PCI DSS v3.0

Control Gap Commentary on the Changes to the PCI Data Security Standard v3.0

CONTROL | GAP

2013-11-13

Get Compliant. Stay Compliant.®

Changes outlined by the PCI SSC

The Summary of Changes Document – PCI DSS v2.0 to v3.0

Clarifications

- Concise wording to convey desired intent of requirements

Additional Guidance

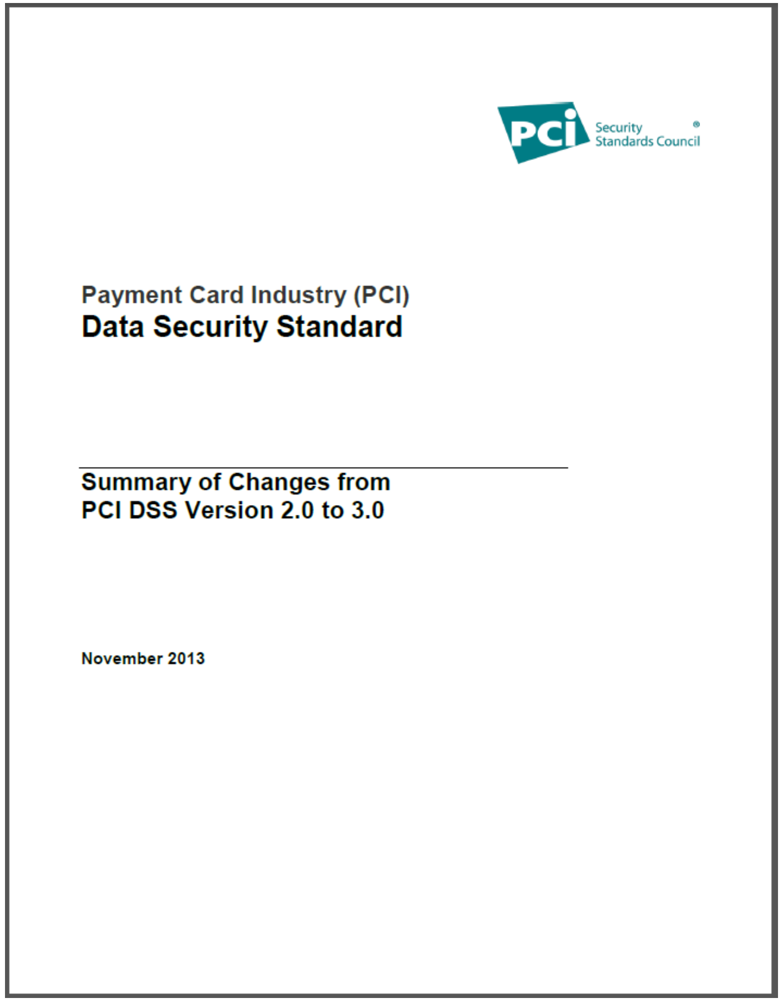
- Explanation, definition and/or instruction to increase understanding or provide further guidance on a topic

Evolving Requirements

- Change to ensure the standards are up to date with emerging threats and changes in the market

Note: The PCI SSC summary document is high-level and does not convey the volume or impact of changes in DSS v3.0

https://www.pcisecuritystandards.org/documents/PCI_DSS_v3_Summary_of_Changes.pdf



PCI Security Standards Council®

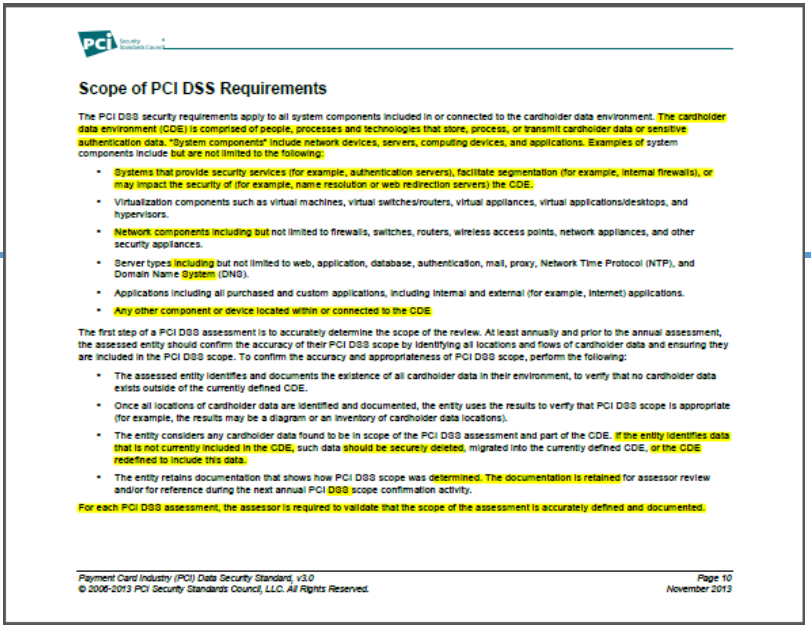
Payment Card Industry (PCI)
Data Security Standard

**Summary of Changes from
PCI DSS Version 2.0 to 3.0**

November 2013

PCI DSS v3.0 - Observed Changes

- Average of 17% increase in size from v2.0 to v3.0
- Thousands of wording changes throughout DSS v3.0
- Changes/Clarifications affecting validation scope
- Numerous re-organized and re-numbered items
  - Complex requirements have been separated
  - A few redundant/overlapping items were removed
- New Requirements requiring additional effort
- New Testing Procedures requiring added validation
  - Jan 2014 – QSA's expect a new validation reporting method with focus on increased validation detail and less writing
  - Jan 2014 – QSA's expect v3.0 ROC Reporting Instructions



Scope of PCI DSS Requirements

The PCI DSS security requirements apply to all system components included in or connected to the cardholder data environment. The cardholder data environment (CDE) is comprised of people, processes and technologies that store, process, or transmit cardholder data or sensitive authentication data. "System components" include network devices, servers, computing devices, and applications. Examples of system components include but are not limited to the following:

