PCI DSS v3.2

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

CONTROL GAP

2016-06-08

Overview

Overview

We cover the following areas in this brief.

- What's new in PCI DSS
  - Critical milestone dates
  - Changes to the PCI DSS lifecycle
  - Scope changes [e-commerce website redirection]
- Our change analysis of DSS v3.2
- Significant impact content changes in PCI DSS v3.2
- Recommendations
- References

What's new in PCI DSS

And other news.

Critical milestone dates

PCI DSS v3.2

- PCI DSS v3.2 has arrived!
- Published April 2016
- Now the current standard in force

PCI DSS v3.1

- DSS v3.1 is being retired
- Published April 2015
- Retires on October 31, 2016
- Visa will accept PCI validation using v3.1 up to December 31, 2016.

Changes to the PCI DSS Lifecycle

In recent updates to assessor companies, the council shared:

- The DSS has matured and its maintenance will not necessitate major change
- Iterative changes will be made to address identified risks in the payment system
- Any new requirements will be future-dated to allow time for adoption

We believe this means:

- No more major 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 PCI DSS v3.1, v3.2
- Effective dates of the current version change with the release of new versions

Scope changes [e-commerce web redirection]

The PCI SSC announced in their May 2016 assessor newsletter that:

- Updates to SAQ-A, and SAQ-A-EP now have a number of increased requirements
- Updates address highly targeted merchant e-commerce web redirection servers

We believe this means:

- SAQ-A: scope impact is significant, even with the small number of requirements
  - E-commerce web redirection servers (*using iFrame or Full URL redirection*) are back in scope when using SAQ-A eligibility requirements
  - Webhosts that host these servers are now third-party service providers for req. 12.8
- SAQ–A-EP: Some new requirements to address; these servers were always in scope.
- The above applies to all entities using either SAQ or ROC for compliance validation.
- We anticipate that redirection related FAQ's will be updated to clarify the above

