ControlCase
Compliance as a Service

PCI DSS V3.2

Larry Newell
MasterCard

PCI DSS – then and now

2006

PCI DSS v1.0 – v1.1

- 12 high-level requirements
- Layered security
- Based on industry-accepted security best practices
- Allows for use of Compensating Controls

2016

PCI DSS v3.2

- 12 high-level requirements
- Layered security
- Based on industry-accepted security best practices
- Allows for use of Compensating Controls

ControlCase
Compliance as a Service

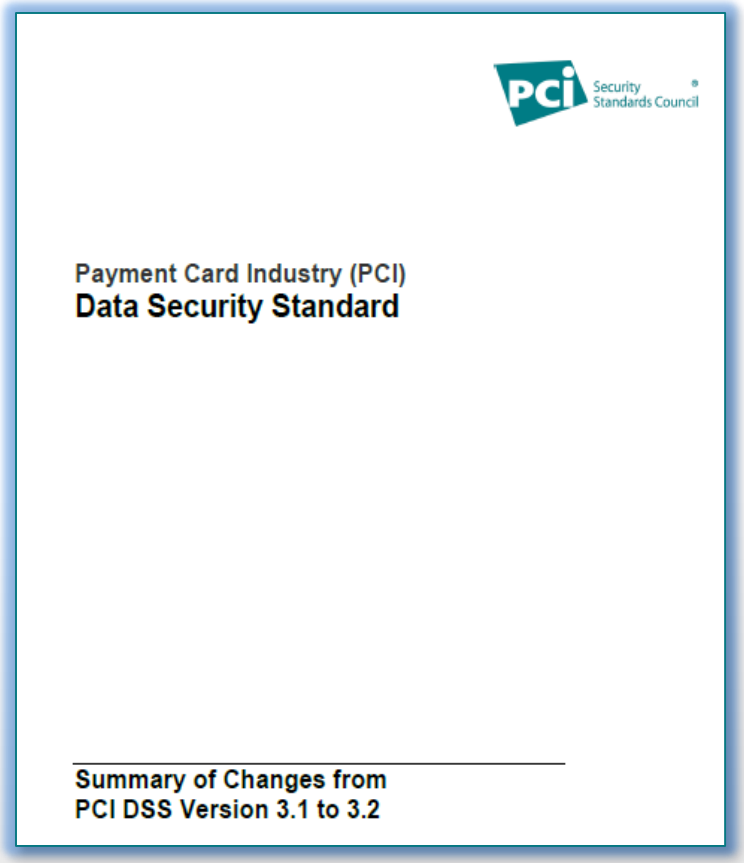
What has changed since the beginning

- Requirements and testing procedures in single document
- More guidance added over time
- Increased flexibility for some requirements
- Evolving requirements – e.g.:
  - What is considered “strong” cryptography
  - Physical security of POI devices

ControlCase
Compliance as a Service

What's new with v3.2

- Summary of Changes
- Glossary
- ROC template and AOCs
- SAQs to incorporate V3.2 changes
- Prioritized Approach
- Information Supplement: Migrating from SSL/Early TLS



ControlCase
Compliance as a Service

Key Changes in PCI DSS 3.2

- Multi-factor authentication (MFA) for non-console administrative access (Req. 8.3., effective January 31, 2018)
- Incorporate business-as-usual principles into change management processes (Req. 6.4.6, effective January 31, 2018)
- New Appendices for SSL/TLS and DESV (Appendix A2 & A3)
- Masking formats to accommodate new bin ranges (Req. 3.3)

ControlCase
Compliance as a Service

Multi-Factor Authentication in V3.2

New Requirement 8.3.1

8.3.1 Incorporate multi-factor authentication for all non-console access into the CDE for personnel with administrative access.

ControlCase
Compliance as a Service

Multi-Factor Authentication in v3.2

- Updated terminology
  - “two-factor” replaced with “multi-factor”
  - Does not change intent of original requirement
  - Still can’t use one factor twice
- MFA already required for all remote access to the CDE
- Now also required for personnel with non-console administrative access into the CDE