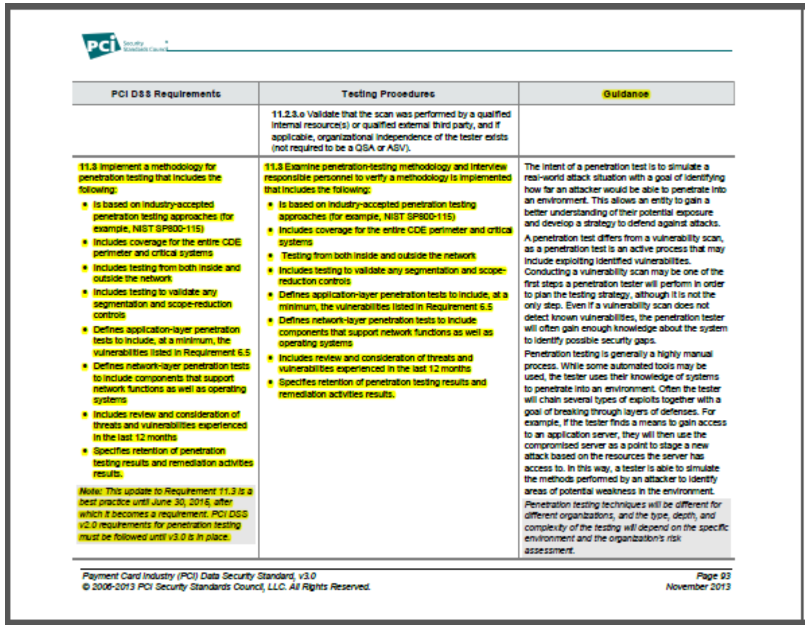
- Systems that provide security services (for example, authentication servers), facilitate segmentation (for example, internal firewalls), or may impact the security of (for example, name resolution or web redirection servers) the CDE.
- Virtualization components such as virtual machines, virtual switches/routers, virtual appliances, virtual applications/desktops, and hypervisors.
- Network components including but not limited to firewalls, switches, routers, wireless access points, network appliances, and other security appliances.
- Server types including but not limited to web, application, database, authentication, mail, proxy, Network Time Protocol (NTP), and Domain Name System (DNS).
- Applications including all purchased and custom applications, including internal and external (for example, Internet) applications.
- Any other component or device located within or connected to the CDE

The first step of a PCI DSS assessment is to accurately determine the scope of the review. At least annually and prior to the annual assessment, the assessed entity should confirm the accuracy of their PCI DSS scope by identifying all locations and flows of cardholder data and ensuring they are included in the PCI DSS scope. To confirm the accuracy and appropriateness of PCI DSS scope, perform the following:

- The assessed entity identifies and documents the existence of all cardholder data in their environment, to verify that no cardholder data exists outside of the currently defined CDE.
- Once all locations of cardholder data are identified and documented, the entity uses the results to verify that PCI DSS scope is appropriate (for example, the results may be a diagram or an inventory of cardholder data locations).
- The entity considers any cardholder data found to be in scope of the PCI DSS assessment and part of the CDE. If the entity identifies data that is not currently included in the CDE, such data should be securely deleted, migrated into the currently defined CDE, or the CDE redefined to include this data.
- The entity retains documentation that shows how PCI DSS scope was determined. The documentation is retained for assessor review and/or for reference during the next annual PCI DSS scope confirmation activity.

For each PCI DSS assessment, the assessor is required to validate that the scope of the assessment is accurately defined and documented.

Payment Card Industry (PCI) Data Security Standard, v3.0 *Page 10*
© 2006-2013 PCI Security Standards Council, LLC. All Rights Reserved. *November 2013*



PCI DSS Requirements	Testing Procedures	Guidance
	11.2.3.c Validate that the scan was performed by a qualified internal resource(s) or qualified external third party, and if applicable, organizational independence of the tester exists (not required to be a QSA or ASV).	
11.3 Implement a methodology for penetration testing that includes the following: • Is based on industry-accepted penetration testing approaches (for example, NIST SP800-115) • Includes coverage for the entire CDE perimeter and critical systems • Includes testing from both inside and outside the network • Includes testing to validate any segmentation and scope-reduction controls • Defines application-layer penetration tests to include, at a minimum, the vulnerabilities listed in Requirement 6.5 • Defines network-layer penetration tests to include components that support network functions as well as operating systems • Includes review and consideration of threats and vulnerabilities experienced in the last 12 months • Specifies retention of penetration testing results and remediation activities results. *Note: This update to Requirement 11.3 is a best practice until June 30, 2015, after which it becomes a requirement. PCI DSS v2.0 requirements for penetration testing must be followed until v3.0 is in place.*	11.3 Examine penetration-testing methodology and interview responsible personnel to verify a methodology is implemented that includes the following: • Is based on industry-accepted penetration testing approaches (for example, NIST SP800-115) • Includes coverage for the entire CDE perimeter and critical systems • Testing from both inside and outside the network • Includes testing to validate any segmentation and scope-reduction controls • Defines application-layer penetration tests to include, at a minimum, the vulnerabilities listed in Requirement 6.5 • Defines network-layer penetration tests to include components that support network functions as well as operating systems • Includes review and consideration of threats and vulnerabilities experienced in the last 12 months • Specifies retention of penetration testing results and remediation activities results.	The intent of a penetration test is to simulate a real-world attack situation with a goal of identifying how far an attacker would be able to penetrate into an environment. This allows an entity to gain a better understanding of their potential exposure and develop a strategy to defend against attacks. A penetration test differs from a vulnerability scan, as a penetration test is an active process that may include exploiting identified vulnerabilities. Conducting a vulnerability scan may be one of the first steps a penetration tester will perform in order to plan the testing strategy, although it is not the only step. Even if a vulnerability scan does not detect known vulnerabilities, the penetration tester will often gain enough knowledge about the system to identify possible security gaps. Penetration testing is generally a highly manual process. While some automated tools may be used, the tester uses their knowledge of systems to penetrate into an environment. Often the tester will chain several types of exploits together with a goal of breaking through layers of defenses. For example, if the tester finds a means to gain access to an application server, they will then use the compromised server as a point to stage a new attack based on the resources the server has access to. In this way, a tester is able to simulate the methods performed by an attacker to identify areas of potential weakness in the environment. *Penetration testing techniques will be different for different organizations, and the type, depth, and complexity of the testing will depend on the specific environment and the organization's risk assessment.*