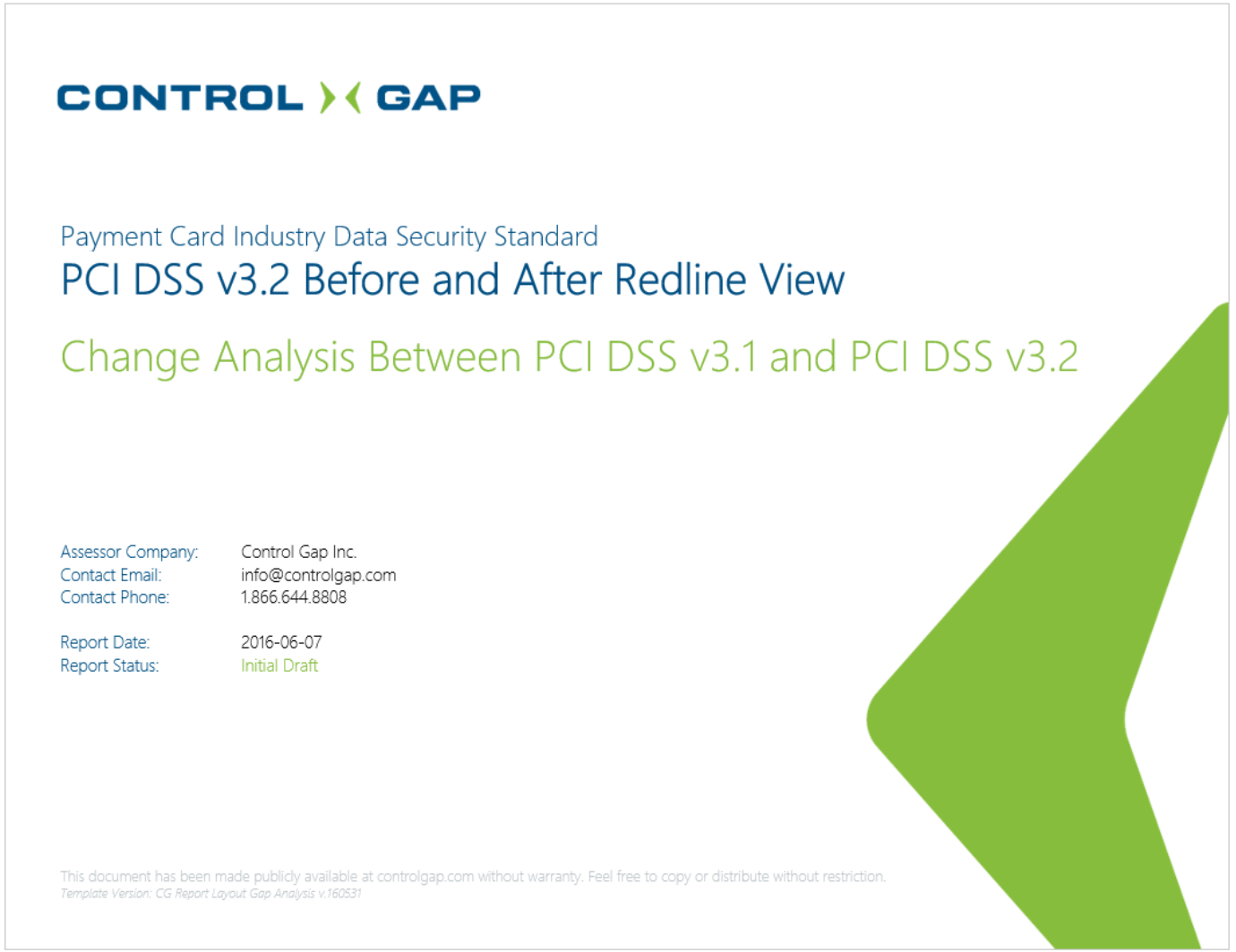
Our change analysis of DSS v3.2

Control Gap DSS v3.2 Change Analysis Companion Document

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

See our detailed change analysis companion document.

PCI 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 DSS v3.1)
