Introduction

- Thanks Sherron (anything else?).
- Great to be here today and actually be in-person again.
- Introduce self.
- I don’t know if you’ve heard?
- PCI DSS v4.0 was published in March of this year?

PCI DSS v4.0 is here!

- This is a culmination of a multi-year-project and we are so excited about it!
- Talk about how important v4.0 feedback was in the dev of v4
- Where to find v4.0 and what are the key updated documents
- Cover some of the new/upd guidance and some of the most sign. changes
- Can’t incl everything – lots of updts and, well, DSS is over 350 pgs now
- Some diff info than if you listened to other PCI DSS v4.0 presentations
- By end of session, hope you identified a few areas you’d like to read more about – Std is full of good info, even for those that may complete an SAQ
- First let’s start with an overview of the v4.0 sessions during this comm mtg

PCI DSS v4.0 Presentation Series

- Today's series starts with this presentation.
- Followed by:
- Quick Fire Round – Your Top 10 Questions about PCI DSS v4.0 Answered - *(Marc B, Tom W, Kandyce Y)*
- And tomorrow:
- Embracing the Journey to PCI DSS v4.0 – *Emma Sutcliffe*
- Seismic change or mere ripple – Understanding Reporting for PCI DSS v4.0 - *(Kandyce Y and Brandy C)*
- And panel discussion about Understanding the New Customized Approach –
- *(Moderated by me, Panelists: Marc B, Tom W, Brandy C)*
- If you are wondering where those v4.0 docs located and what's been published so far…

PCI DSS v4.0 Documents Available Now in the PCI SSC Document Library

- Drop down menu so you can choose v3.2.1 or v4.0
- In addition to PCI DSS v4.0, the following docs are available in our Doc Library
- SOC from PCI DSS v3.2.1 to v4.0; (ROC) Template, ROC AOCs, ROC FAQ
- DESV ROC, AOC, and Frequently Asked Questions
- (SAQs) and AOCs, Prioritized Approach, QRG
- The SOC is a great resource, Summ changes in intro, Describes general changes, those within each req. Summ of all new reqs too.
- Transl – Port, Ger, Sp, Ch, Ja, Fr - available for std, SOC, ROC AOCs, and SAQs

Goals for PCI DSS v4.0

- By now, some of you may be as familiar with these goals for DSS v4.0 as I am
- Not going to recite the goals today but I will be mentioning some during pres
- These goals have been with us this entire journey, since we started planning for v4.0 in 2017, back when v3.2 was the current version
- Pleased to say we've been able to incorporate all these goals into v4
- Very important aspect of how we met these goals is our **<click>** RFC process.

PCI DSS v4.0 RFC Participation

- Global Industry feedback - fundamental to evolution of v4
- Held 3 separate RFCs while v4 was in development:
- 2 RFCs for draft Std and 1 for Valid Docs – includes ROC temp, SAQs, AOCs
- Incredible amount of input- over 6k comments from more than 200 companies from these 3 feedback periods
- Average for a PCI SSC RFC is around 300-500 comments; see this was a lot
- Reviewed every single item, categorized it, discussed it, and actioned it.
- v4.0 is truly the result of a collabor. effort with the PCI Comm

Inside PCI DSS v4.0

- That’s how we got here

- Now let’s look inside the standard, and some of the key changes

PCI DSS can also be used…

- Added wording into v4.0 to help ensure the std continues to meet the security needs of the pays ind –
- and to help understand broad applic of DSS to payments
- Payments are starting to happen in different ways now - but the payment ecosystem still needs to be protected.
- PCI SSC has always promoted PCI DSS as a robust set of security controls that can be used to help secure any environment
- (refer to FAQ 1437 Can PCI DSS be used to protect non-payment card data?).

A Lot of New Guidance!

- First, lots of new and upd guid. in intro - E.g., which reqs may apply even if an entity does not S, P, or T PAN
- Clarified terms - account data, CHD, SAD, and PAN; each has a diff meaning, not interchangeable; used purposefully
- Clarified def. of CDE
- Lots more guidance on TPSPs – really a lot more, please read.
- New section on timeframes, help orgs understand the intent of daily, weekly, monthly, quarterly and more timeframes terms used in DSS
- And several new appendices to hold more info, incl CA, SW frame, Glossary- speaking of SW frame <click>

Leveraging the PCI S/W Security Framework

- Section now focuses on how SSF stds can support DSS, and new app F expands on topic
- Because the SSF stds include rigorous S/W sec reqs, the use of S/W dev'd and maint'd according to either the Secure S/W Std or the Secure SLC Std can:
- Help the entity meet several reqs in Req 6 w/o add'l testing OR May also support use of the CA for other reqs
- Remember that PCI DSS goal about flexibility? A big part of DSS.
- the new CA **<click>** is all about flexibility

Two Approaches for Meeting PCI DSS Requirements

- V4.0 introduces the CA; two options now to impl and valid. reqs
- DA is what orgs have been doing for years, the org impl reqs as stated in the std
- and assessor follows the TPs as written to validate the req is met
- **<click> CA provides more flex**