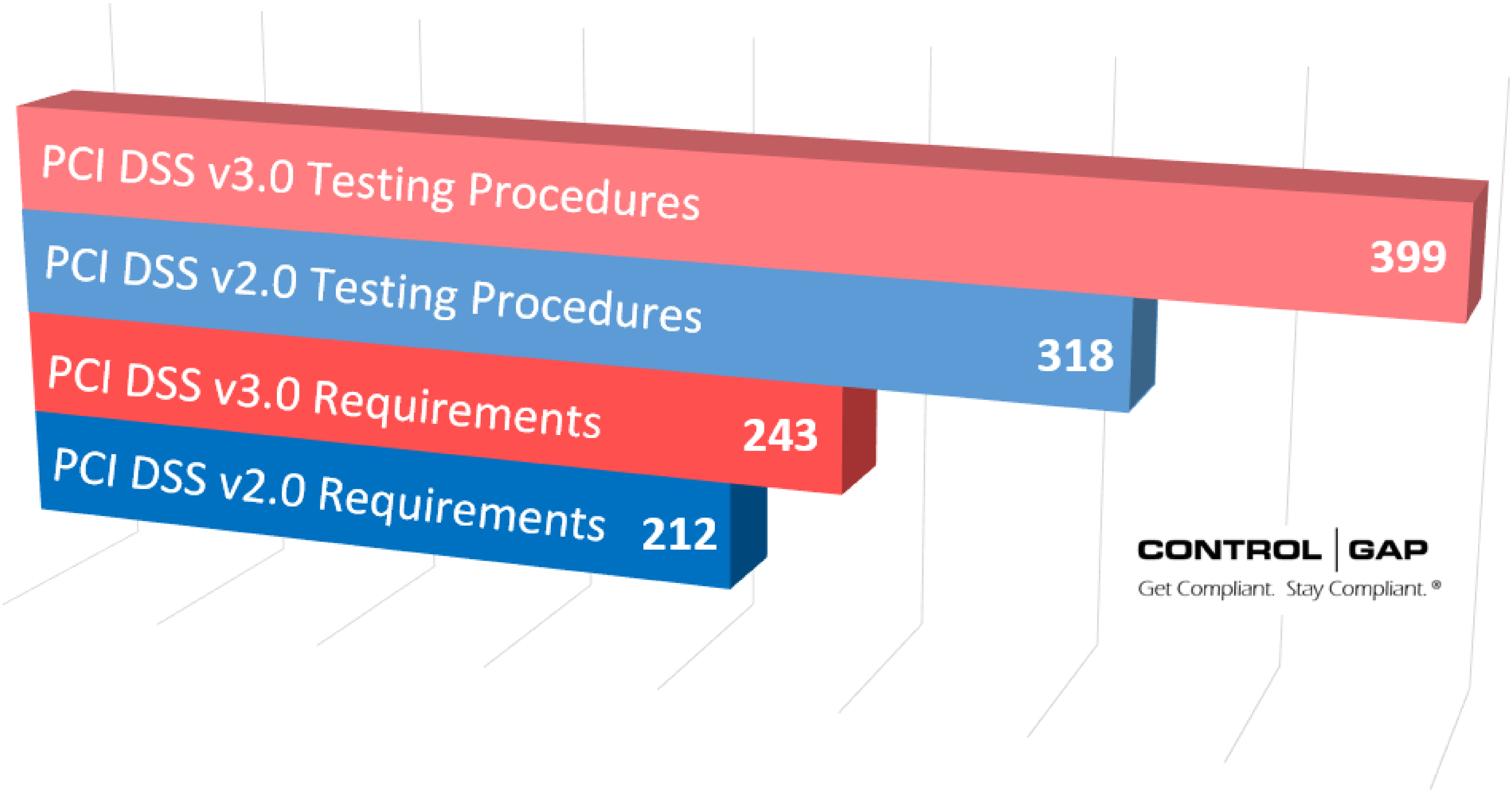
Payment Card Industry (PCI) Data Security Standard, v3.0 *Page 93*
© 2006-2013 PCI Security Standards Council, LLC. All Rights Reserved. *November 2013*

PCI DSS v2.0 vs. v3.0 Statistics

PCI DSS	DSS Requirements	DSS Testing Procedures	DSS Reporting Instructions
DSS v2.0 (75 Pages)	**212***	**318***	**1031***
DSS v3.0 (112 Pages)	**243*** (~14% increase)	**399*** (~25% increase)	TBD Jan 2014
Content Changes	**7** Items Removed **38** Items Added • **17** New Re-Organized Items Added • **21** Brand-New Items Added	**21** Items Removed **102** Items Added • **64** New Re-Organized Items Added • **38** Brand-New Items Added	TBD Jan 2014
Numbering Changes	**56** Items Re-numbered	**122** Items Re-numbered	n/a

*Amounts above do not include Items in Appendix A of the PCI DSS.