- The possible impact of the changes (of 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 environments. Each entity must separately judge the actual severity of each impact.

Summary of DSS v3.2 content changes

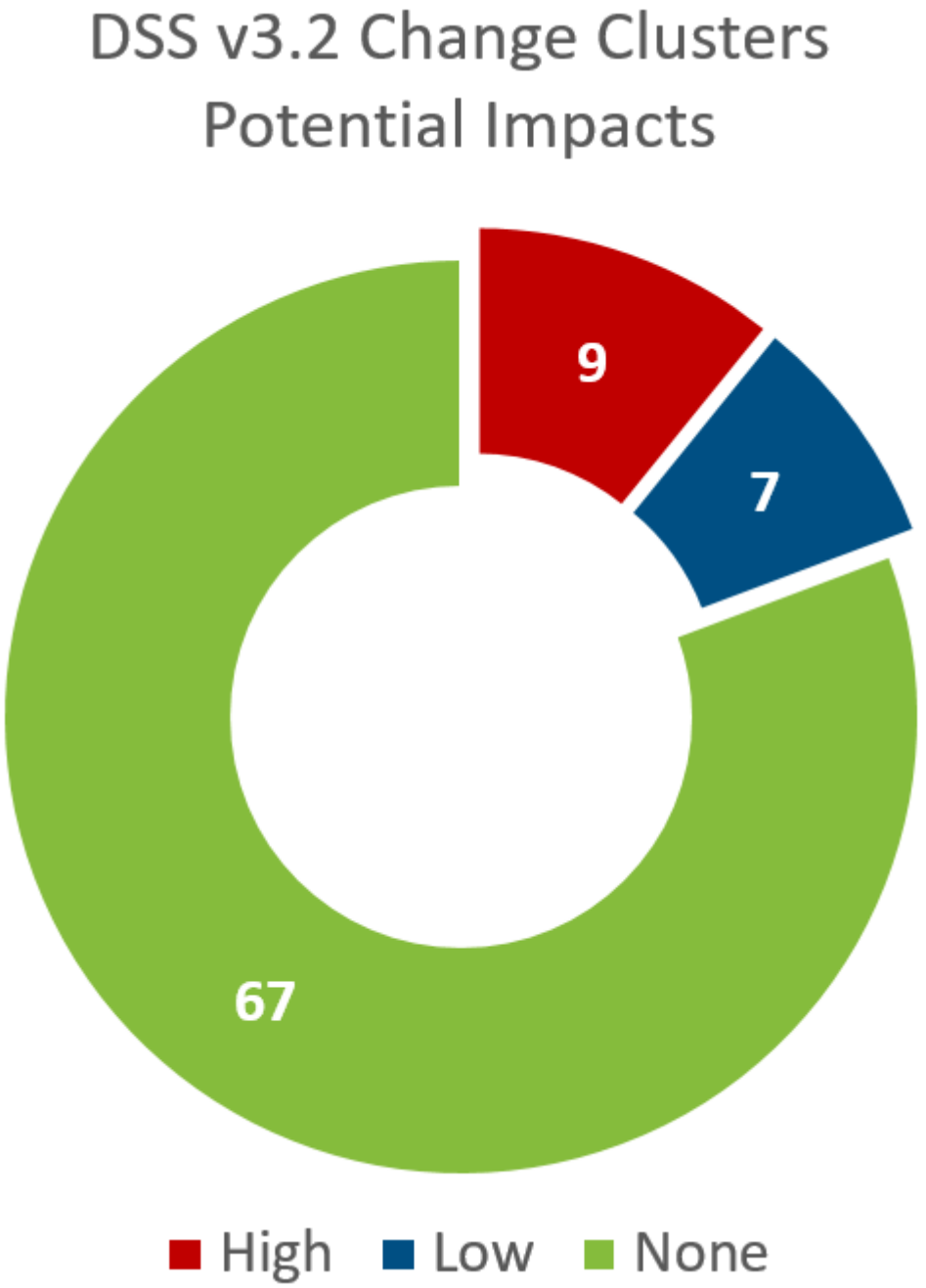
We found:

- No identified changes to scope (except those noted on slide #7)
- Thousands of wording changes
- 84 total discrete change clusters
- 14 numbering changes
- 11 evolving (new or changed) requirements
- 2 items removed
  - 1 requirement
  - 1 testing procedure

Summary of DSS v3.2 content changes

84 total discrete change clusters rated as:

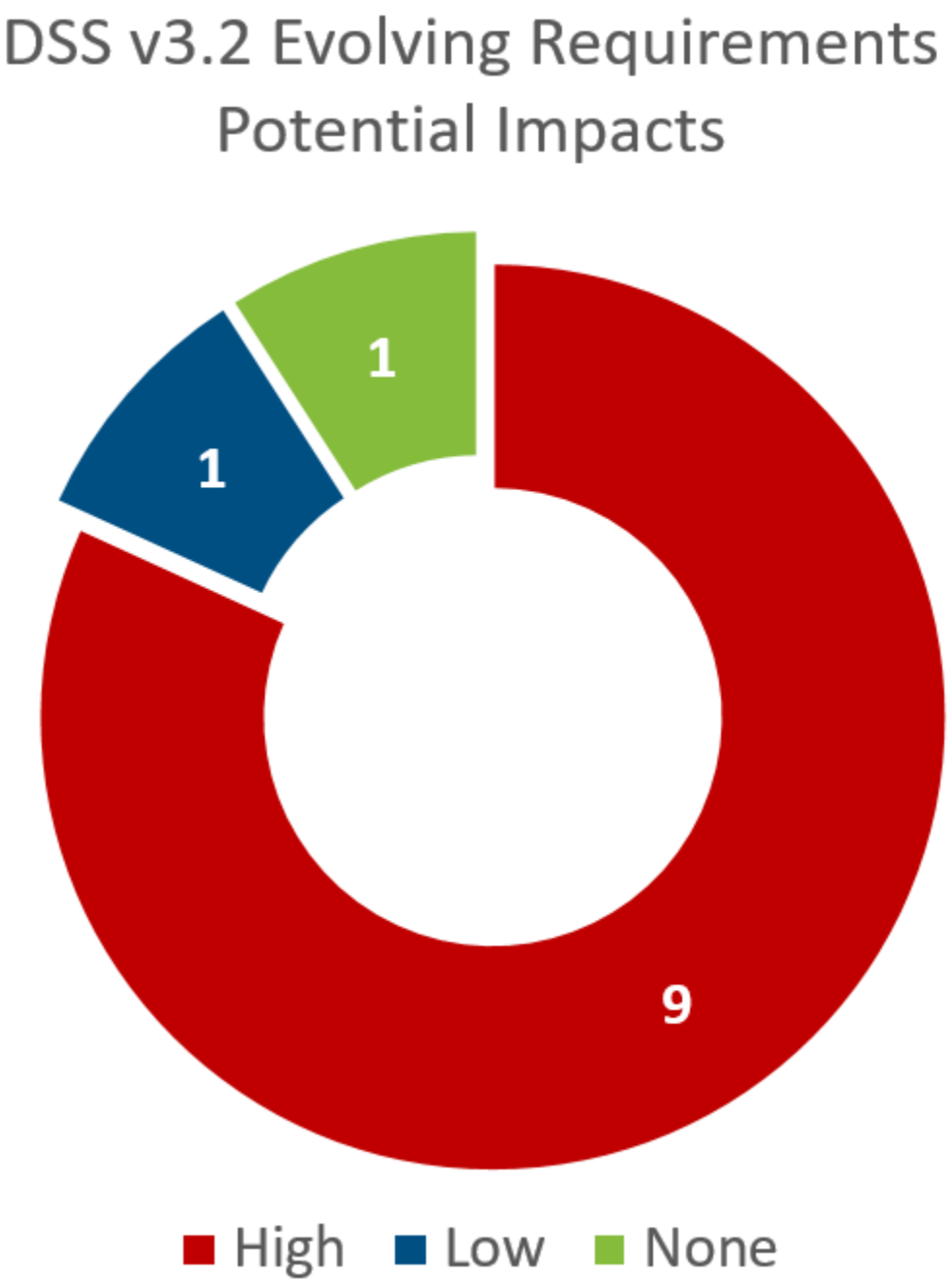
- 67 = None
- 7 = Low (#'s 7, 21, 35, 37, 68, 70, 73)
- 8 = High (#'s 24, 34, 48, 55, 56, 62, 66, 74, 75)



Summary of DSS v3.2 content changes

11 evolving requirements

- 2 existing requirements changed
  - (#'s 21, 49)
- 9 new requirements added
  - (#'s 24, 34, 48, 55, 56, 62, 66, 74, 75)
  - These are effective Feb 1, 2018



Significant (Low & High) impact content changes in DSS v3.2

Impacts of None are not covered in this document

#7 – DSS Req. 1.1.6

Potential Impact: Low

PCI SSC Clarification

Changed Requirement

PCI SSC Change Comments:

- Clarified that approval of business use is included in the justification

This means:

- Documented lists of all services, protocols, ports allowed must now also include approval(s)
- Entities may not have documented approvals in place
- Delays to remediate if this is found in a ROC

#21 – DSS Req. 3.3

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
  - Entities may not have documentation in place to authorized views of partial PAN
- Delays to remediate if this is found in a ROC

#24 – DSS Req. 3.5.1

Potential Impact: High for service providers only

PCI SSC Evolving Requirement

New Requirement

PCI SSC Change Comments:

- New requirement for service providers to maintain a documented description of the cryptographic architecture
- Effective February 1, 2018

This means:

- New detailed governance documentation is required to describe the cryptographic architecture
- Long delays to remediate if this is found in a ROC

#34 – DSS Req. 6.4.6

Potential Impact: High

PCI SSC Evolving Requirement

New Requirement

PCI SSC Change Comments:

- New requirement for change control processes to include verification of PCI DSS requirements impacted by a change
- Effective February 1, 2018

This means:

- Significant changes must be formally tracked with processes to revise and update documentation
- Maintain documentation of significant changes
- Delays to remediate if this is found in a ROC

#35, 37 – DSS Req. 6.5, 6.5.b

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:

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

#48 – DSS Req. 8.3.1

Potential Impact: High

PCI SSC Evolving Requirement

New Requirement

PCI SSC Change Comments:

- New Requirement 8.3.1 addresses multi-factor authentication for all personnel with non-console administrative access to the CDE
- Effective February 1, 2018

This means:

- Multi-factor authentication is now required for all admin personnel accessing the CDE network or individual systems in the CDE.
- We believe this will be the most challenging new requirement to implement.
- Long delays to remediate if this is found in a ROC

#55, 56 – DSS Req. 10.8, 10.8.1

Potential Impact: High for service providers only

PCI SSC Evolving Requirement

New Requirement

PCI SSC Change Comments:

- New requirement for service providers to detect and report on failures of critical security control systems
- Effective February 1, 2018

This means:

- New policy, process, procedures to detect and report failures of critical system controls
- New policy, process, procedures to respond to failures of critical system controls
- Long delays to remediate if this is found in a ROC

#62 – DSS Req. 11.3.4.1

Potential Impact: High for service providers only

PCI SSC Evolving Requirement

New Requirement

PCI SSC Change Comments:

- New requirement for service providers to perform penetration testing on segmentation controls at least every six months
- Effective February 1, 2018

This means:

- If network segmentation is used, conduct penetration testing on segmentation controls every 6 months.
- Long delays to remediate if this is found in a ROC

#66 – DSS Req. 12.4.1

Potential Impact: High for service providers only

PCI SSC Evolving Requirement

New Requirement

PCI SSC Change Comments:

- New requirement for service providers' executive management to establish responsibilities for the protection of cardholder data and a PCI DSS compliance program
- Effective February 1, 2018

This means:

- Establish accountability for maintain PCI DSS compliance
- Create a charter for a PCI DSS compliance program and communication to executive management.
- Long delays to remediate if this is found in a ROC

#68 – DSS Req. 12.6

Potential Impact: Low

PCI SSC Clarification

Changed Requirement

PCI SSC Change Comments:

- Clarified intent of security awareness program is to ensure personnel are aware of the cardholder data security policy and procedures

This means:

- As part of annual security awareness training, entities must train personnel on cardholder data security policies and procedures
  - Previously this requirement specified training on "the importance of cardholder data"
- Some entities may need to change existing training
- Long delays to remediate if this is found in a ROC

#70 – DSS Req. 12.8.1

Potential Impact: Low

PCI SSC Clarification

Changed Requirement

PCI SSC Change Comments:

- Clarified that the list of service providers includes a description of the service provided

This means:

- Inventories of service providers must include a description of the service provided by each service provider
- Entities may not have this documentation in place
- Delays to remediate if this is found in a ROC

#73 – DSS Req. 12.10.2

Potential Impact: Low

PCI SSC Clarification

Changed Requirement

PCI SSC Change Comments:

- Clarified that review of the incident response plan encompasses all elements listed in Requirement 12.10.1.

This means:

- Review and test the incident response plan annually in accordance with all items specified in 12.10.1
- Entities may not have this process or the necessary evidence artifacts in place.
- Delays to remediate if this is found in a ROC

#74, 75 – DSS Req. 12.11, 12.11.1

Potential Impact: High for service providers only

PCI SSC Evolving Requirement

New Requirements

PCI SSC Change Comments:

- New requirements for service providers to perform reviews at least quarterly, to confirm personnel are following security policies and operational procedures
- Effective February 1, 2018

This means:

- Conduct quarterly reviews to confirm personnel are following security policies and operational procedures.
- Maintain documentation of quarterly review processes.
- Long delays to remediate if this is found in a ROC

Recommendations

Recommendations

1. For continued compliance success, don't delay the review of v3.2.
   - There are many new and changed items that will take time to implement.

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 DSS v3.2 References

PCI SSC Website

https://www.pcisecuritystandards.org

PCI DSS v3.2

https://www.pcisecuritystandards.org/documents/PCI_DSS_v3-2.pdf

PCI Self-Assessment Questionnaires (SAQ)

https://www.pcisecuritystandards.org/document_library?category=saqs

PCI DSS v3.2 Summary of Changes

https://www.pcisecuritystandards.org/documents/PCI_DSS_v3-2_Summary_of_Changes.pdf

CONTROL GAP

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