Two Approaches for Meeting PCI DSS Requirements

- The CA is an alternative for orgs that choose to dev an innovative/diff control or process, but it must meet the stated CA objective.
- Most but not all requirements are eligible for CA – those not eligible no CAO
- Orgs can use either approach with v4.0, can mix and match in your env, decide based on what works best.
- Come to our panel tomorrow on CA with me, MB, BC, TW
- – lots more details - Blog posts on CA too <pause>
- Before I start to walk you thru some req updates – some of you may have seen this new diagram <click>
- That describes the layout and content of the requirements

Layout and Content of Requirements

- New graphic is right before reqs start, Describes each element of a req:
- *The Req description* – added to organize and descr reqs that fall under it
- I just mentioned the DA and CA – can see the *DA reqs and DA TPs* headings
- And the *CAO* – appears right under the applicable requirement
- Meaning of these columns is summ'd in this diagram too
- App Notes for many reqs, how or where the req applies E.g., SP only reqs, Also indicates new reqs with a FD
- For Guid col, added headers to organize and clarify diff types of guidance
- Let's look at some updates to existing reqs **<click>**

Noteworthy Updates

- Some changes that are not “new” reqs – In R1, clari that network changes must follow change control processes defined in req 6
- Also in R1, no more mention of DMZ, controls now focus on trusted/ untrusted NWs (untrusted is any w/o DSS controls appl or that org not cntrl)
- In R3, clarified BIN ranges for masking to align with FAQ 1091 for trunc – BIN and last 4. Be sure to listen to Emma’s preso on BIN ranges tom..
- In R8, for group, shared, generic accts – added flex. Can use these accts as long as properly mnged following several specific criteria.
- In R12, removed req for an org-wide RA, replaced with TRAs – more on this in a bit.
- And we do get lots of Qs about our <click> PW reqs

Passwords

- Some stkhldrs still rely on PWs - the std continues to support PW reqs.
- **PW length >** from 7 to 12 - 7 chars no longer suff with mod comp power.
- FD so it is not req'd until 31 Mar 2025 - But orgs must have PW of at least 7 chars per v3.2.1 until the longer length is req'd.
- Also, the req to change PWs every 90 days remains -if PWs/phrases are the only auth factor for user access (any single-factor authent to in-scope sys),
- However – **we added more flex. to this req**
- For orgs using dynamic analysis to make real-time decisions for access to resources (e.g., zero-trust implementations) - PWs don't have to change.
- This is another option for meeting the password req so it is not FD
- Next up, **<click>** how about some info about new reqs?

New Requirements for all Entities (53)

- *Lots of reqs added to ensure std continues to meet the Sec Needs of Pay Ind*
- 53 new requirements in PCI DSS that apply to all entities, including:
- 2 new reqs if SAD is stored prior to authorization – include in data ret and disp policies & encrypt using strong cryptography
- Use keyed crypto hashes, if hashes used to render PAN unreadable
- Perform authenticated scanning for internal vuln scans;
- **<click>** Additional 11 reqs for service providers only

New Requirements for SPs only (11)

- New reqs for SPs including:
- SAD stored by issuers/those supp issuing srvcs is encry with strong crypt.
- MTSP provide support for customers for external pen testing

- A total of 64 new reqs
- Most new reqs have an extended impl date before they become effective
- These reqs identified as best practices in v4.0; are effective 31 March 2025.

- However **<click>**

New Requirements Effective Immediately (13)

- 13 new reqs with no future date; eff immed for all v4.0 assessments.
- *Rs and Rs* - for reqs 2-11 – Documentation req; easy to impl b4 a v4.0 assmnt.
- ***TRAs for any req met with the CA –*** Req'd for anyone using a CA – which is why it is eff immed
- ***Doc and confirm DSS scope at least once every 12 months –*** Informal req to doc and confirm scope b4 an annual assmnt; now formal req
- ***TPSPs to support customers' requests to provide DSS compl. status*** and info about which DSS reqs are the TPSP's responsibility
- Was required for custs. to get it from TPSPs, now req'd for TPSPs to provide it.

- Where can you find details about these new reqs and when eff? <Click>

New Requirements Effective Immediately (13) 2 of 2

- If you guessed the SOC, ding, ding, ding, you're right!
- Details about new reqs, incl whether they are eff immed for v4.0 assessments or not until 31 March 2025 - provided in the SOC
- Encourage you to download and review the SOC if you haven't already
- Lots of good info in there, I promise

- Now let's focus on a few other new reqs in a bit more detail **<click>**

Multi-Factor Authentication

- MFA is new?
- Two current MFA reqs: for remote access from outside of entity's network and for all admin access into CDE
- New requirement eff 31 March 2025 MFA for all access into the CDE
- Replacing existing req for MFA for all admin access into the CDE, once eff
- Lots of guidance added to these reqs
- to help explain where/how to impl MFA
- Also a new requirement for proper impl. of MFA systems.
- Next Phishing

Prevent Phishing

- Phishing is all about targeting people to take an action that benefits the attacker (click on link that gives access or provides info)
- A two-pronged approach to address phishing attacks - Both focus on people
- The first – a tech req - Processes and auto mechs to detect and protect personnel against phishing attacks
- The second – for sec aware. training that incl phish and social eng. - Both are required; meeting one does not satisfy the other one.
- Another big threat area PCI DSS now addresses is one that has been hitting e-commerce merchants hard – **<click>** web-based attacks

Prevent Web Attacks

- Also, a two-pronged approach to address the ecomm skimming (or Magecart) attacks happening over the web:
- One: Managing payment page scripts that are loaded and executed in the consumer's browser.
- Attackers use these scripts to upload their own malicious code, in order to capture cardholder data from consumers' browsers.