PCI DSS v2.0 vs V3.0 Number of Requirements and Testing Procedures



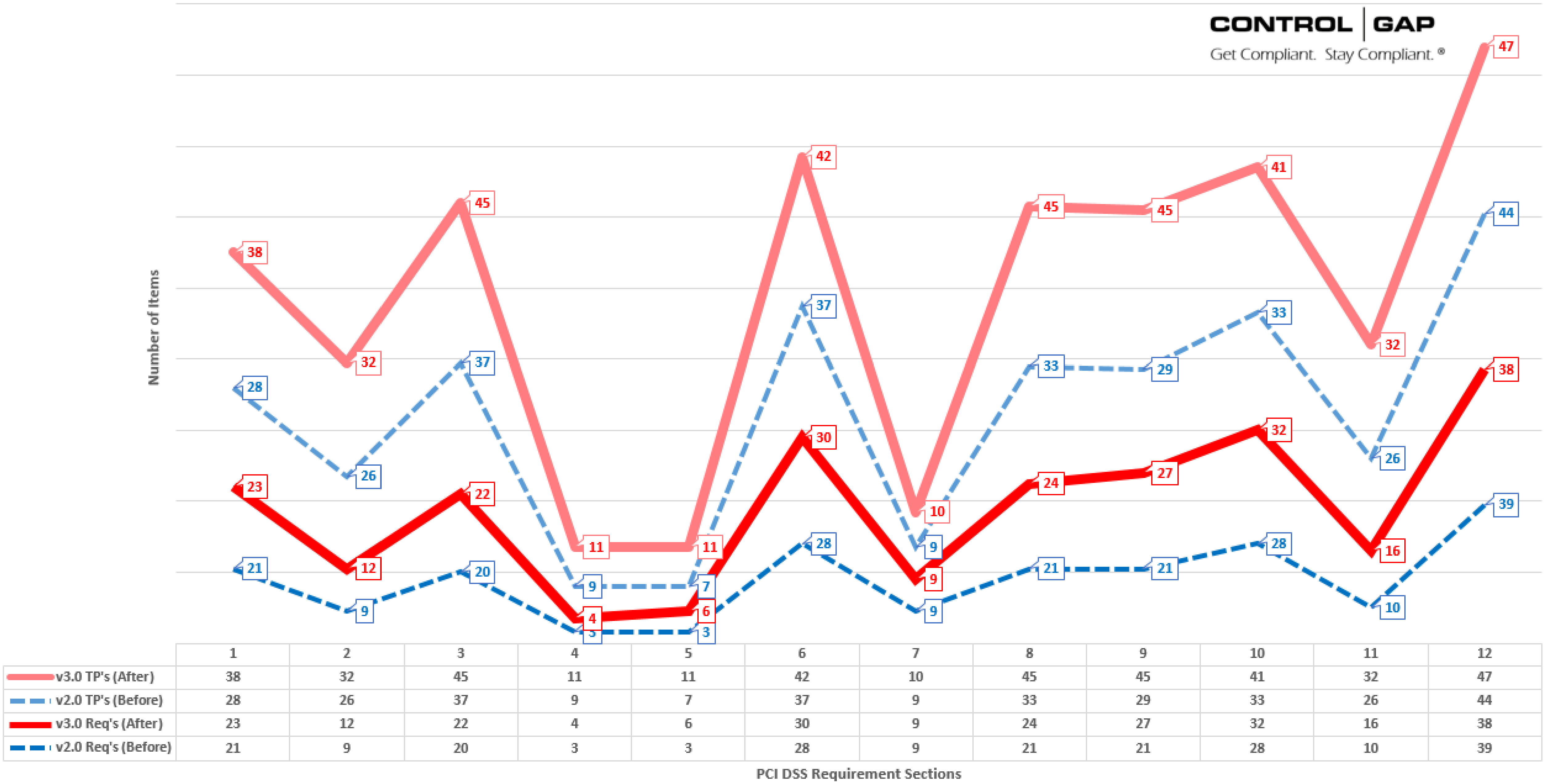
CONTROL | GAP

Get Compliant. Stay Compliant.®

PCI DSS v2.0 vs V3.0 Number of Requirements and Testing Procedures

CONTROL | GAP

Get Compliant. Stay Compliant.®



	1	2	3	4	5	6	7	8	9	10	11	12
v3.0 TP's (After)	38	32	45	11	11	42	10	45	45	41	32	47
v2.0 TP's (Before)	28	26	37	9	7	37	9	33	29	33	26	44
v3.0 Req's (After)	23	12	22	4	6	30	9	24	27	32	16	38
v2.0 Req's (Before)	21	9	20	3	3	28	9	21	21	28	10	39

Analysis of Change-Severity

- Our change analysis has outlined many changes between DSS v2.0 and v3.0.
- Each item (a Requirement or Testing Procedure) has been assigned a change-severity label representing our initial subjective interpretation of the change.

Change-Severity Legend:

Removed - Item was removed (item content might be re-organized into other items)

Unchanged - Item content appears to be unchanged (no words added/removed)

Clarified - Item with words added/removed (same effective meaning to a QSA)

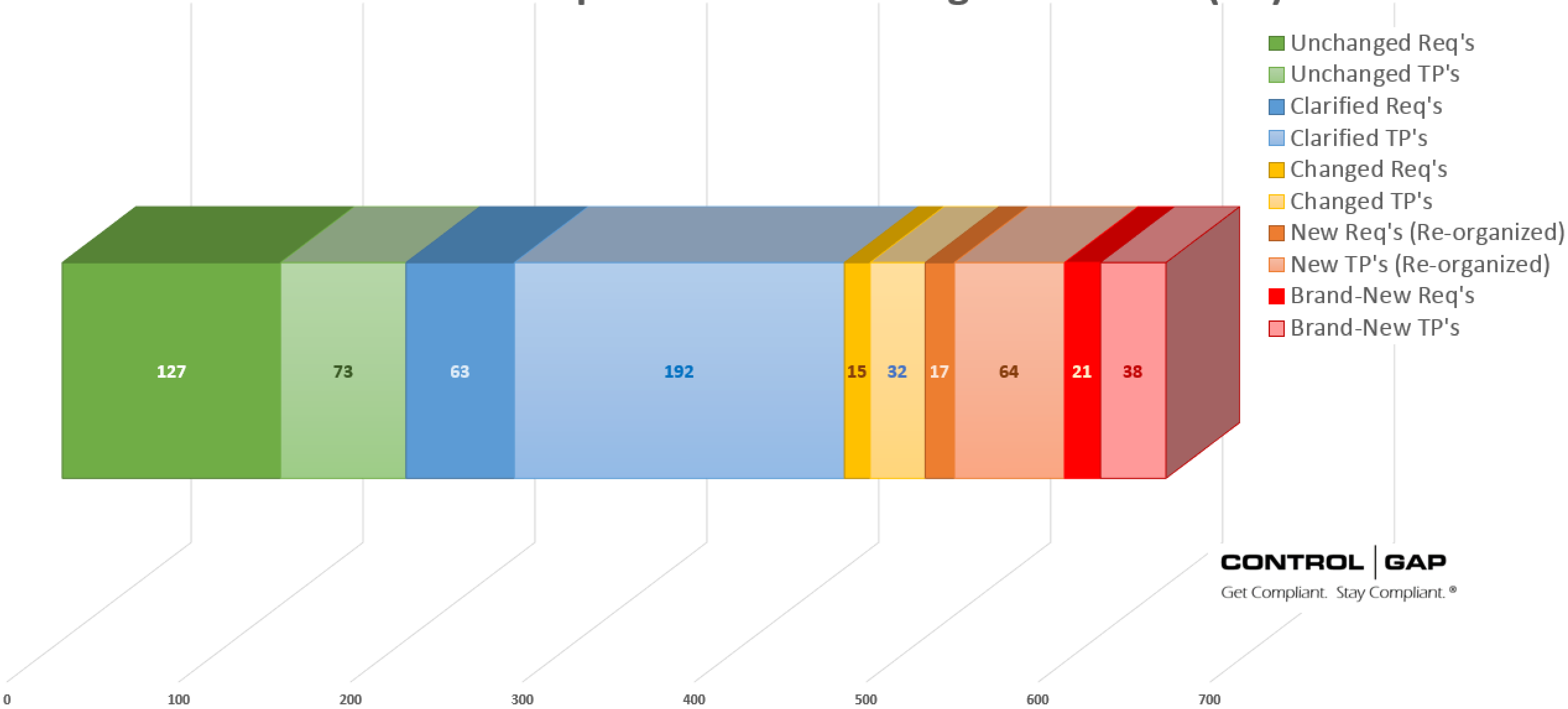
Changed - Intent of an item changed (scope impacting new/changed meaning)

