installation of patches and updates.

This means:

- Vendors must provide clear guidance to customers, and integrators/resellers on how to ensure all patches and updates are securely communicated and installed
- Delays to remediate if this is found in an ROV
- Potential impact and delays to Implementer/Operator ROC

#18 – PA-DSS Req. 12.2

Potential Impact: High

PCI SSC Evolving Requirement

New Requirement

PCI SSC Change Comments:

- New Requirement addresses multi-factor authentication for all personnel with non-console administrative access to the application. Aligns with PCI DSS Requirement 8.3.1.
- Effective immediately – not future dated

This means:

- Multi-factor authentication is now required for all administrative access to the application and/or supporting infrastructure
- Application changes may be needed to support multi-factor authentication
- Clear guidance is needed for customers, and integrators/resellers
- Customers will also need to implement this control
- Long delays to remediate if this is found in an ROV
- Potential impact and delays to Implementer/Operator ROC

#20-23, 25, 28 – PCI Implementation Guide

Potential Impact: Low

PCI SSC Clarification

Changed Requirements

PCI SSC Change Comments:

- Updated to reflect changes made to requirements, as applicable

This means:

- Vendors must update and communicate their PCI Implementation Guide
- Implementers and operators of PA-DSS applications must review guidance and potentially remediate
- Delays to remediate if this is found in an ROV
- Potential impact and delays to Implementer/Operator ROC

Recommendations

Recommendations

1. For continued compliance success, don't delay the review of PA-DSS v3.2.
   - There are new and changed items that will take time to implement
   - Minimally the PCI Implementation Guide will need to be updated and communicated

2. Conduct a gap analysis against v3.2
   - Identify any gaps and establish a remediation/implementation plan
   - Ensure plans consider the DSS v3.2 critical milestone dates

3. Engage Control Gap for support, assistance, advisory
   - With our experience, we help our customers save time and money with compliance.

References

PCI PA-DSS v3.2 References

PCI SSC Website

https://www.pcisecuritystandards.org

PCI PA-DSS v3.2

https://www.pcisecuritystandards.org/documents/PA-DSS_v3-2.pdf

PCI DSS v3.2 Summary of Changes

https://www.pcisecuritystandards.org/documents/PA-DSS_v3-2_Summary_of_Changes.pdf

Get Compliant. Stay Compliant.®

Control Gap Inc. is a privately held company, headquartered in Toronto, with hundreds of satisfied customers across North America including retail and e-commerce merchants, service providers, financial services, healthcare, government, and more. We help businesses safeguard sensitive data, reduce security risk and avoid fines. We are Canada's foremost leader in Payment Card Industry (PCI) compliance validation and advisory services, founded from decades of information security, privacy data protection, and payment industry experience.

controlgap.com