- And two: deploying change detection mechs to look for indicators of malicious activity on payment pages. Lots of good guidance incl in DSS
- And the last set of new reqs I will discuss today are **<click>** the two types of TRA reqs

CLICK

Targeted Risk Analyses: First Type

- First type –gives orgs flex. to define how freq to perf certain activities
- Orgs can establish the frequencies that work for their business
- 9 new reqs specify that doc'd TRA be completed to define a frequency – e.g.
- How freq to eval sys comps not at risk for malware – to make sure they are still not at risk
- – and for type and frequency of periodic POI device inspect.
- This is not the same as an enterprise-wide RA, (said before req was deleted)
- Targeted analysis looking at risk related to that specific req based on the ident. of threats, likelihood, and/or impact. The 2nd type **<click>** of TRA

Targeted Risk Analyses: Second Type

- I mentioned before when I talked about new reqs that are eff immed for all v4.0 assessmnts - for any req an entity meets with a CA
- To help peop understand how to impl both types of TRAs, the elements of each type are detailed in two reqs in Requirement 12.
- And for CA, a template for the TRA is provided in Appendix E
- Outlines the minimum information that must be doc'd in a TRA for CA
- <Pause>
- Tomorrow KY and Brandy are cover new v4.0 rept options in detail but
- Before wrapping up, I want to cover one reporting option <click> IPWR that you may have heard about

What's Next for In Place with Remediation?

- The PCI DSS v4.0 ROC Template, SAQs, and AOCs currently include IPWR as a new reporting response option.
- New option intended to **support security as a continuous process** by providing an oppor for orgs to target areas for improvement year over year.
- Since the Mar 2022 release of these docs, PCI SSC has received a lot of FB about this new reporting option from our BOA and GEAR
- They expressed concerns about the best way to incorporate it into the assessment process without it impacting reporting.
- We listened and took a step back to review the best ways to document this option.

Positive Feedback about IPWR

- We also received positive feedback about this option.
- Value to this information being provided internally for use with leadership
- Good tool to elevate issues to executive level
- Addresses a long-term gap in reporting
- But concerns if this is reported in any public/shared document (like an AOC)
- Looking at ways retain value by reporting in a separate summary worksheet

Encourage Security as a Cont Process

- Based on discussions, idea has merit and want to retain its value
- Continue to support intent of IPWR - encourage sec as a cont process
- Value can be retained by separating info about gaps and imp's needed from formal rpt'ing docs - E.g., separately provided worksheet as a ROC addendum
- Update IPWR terminology to reflect focus on areas needing imp't.
- Provide add'l guidance (e.g., FAQs and other supp docs) to help orgs understand
- Update QSA Program Guide to clarify assessor expectations and requirements for this separate reporting– Updates planned for Q4/Q1 – Next: timeline slide

Implementation Timeline

- Reminder - v3.2.1 will remain active for 2 years from the v4.0 release - will be retired on 31 March 2024.
- As I've mentioned, many new reqs are BPs until 31 March 2025 to give orgs time to impl upds.
- Prior to this date, orgs can, but not required to, include new reqs in their assessment if ready
- Once that March 2025 eff date is reached – new reqs must be fully considered during a PCI DSS assessment.
- Encourage you to join Emma Sutcliffe's session tomorrow about planning for your transition to v4.0.

Resources

- Reminder that you cann access all our v4.0 resources
- through the PCI DSS v4 resource hub on our blog
- And please join Lindsay G and Elizabeth T tomorrow afternoon for a discussion of our various PCI SSC resources and engagement opportunities

Conclusion

- 6000 comments – wow! I'm still blown away by that; and by the fact that I reviewed all that feedback too!
- Your FB has been fundamental to what PCI DSS v4.0 is today.
- We added a lot more guidance and clarifications because you provided comments, asked questions, and told us what was unclear.
- And FB continues to be vital, as ind. by changes we are making to IPWR.
- So please, go to our Doc Lib, download the SOC and the Standard (at least, as the first docs)
- Hopefully you ident. a few areas of interest that you want to read more abt And read up on those areas that hopefully you identified today as areas of interest
- And let us know what you think and what questions you have <click>

Thank You!

- I will be here all week, if you have any questions
- Come find me or come to our office hours
- If I'm not in the office, leave a message for me or ask someone to find me.
- Next up we have the Quick Fire round to answer your Top 10 questions – this one should be a lot of fun.
- And thank you for your time and attention today.
- Turn it back to Sherron to introduce the next session