New (Re-Organized) - The row is new with re-organized content or RI-type content

Brand-New - Item is a new row and appears to be brand new

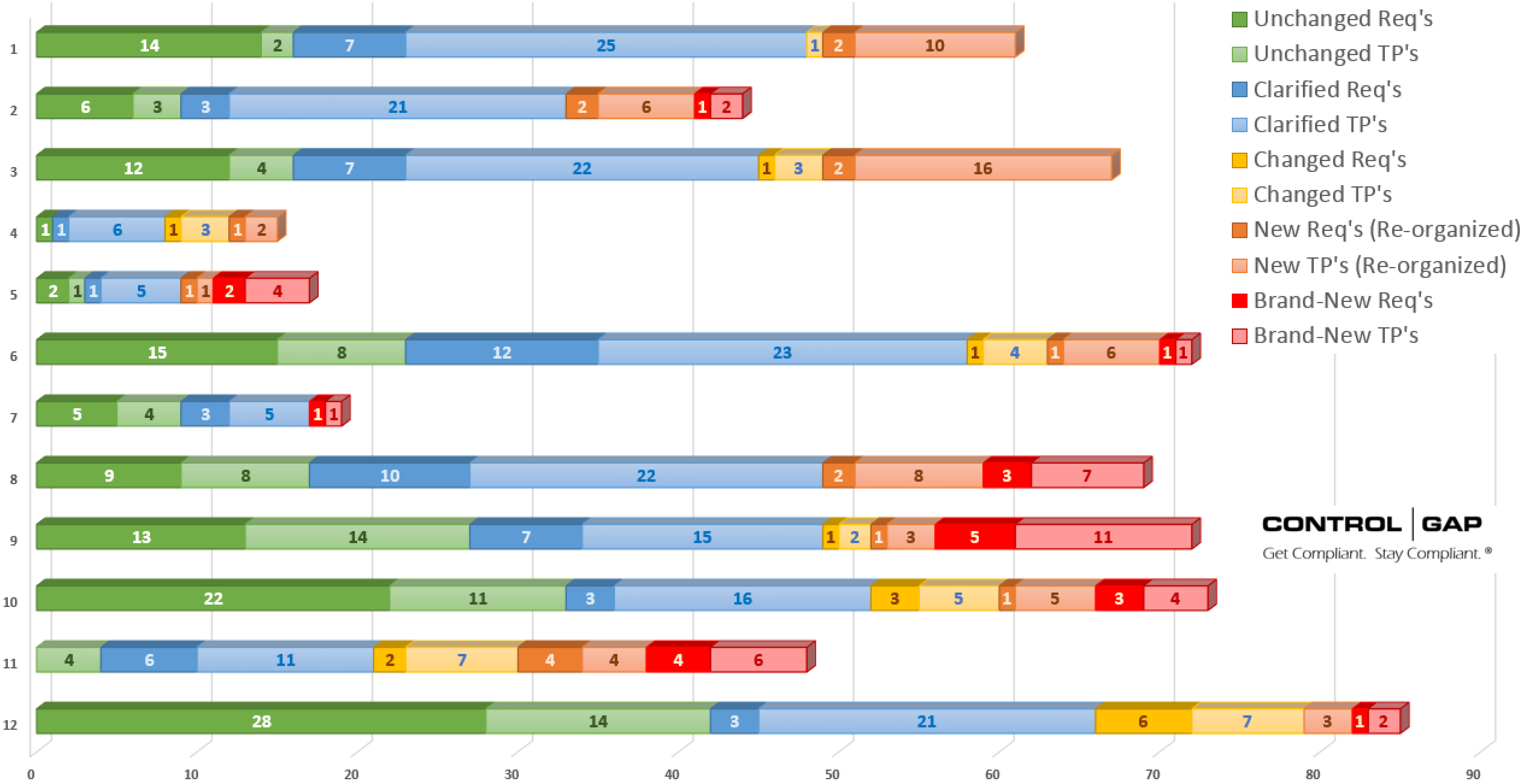
Note: There are numerous re-numbering changes that have not been labelled as a content change in the above.

DSS v3.0 vs v2.0 Requirements & Testing Procedures (All)



CONTROL GAP
Get Compliant. Stay Compliant.®

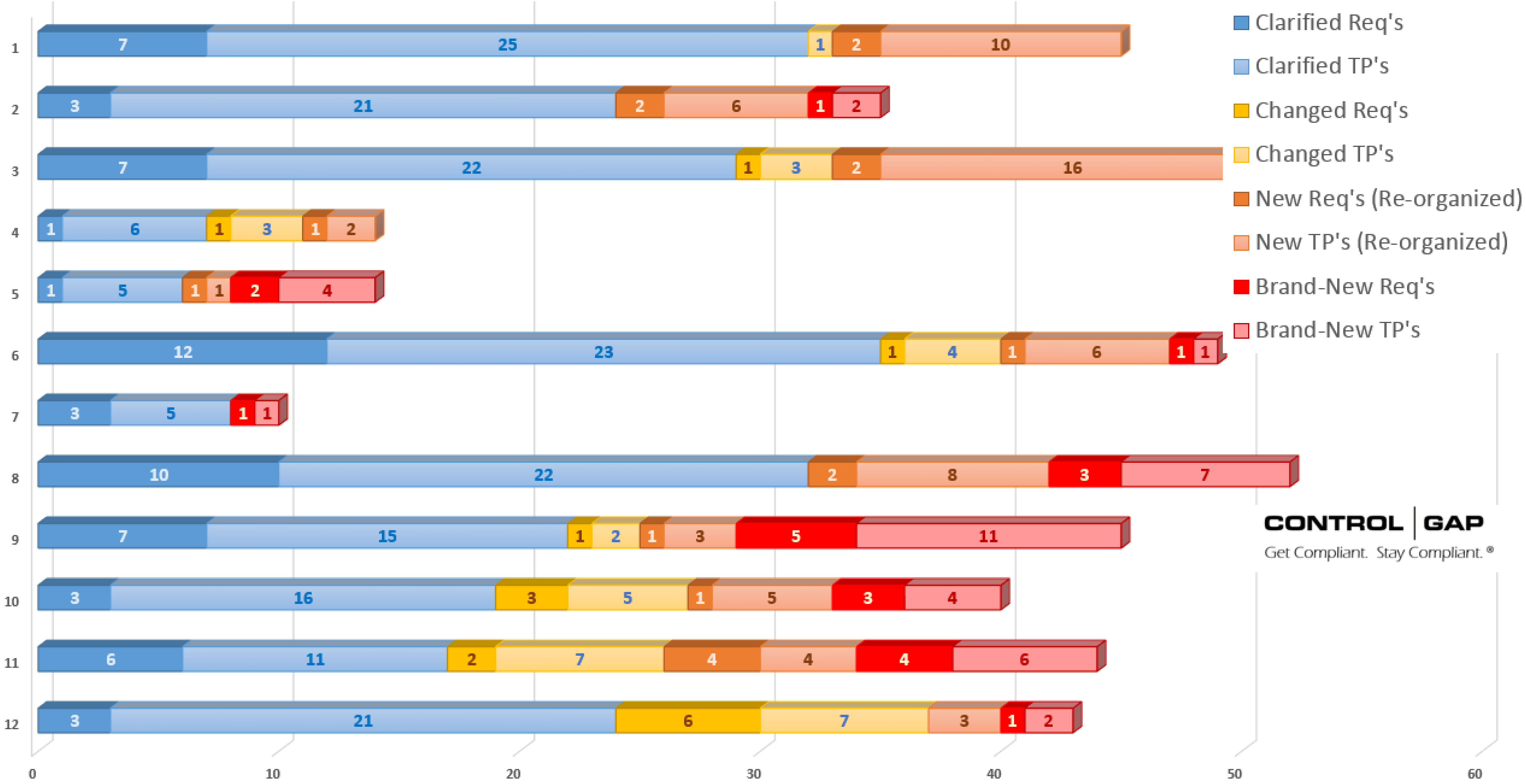
DSS v3.0 vs v2.0 Requirements & Testing Procedures (All)