ControlCase
Compliance as a Service

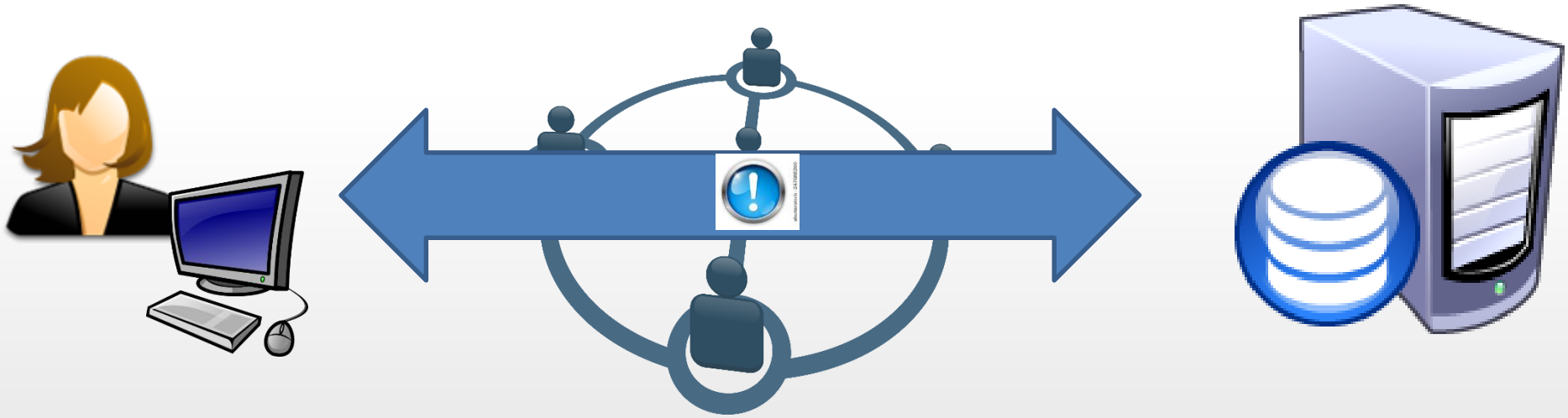
Understanding “non-console” access

- Glossary definition
  - Logical access to a system component that occurs over a network interface rather than via a direct, physical connection to the system component.
- Examples:
  - Non-console access includes access from within local/internal networks as well as access from external, or remote, networks. (i.e. corporate network to CDE)
  - Non-console access can be between systems on the same network subnet/zone or on different subnet/zones. (system to system inside the CDE)

ControlCase
Compliance as a Service

What is “non-console administrative access”?

- Individual (human) with administrator privileges connecting to a system in the CDE over a network



ControlCase
Compliance as a Service

Examples of non-console administrative access

- Manage POS terminal configurations via terminal management system
- Database Administrator (DBA) connecting to a database that contains CHD
- System Administrator using their system administrator account to connect to a system in the CDE for any reason
  - *Best practice:* Administrator personnel connecting to a system over the network for purposes other than to perform an administrative task should use an alternative account with user-level privileges.

ControlCase
Compliance as a Service

When does MFA apply?

- MFA applies to:
  - Any non-console connection to the CDE by an individual with administrative access
  - Any remote connection to the CDE, where the access originates from outside the entity's network
- Multi-factor authentication can be implemented at network level or at system/application level; it does not have to be both.
- MFA is not required for:
  - Logon to a standalone system not connected to a network
  - Logon to a networked system with a local system admin account (no network privileges)
  - Connections via direct physical connection between the input device and target system that do not travel over a network connection (i.e. Console Access)

ControlCase
Compliance as a Service

Maintaining PCI –DSS – Business As Usual

Requirement 6.4.6

6.4.6 Upon completion of a significant change, all relevant PCI DSS requirements must be implemented on all new or changed systems and networks, and documentation updated as applicable.

ControlCase
Compliance as a Service

What does 6.4.6 imply?

- Does not mean every PCI DSS requirement has to be reviewed for every change
- Use common sense – how does the change impact PCI DSS compliance and does it meet the intent of the requirements
  - If a new system is being added … is it hardened to meet or exceed the PCI DSS requirements? Has it undergone vulnerability scans? Is the software up to date?
  - New technology introduced – training for employees on proper use; update policies
  - New POI terminals – req. 9.9
  - And so on…

ControlCase
Compliance as a Service

Appendix A2 – SSL/early TLS

- Migration deadlines for SSL/early TLS extended to 30 June, 2018
  - New implementations must not use SSL/early TLS
  - Service Providers must have secure service offering by 30 June, 2016
  - All entities must cut over to secure versions of TLS by 30 June, 2018
  - Prior to June 30, 2018, existing implementations must have a formal Risk Mitigation and Migration Plan in place
  - POIs verified as not susceptible to known SSL vulnerabilities may use SSL/earl TLS beyond 30 June, 2018
  - Do not wait until 2018 to start doing something!

ControlCase
Compliance as a Service

What is a Risk Mitigation and Migration Plan?

- Same content as defined in PCI DSS v3.1
- Details how entities are addressing migration to secure protocol(s)
  - How vulnerable protocols are used in environment
  - Implemented controls to reduce risk associated with use of SSL/early TLS until migration is complete
  - Processes for monitoring new vulnerabilities associated with vulnerable protocols
  - Overview of migration project plan

ControlCase
Compliance as a Service

Why the Extension on SSL/TLS?

