Mind The Gap

PCI DSS v4.0 vs v3.2.1

Presented by **Johan van Zyl**

About Me

I started my career in **specialist IT auditing** in **1997**.

I am now the **Managing Director** of **Risk X Data Assurance**.

If I had a middle name, it would have been **“Pragmatic”**.

I first “met” **PCI DSS** in 2009 while employed in the Internal Audit Department at a **level 1 merchant** and we have been in a close relationship since.

PCI Security Standards Council®

About RISKX

Your data. Assured.

Company is **7 Years** young.

Three verticals:

- **Assurance**
- **Advisory**
- **Testing**

PCI Security Standards Council

Assurance consists of:
PCI DSS, **P2PE** and **PFI**.

We have performed more than **15 full ROC** and **SAQ assessments** using the updated Standard.

What Entities Experience

1. Concern

2. Uncertainty

3. Panic

4. Excitement

Is There A Difference For Entities?

It is possible to pass a **PCI DSS v4.0 assessment** if the entity has previously passed a **v3.2.1 assessment**, but you have to do a few things first.

Come March 2025, there are significant changes to how entities comply with **PCI DSS**.

PCI Security Standards Council

Immediate Difference For Merchants

1. Ensure to update **roles** and **responsibilities**

2. Define your own **scope of compliance**

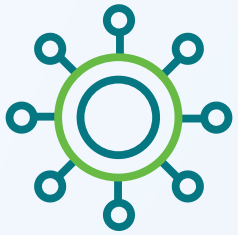
3. **TRA** for customized approach

4. **SAQ A** now has ASV validated external vulnerability scans

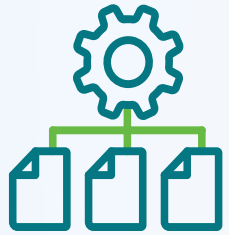
PCI Security Standards Council

Immediate Difference For Service Providers

1. Ensure to update **roles** and **responsibilities**



2. Define your own **scope of compliance**

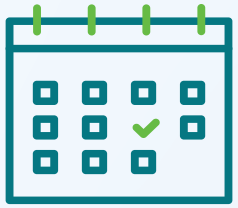


3. **Matrix of Responsibility** (req 12.9.2)

PCI Security Standards Council

Entities: What Doesn't Work

1. Continue to **build v3.2.1 artefacts** without v4.0 consideration



2. **Delay planning** for future dated requirements

3. Wait for the **QSA** to tell you what is in scope for PCI DSS

PCI Security Standards Council

What Our QSAs Experience

1. Overwhelmed

2. Concern for time

PCI Security Standards Council

The ROC: Is It A Different PCI DSS?

258 requirements and **sub-requirements** in **PCI DSS v3.2.1**

322 requirements and **sub-requirements** in **PCI DSS v4.0**

So, **64** new requirements, correct?

Search "**Validation Method – Defined Approach**"

You get **260** entries. 250 in 12 Main Requirements and 10 in the Appendices

62 requirements have sub-requirements and **no documentation requirement**

PCI Security Standards Council

Evidence Like An Auditor

Evidence have been split into **four** sections.

Some highlights as follows:

	Main ROC	Appendices	Total
Section 6 Evidence	686	16	702
Documentation Evidence	303	9	312
Interview Evidence	167	2	169
Observation Evidence	61	0	61
System Evidence	155	5	160

PCI Security Standards Council

QSAs: What Doesn't Work

1. Try to **retrofit** a v3.2.1 ROC into a v4.0 ROC

2. **Imbedding images** into the v4.0 ROC template

3. **Requesting the same evidence** for a v4.0 assessment as for the previous year's v3.2.1 assessment

4. Writing a ROC **directly** into the Word template

PCI Security Standards Council

What Works For Us

1. Keep **calm** & breathe

2. I **love Excel!** We captured PCI DSS v4.0 in Excel

3. We **mapped** v3.2.1 to v4.0 and **flagged** the new requirements

4. We then created **worksheets** for documentation, observation, interview and systems evidence, and **referenced** these to our PCI DSS v4.0 worksheet

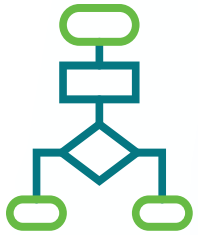
5. We **pre-referenced** the ROC template in **Word**

6. We use the Excel document to **scope and collect** the required evidence for our assessments

7. We then complete the **ROC** in **Word**

PCI Security Standards Council

Important Lessons From Real Life



While **702 evidence pieces** appeared daunting, we soon realised that there are many evidence pieces required with multiple referencing.

You can reduce your reporting and QA time through **pre-referencing the ROC**.

The new ROC documents easier.

PCI Security Standards Council

Take Home For Entities

PCI DSS v4.0 **early socialisation** paramount.

Do not wait until 2025 to consider **mandatory new requirements**.

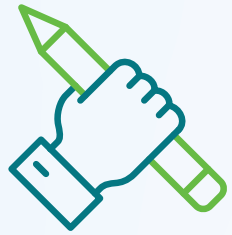
Customised controls need to be in place **before** the assessment starts.

PCI Security Standards Council

Take Home For QSAs

Set **enough time** for reporting

Don’t be **complacent**



Enjoy what you are doing

PCI Security Standards Council