CONTROL | GAP

Get Compliant. Stay Compliant.®

DSS v3.0 vs v2.0 Requirements & Testing Procedures (Changes)



CONTROL | GAP

Get Compliant. Stay Compliant.®

PCI DSS v3.0 Exec Summary Significant Changes/Clarifications

- (Pg.7) – Clarified - All entities involved in the payment card processing are in scope.
- (Pg.7, 12) Clarified - Organizations outsourcing to third-parties remain responsible for ensuring the third-parties protect account data (and system components) in accordance with all applicable PCI requirements. Some PCI requirements may still be applicable to the original organization.
- (Pg.12) New – Organizations and third-parties must clearly identify the system components and PCI Requirements in scope for the third-party service provider's PCI compliance assessment, and any responsibilities and PCI Requirements for the original organization.
- (Pg.12) New – Third-party service providers conducting an independent PCI assessment should provide sufficient evidence to their customers to verify that the scope of the assessment covered the services applicable to the customer and that the relevant PCI DSS requirements were examined and determined to be in place.

PCI DSS v3.0 Exec Summary Significant Changes/Clarifications (Cont'd)

- (Pg.8) Clarified – Sensitive authentication data (SAD) must not be stored after authorization, including where no PAN is present in the environment.
- (Pg.8) New – Confirm with your acquiring bank if sensitive authentication data (SAD) is permitted to be stored prior to authorization, for how long, and any related usage and protection requirements.
- (Pg.9) Clarified – All applications that store, process or transmit cardholder data are in scope for PCI, including PA-DSS validated applications.

PCI DSS v3.0 Exec Summary Significant Changes/Clarifications (Cont'd)

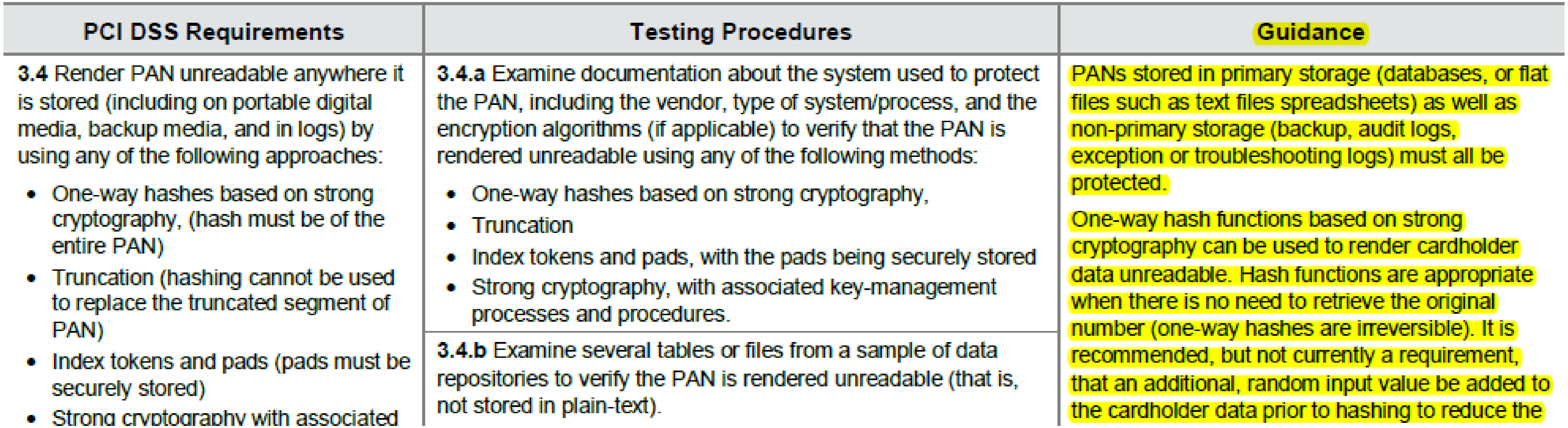
- (Pg.10) New - Any system component that provides security services, network segmentation, or that can impact the security of the CDE is in scope.
  - Security Services (e.g. Authentication servers, etc.)
  - Facilitate Segmentation (e.g. Internal firewalls/routers, etc.)
  - Security Impacting (e.g. Name Resolution, Web Redirection Servers, etc.)
  - Any other component or device located within or connected to the CDE, etc.
- (Pg.11) New – To determine systems out of scope via network segmentation, the systems must not impact the security of the CDE, even if compromised.

PCI DSS v3.0 Exec Summary Significant Changes/Clarifications (Cont'd)

- (Pg.13) New Guidance – Best Practices for Implementing PCI DSS into Business-as-Usual Processes.
- (Pg.14) Clarification – Sampling of system components must be representative of every type and combination in use.

PCI DSS v3.0 Layout & Appearance Changes

- (Pg.18+) New – Layout of PCI DSS Requirements tables have changed to now include guidance from the PCI DSS Navigating document.
  - In-place, not in place, comments columns have been removed.
  - A new separate reporting template will be used for Reports on Compliance.