- Extensive consultation with industry
  - Consider business relationships and interdependencies
  - More time to complete complex migrations
- Extended dates not an excuse to delay
  - Potential risk to organization
  - Still need to address vulnerabilities per Requirements 6.2 and 11.2

ControlCase
Compliance as a Service

DESV – Designated Entity Supplemental Validation

- Designated by the payment brand or acquirer as requiring additional validation of existing PCI DSS requirements

The additional validation steps include:

- Implementation of a PCI DSS compliance program
- Documentation and validation PCI DSS scope
- Validation that PCI DSS is incorporated into business-as-usual (BAU) activities
- Control and management of logical access to the cardholder data environment
- Identification and response to suspicious events

ControlCase
Compliance as a Service

PAN masking formats

- “First six / last four” still rule-of-thumb
- Business justification for any format that displays more than first six and/or last four PAN digits

1234 56xx xxxx 0123

1234 56xxxx x0123

ControlCase
Compliance as a Service

When will a new release of PCI DSS be released?

Good News! There is no expectation of a PCI DSS release in November 2016?

That's correct. We are not planning any additional releases of PCI DSS during 2016. The version 3.2 release in the first half of 2016 replaces the expected fourth quarter 2016 release.

Reasoning:

- We must address the revised migration dates away from SSL/early TLS.
- The industry recognizes PCI DSS as a mature standard now, which doesn't require as significant updates as we have seen in the past
  - Moving forward, you can likely expect incremental modifications to address the threat landscape versus wholesale updates to the standard.
- We are sensitive to the drastic changes that are happening with payment acceptance - from advancements in mobile payments to EMV chip rollout in the United States, to adoption of other forms of dynamic data and authentication.
  - By releasing the standard early, with long sunrise dates, organizations can evaluate the business case for their security investments.

ControlCase
Compliance as a Service

PA-DSS V3.2

- Updated to align with PCI DSS v3.2 changes
- Additions to Implementation Guide content:
  - Debugging logs that include PAN must be protected, disabled as soon as troubleshooting is complete, and deleted when no longer needed
  - Secure installation of patches and updates
- PA-DSS not impacted by SSL/TLS migration dates
- Key dates:
  - PA-DSS v3.2 was released in May 2016; therefore, PA-DSS v3.1 was retired 31 August, 2016.

ControlCase
Compliance as a Service

Can TLS v1.1 be used for PA-DSS?

- Yes, if configured properly
  - Disable weak ciphers/cipher suites (MD5, RC4, SHA-1, etc.)
  - Use sufficient key sizes
  - Prevent fallback to SSL and TLS 1.0
- TLS 1.2 or higher recommended
- See NIST SP 800-52, rev. 1 for guidance on secure TLS configurations

ControlCase
Compliance as a Service

SSL/TLS Considerations for ASVs

- ASV not responsible for evaluating scan customers' RMMP
- ASV focus is on detection and reporting of vulnerabilities
- Detection of SSL/TLS should result in a failed scan, with exceptions handled according to the ASV Program Guide
- ASVs may issue a passing scan where Exception process is met

ControlCase
Compliance as a Service

Additional PCI SSC Resources

PCI DSS 3.2 Resource Guide

The Payment Card Industry Security Standards Council (PCI SSC) has published a new version of the industry standard that businesses use to safeguard payment data before, during and after purchase. PCI Data Security Standard (PCI DSS) version 3.2 replaces version 3.1 to address growing threats to customer payment information. Companies that accept, process or receive payments should adopt it as soon as possible to prevent, detect and respond to cyberattacks that can lead to breaches. Read on for answers to key questions about updates to the standard, timelines, and resources available for understanding and adopting PCI DSS version 3.2.

Q **Why is the PCI DSS being updated?**

A: The Council updates the PCI DSS to ensure it continues to protect against old exploits that are still causing problems, addresses new exploits and provides greater clarity for implementing and maintaining PCI DSS controls.

Q **Why is it PCI DSS 3.2 and not PCI DSS 4.0?**

A: The industry recognizes PCI DSS as a mature standard now, which doesn't require the significant updates we have seen in the past. Moving forward, the marketplace can expect incremental revisions like 3.2 to address the changing threat and payment landscape, with a focus on providing clarity and guidance to help companies use and maintain the standard as everyday business practice.

Q **What are the types of changes included in PCI DSS 3.2?**

A: PCI DSS 3.2 includes clarifications to existing requirements, new or evolving requirements, and additional guidance. These are outlined in the Summary of Changes from PCI DSS 3.1 to PCI DSS 3.2.

PCI DSS 3.2 Highlights Webinar

ControlCase
Compliance as a Service

Additional PCI SSC Resources

- PCI SSC blog: http://blog.pcisecuritystandards.org
  - What's "new" postings
  - Sort by categories (i.e. TLS/SSL: Working with ASVs on Failed Scans
- SSL/Early TLS Information Supplement (April 2015)
  - https://www.pcisecuritystandards.org/documents/Migrating_from_SSL_Early_TLS_Information_Supplement_v1.pdf
- Bulletin on updated migration dates (Dec 2015)
  - https://www.pcisecuritystandards.org/documents/Migrating_from_SSL_and_Early_TLS_-v12.pdf

ControlCase
Compliance as a Service

Thank You!

ControlCase
Compliance as a Service