Community Questions with the Council

Notes Page: 1

Thank Alicia & Emma – Closing Remarks

INTRO QUESTION

So, it’s been 3 years since we’ve all been together in person.

Let’s talk a little about what has changed at the PCI Security Standards Council.

Lance, let’s start with you. *(HE ANSWERS)*

And Emma, what about you?

Participating ORG RESTRUCTURE

1. As many of you heard in Lance Johnson's opening remarks today, the Council is restructuring its existing Participating Organization Program. So, we brought back Lance to help clarify some of the information that was presented.

Under this new program, Lance, there are different levels. The Associate PO is comparable to our existing PO program. Why should organizations consider joining as a Principal PO?

Participating ORG RESTRUCTURE

- A: The Principal PO is designed to enable a deeper level of collaboration and interaction with the Council on both a tactical and strategic level. Principal POs will have the opportunity to have greater dialogue with the Council's staff and leadership on the direction of standards as well as have a greater likelihood of serving on the Council's Board of Advisors. Joining as a Principal PO establishes an organization as a leader in the payment security community. It offers an unparalleled opportunity to provide influence on the technical direction of the Council's standards.

Participating ORG RESTRUCTURE

2. How does this change the Board of Advisors?

A: In recognition of the ever-changing needs of the payments industry, the Board of Advisors will be expanding to provide a greater range of input for the Council. It will be comprised of:

24 Principal PO Seats (Principal Seats)

20 Elected Seats

12 appointed seats to provide sector and global coverage

Participating ORG RESTRUCTURE

3. How will this PO/BoA restructure impact the development of standards?

A: The BoA will have the opportunity to vote on new standards and major revisions to standards prior to their release. The increased number of board seats will ensure greater global involvement in PCI SSC standards, providing even more opportunities for discussion and collaboration. This ensures that our standards continue to be globally relevant, appropriate, and up to date to ensure the best levels of security for cardholder data.

Participating ORG RESTRUCTURE

4. How do I join and when?

A: The existing Participating Organization structure will remain in effect until 31 December 2022. Existing POs who are happy with their current level of participation will automatically transfer to the Associate PO level on 2 January 2023.

It’s easy! An organization or individual wishing to become a PCI Participant should visit the PCI SSC website at www.pcisecuritystandards.org and select the “Get Involved” tab and choose “Ways to Participate”

PCI DSS v4.0

- **Thank you, Lance.**
- **We've also received numerous questions about PCI DSS v4.0 and I want to note that we will have dedicated sessions available tomorrow and Thursday to get more in-depth on this topic. Emma is presenting a session on Embracing the Journey to PCI DSS v4.0 on Thursday.**
  So, while we have you here, Emma, let's take a moment today to answer some of the most frequently asked questions we've received lately:

PCI DSS v4.0

5. One big question is What's the Difference Between Compensating Controls and the Customized Approach?

A: PCI DSS v4.0 offers two ways for an entity to implement and validate PCI DSS requirements - the defined approach and customized approach.

Compensating controls are still an option within the defined approach for entities that have a legitimate and documented technical or business constraint that prevents them from meeting the Defined Approach Requirement as stated. Compensating controls are often used in situations where there is a legacy system or process that cannot be updated to meet the requirement.

PCI DSS v4.0

6. Who decides whether an entity should implement a customized approach?

A: Each entity determines how it will meet PCI DSS requirements, including whether to follow the defined approach or the customized approach.

This approach is suited for organizations that already have controls in place to meet a requirement and are comfortable with the current methods for validating those controls. It is also suitable for organizations that are new to PCI DSS and may be looking for more specific direction on how to meet security objectives.

The customized approach is an alternative to the defined approach and focuses on a PCI DSS requirement's stated Customized Approach Objective. This approach provides greater flexibility and is suited for organizations that want to use alternate security controls or new technologies that meet the PCI DSS Customized Approach Objective.

PCI DSS v4.0

7. Can compensating controls and customized approach be used for the same requirement?

Yes. An entity can use compensating controls for certain system components and the customized approach to meet that same requirement for other system components.

As an example, an entity could use a compensating control to meet that requirement for a certain type of server where there is a legitimate and documented business constraint that prevents that server from meeting the stated requirement.

The entity may also choose to use the customized approach to meet that same requirement for other system components, where it has implemented a unique approach to detect and address the latest malware threats. The entity could also use the defined approach as stated, to meet that same requirement for another group of system components.

PCI DSS v4.0

8. Does PCI DSS apply to paper with cardholder data (for example, receipts, reports, etc.)?

A: Yes, PCI DSS requirements are applicable if a Primary Account Number (PAN) is stored, processed, or transmitted on or by any media, including paper records. PCI DSS Requirement 9 specifically addresses the safeguarding of physical media, including paper records, containing cardholder data.

PCI DSS v4.0

9. Do PCI DSS Requirements apply to Bluetooth technology?

Yes. PCI DSS requirements apply wherever payment card account data is stored, processed, or transmitted.

For example, PCI DSS Requirement 4 states that strong cryptography and security protocols must be used to safeguard sensitive cardholder data during transmission over open, public networks. Bluetooth technology is included in Requirement 4 guidance as an example of an open, public network, and cardholder data sent over Bluetooth must therefore be protected in accordance with this requirement.

PCI DSS v4.0

10. Which of the PCI DSS Requirements have you received the most questions about?

- Requirement 8
- MFA
- Shared user accounts
- Passwords
- Lauren

PCI DSS v4.0

11. So Emma, besides PCI DSS v4… are there any other significant Standards Updates coming this year?

- MPOC
- SSF – Web Software Module

PCI DSS v4.0

12. So Lance, with all these Standard changes and the PO Re-structure, how is the council communicating all of these updates?

- Website re-design
- Mobile App
- Lindsay, Elizabeth, Mark – Session Thursday afternoon

Notes Page: 16

LAST QUESTION

CLOSING

Thank you everyone for joining Community Day Questions with the Council.

And thank you Lance and Emma for all of the great information.

THEY EXIT

Notes Page: 17

CLOSE

Sherron to Thank Alicia & Emma – Closing Remarks

- Thanks, Alicia and Emma.
- To wrap us up, I just want to thank you for your participation, this Community Day was meant for you.
- Toronto is a beautiful city and as part of our meeting we wanted to bring Toronto to you. We want to invite you to our version of “Downtown” right next door in our Vendor Showcase sponsored by Security Metrics. Here you can see and interact with leading payment security vendors, network and play games in our “Town Green” and grab a coffee at the PCI Café”

- So let’s join everyone now at the Vendor Showcase sponsored by SecurityMetrics and then don’t miss tonight's welcome reception at the Steam Whistle Brewery across the street, sponsored by Verizon.

- See you all tomorrow, back here at 9 AM to kick-off General Session.

Notes Page: 18

END