PCI DSS Requirements	Testing Procedures	Guidance
3.4 Render PAN unreadable anywhere it is stored (including on portable digital media, backup media, and in logs) by using any of the following approaches: • One-way hashes based on strong cryptography, (hash must be of the entire PAN) • Truncation (hashing cannot be used to replace the truncated segment of PAN) • Index tokens and pads (pads must be securely stored) • Strong cryptography with associated	**3.4.a** Examine documentation about the system used to protect the PAN, including the vendor, type of system/process, and the encryption algorithms (if applicable) to verify that the PAN is rendered unreadable using any of the following methods: • One-way hashes based on strong cryptography, • Truncation • Index tokens and pads, with the pads being securely stored • Strong cryptography, with associated key-management processes and procedures.	PANs stored in primary storage (databases, or flat files such as text files spreadsheets) as well as non-primary storage (backup, audit logs, exception or troubleshooting logs) must all be protected. One-way hash functions based on strong cryptography can be used to render cardholder data unreadable. Hash functions are appropriate when there is no need to retrieve the original number (one-way hashes are irreversible). It is recommended, but not currently a requirement, that an additional, random input value be added to the cardholder data prior to hashing to reduce the
	3.4.b Examine several tables or files from a sample of data repositories to verify the PAN is rendered unreadable (that is, not stored in plain-text).	

PCI DSS v3.0 Requirements & Testing Procedures Brand-New Items

- 2.4 (2.4.a-2.4.b) – Maintain an inventory of system components in scope for PCI DSS.
- 5.1.2 – For systems not commonly affected by malware, evaluate evolving threats and the need for Anti-Virus.
- 5.3 (5.3.a - 5.3.c) – Ensure Anti-Virus is actively running.
- *6.5.10 - Secure Coding - Broken Authentication and Session Mgmt.
- 7.1.1 – Access Control – Define access needs for each role.
- 8.1 (8.1.a - 8.1.b) – ID Management Policies & Procedures
- *8.5.1 - Service Providers with remote access to customer premises - use a unique authentication credential for each customer.

* These items are best practice until June 30, 2015

PCI DSS v3.0 Requirements & Testing Procedures Brand-New Items (Cont'd)

- 8.6 (8.6.a – 8.6.c) - "Other" authentication mechanisms (like tokens or certificates) must be assigned to individual accounts and not shared.
- 9.3 (9.3.a – 9.3.c) - Control physical access for onsite personnel - access based on individual job function; access revoked immediately upon termination.
- *9.9 - Payment Devices - Protect devices that capture payment card data via direct physical interaction with the card from tampering and substitution.
- *9.9.1 (9.9.1.a – 9.9.1.c) - Payment Devices - Maintain an inventory (make, model, location, serial, other)

* These items are best practice until June 30, 2015

PCI DSS v3.0 Requirements & Testing Procedures Brand-New Items (Cont'd)

- *9.9.2 (9.9.2.a – 9.9.2.b) - Payment Devices - Periodically inspect device surfaces to detect tampering.
- *9.9.3 (9.9.3.a – 9.9.3.b) - Payment Devices - Provide training for personnel to be aware of attempted tampering or replacement of devices.
- 10.6.2 (10.6.2.a – 10.6.2.b) - Review Logs - of all "other" system components periodically.
- 10.6.3 (10.6.3.a – 10.6.3.b) - Review Logs - follow-up on identified exceptions and anomalies
- 11.1.1 - Maintain an inventory of authorized wireless access points

* These items are best practice until June 30, 2015

PCI DSS v3.0 Requirements & Testing Procedures Brand-New Items (Cont'd)

- 11.1.2.b - Verify action is taken by personnel to respond to unauthorized access points that have been identified.
- *11.3 - Implement a methodology for penetration testing
- 11.3.4 (11.3.4.a – 11.3.4.b) – If network segmentation is used - validate segmentation effectiveness as part of penetration testing.
- 11.5.1 – Change-Detection Mechanism - implement a process to respond to alerts.

* These items are best practice until June 30, 2015

PCI DSS v3.0 Requirements & Testing Procedures Brand-New Items (Cont’d)

- 12.8.5 - Outsourcing to third-parties - maintain info about which requirements are managed by the service provider and which are managed by the entity.
- *12.9 - Service Providers must acknowledge in writing to customers that they are responsible for security of CHD, systems and otherwise where they can impact the security of the CDE.

* These items are best practice until June 30, 2015

Recommendations

1. For continued compliance success, don’t delay review and adoption of v3.0.
   - There are many changes and new items that will take time to implement.
   - Review the changes in the DSS executive summary affecting scope
   - Review the changes in the DSS Requirements and Testing Procedures

2. Review existing PCI Cardholder Data Environment (CDE) scope against v3.0
   - Confirm scope and update the list of in-scope system components for the CDE.

3. Conduct a Gap Analysis of the system components and CDE for v3.0
   - Identify any gaps and establish a remediation/implementation plan
     - Ensure plans consider the DSS v3.0 critical milestone dates on the following slide

4. Engage Control Gap for support, assistance, advisory – we are here to help.

PCI DSS v3.0 Milestone Dates

PCI DSS v2.0

- **2014-1-1** – Companies can optionally validate against v2.0 or v3.0
- **2014-12-31** –v2.0 expires and must not be used for validation

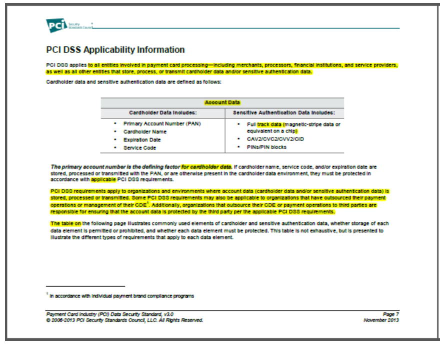
PCI DSS v3.0

- **2013-11-7** – Public release of PCI DSS v3.0
- **2014-1-1** – Companies can optionally validate against v2.0 or v3.0
  - Updated tools from PCI SSC are anticipated in January 2014. or later (E.g. ROC Reporting Instructions, Prioritized Approach, Self-Assessment Questionnaires, etc.)
- **2015-1-1** – Companies must use v3.0 for compliance validation
- **2015-7-1** – Best practice items become mandatory for compliance validation
  - DSS Requirements - 6.5.10, 8.5.1, 9.9, 11.3, 12.9

Control Gap Resources for DSS v3.0

PCI_DSS_v3.annotated changes.pdf

- Highlighted in yellow are all identified additions/changes made to DSS v3.0 vs. v2.0.



PCI DSS Applicability Information

PCI DSS applies to all entities involved in payment card processing—including merchants, processors, financial institutions, and service providers, as well as all other entities that store, process, or transmit cardholder data and/or sensitive authentication data.

Cardholder data and sensitive authentication data are defined as follows:

Account Data	
Cardholder Data includes:	**Sensitive Authentication Data includes:**
• Primary Account Number (PAN) • Cardholder Name • Expiration Date • Service Code	• Full track data (magnetic-stripe data or equivalent on a chip) • CAV2/CVC2/CVV2/CID • PINs/PIN blocks

The primary account number is the defining factor for cardholder data. If cardholder name, service code, and/or expiration date are stored, processed or transmitted with the PAN, or are otherwise present in the cardholder data environment, they must be protected in accordance with applicable PCI DSS requirements.

PCI DSS requirements apply to organizations and environments where account data (cardholder data and/or sensitive authentication data) is stored, processed or transmitted. Some PCI DSS requirements may also be applicable to organizations that have outsourced their payment operations or management of their CDE[1]. Additionally, organizations that outsource their CDE or payment operations to third parties are responsible for ensuring that the account data is protected by the third party per the applicable PCI DSS requirements.

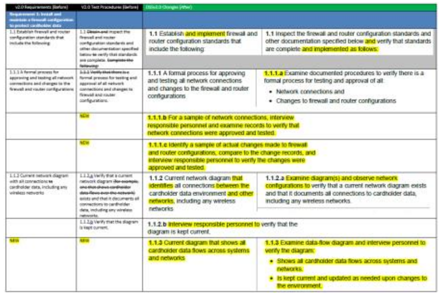
The table on the following page illustrates commonly used elements of cardholder and sensitive authentication data, whether storage of each data element is permitted or prohibited, and whether each data element must be protected. This table is not exhaustive, but is presented to illustrate the different types of requirements that apply to each data element.

[1] In accordance with individual payment brand compliance programs

Payment Card Industry (PCI) Data Security Standard, v3.0 *Page 7*
© 2006-2013 PCI Security Standards Council, LLC. All Rights Reserved. *November 2013*

PCI DSS v3 vs v2 Changes Grid.pdf

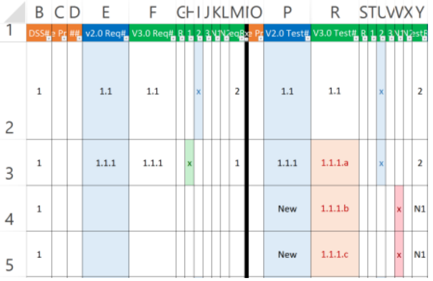
- A row-by-row mapping of PCI DSS v2.0 to v3.0 Requirements and Testing Procedures content.
  - Deletions from DSS v2.0 are noted with strike-through text
  - Additions to DSS v3.0 are noted with the yellow-highlighted snippits



v2.0 Requirements (Before)	V2.0 Test Procedures (Before)	DSSv3.0 Changes (After)	
Requirement 1: Install and maintain a firewall configuration to protect cardholder data			
1.1 Establish firewall and router configuration standards that include the following:	1.1 ~~Obtain and~~ inspect the firewall and router configuration standards and other documentation specified below ~~to~~ verify that standards are complete. ~~Complete the following:~~	**1.1** Establish and implement firewall and router configuration standards that include the following:	**1.1** Inspect the firewall and router configuration standards and other documentation specified below and verify that standards are complete and implemented as follows:
1.1.1 A formal process for approving and testing all network connections and changes to the firewall and router configurations	~~1.1.1 Verify that there is a~~ formal process for testing and approval of all network connections and changes to firewall and router configurations.	**1.1.1** A formal process for approving and testing all network connections and changes to the firewall and router configurations	**1.1.1.a** Examine documented procedures to verify there is a formal process for testing and approval of all: • Network connections and • Changes to firewall and router configurations
	NEW	**1.1.1.b** For a sample of network connections, interview responsible personnel and examine records to verify that network connections were approved and tested.	
	NEW	**1.1.1.c** Identify a sample of actual changes made to firewall and router configurations, compare to the change records, and interview responsible personnel to verify the changes were approved and tested.	
1.1.2 Current network diagram with all connections to cardholder data, including any wireless networks	1.1.2.a Verify that a current network diagram ~~(for example, one that shows cardholder data flows over the network)~~ exists and that it documents all connections to cardholder data, including any wireless networks.	**1.1.2** Current network diagram that identifies all connections between the cardholder data environment and other networks, including any wireless networks	**1.1.2.a** Examine diagram(s) and observe network configurations to verify that a current network diagram exists and that it documents all connections to cardholder data, including any wireless networks.
	1.1.2.b Verify that the diagram is kept current.	**1.1.2.b** Interview responsible personnel to verify that the diagram is kept current.	
NEW	NEW	**1.1.3** Current diagram that shows all cardholder data flows across systems and networks	**1.1.3** Examine data-flow diagram and interview personnel to verify the diagram: • Shows all cardholder data flows across systems and networks. • Is kept current and updated as needed upon changes to the environment.

PCI DSS v3 vs v2 Change-Severity and Mapping.pdf

- A row-by-row mapping of PCI DSS v2.0 to v3.0 Requirements and Testing Procedures numbering and change-severity labelling.



	B	C	D	E	F	G	H	I	J	K	L	M	O	P	R	S	T	U	V	W	X	Y
1	DSS#	e Pr	##	v2.0 Req#	V3.0 Req#	R	1	2	3	N1	N2	eqRx	e Pr	V2.0 Test#	V3.0 Test#	R	1	2	3	N1	N2	estR
2	1			1.1	1.1			x				2		1.1	1.1			x				2
3	1			1.1.1	1.1.1		x					1		1.1.1	1.1.1.a			x				2
4	1													New	1.1.1.b					x		N1
5	1													New	1.1.1.c					x		N1

PCI SSC References for DSS v3.0

PCI SSC Website

https://www.pcisecuritystandards.org

PCI DSS v3.0

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

PCI DSS v3.0 Summary of Changes

https://www.pcisecuritystandards.org/documents/PCI_DSS_v3_Summary_of_Changes.pdf

PCI DSS v3.0 Press Release

https://www.pcisecuritystandards.org/pdfs/13_11_06_DSS_PCI_DSS_Version_3_0_Press_Release.pdf

PCI DSS v3.0 InfoGraphic

https://www.pcisecuritystandards.org/pdfs/PCIDSS.pdf

CONTROL | GAP

Get Compliant. Stay Compliant.®