PCI Security Standards Council

The Journey to Harmonisation:

Successful Alignment of PCI Assessments in a Global Enterprise Environment

Your Speakers

WORLDLINE

Isil Ugurlu

PCIP, ISA, CISM

Head of Worldline Group PCI Program

more security. usd

Christopher Kristes

QSA, 3DS Assessor, P2PE QSA, CISSP, CISA

Executive Board Member, Head of Security Audits & PCI

Agenda

Embark on our journey where we answer these questions:

What challenges did Worldline face?

What was our vision for overcoming them?

How did we do it?

How do we move forward with PCI DSS v4.0?

PCI Security Standards Council

PCI Security Standards Council

Situation at Worldline

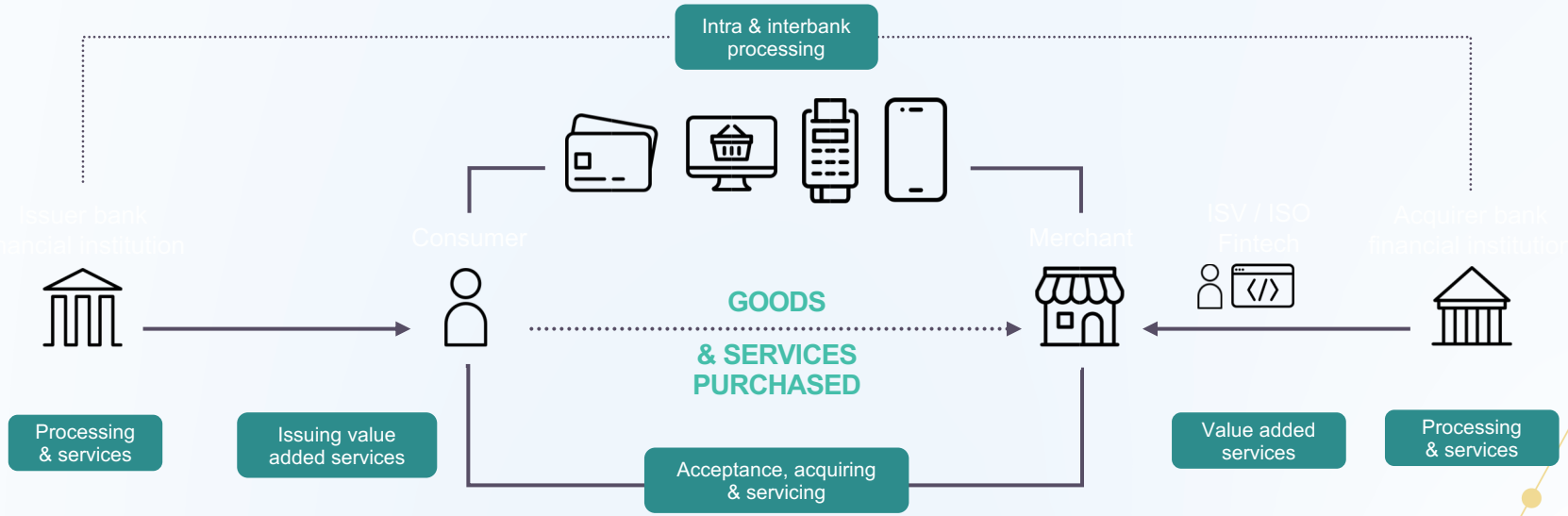
What challenges did Worldline face?

About Worldline

c. 18,000 Worldliners in 40+ countries

Commercial presence in **170+** countries

Covering the whole payment value chain



Merchant Services

1.25 M merchants served

Financial Services

c. 126 M cards under management

Mobility & e-Transactional Services

350+ clients in various industries

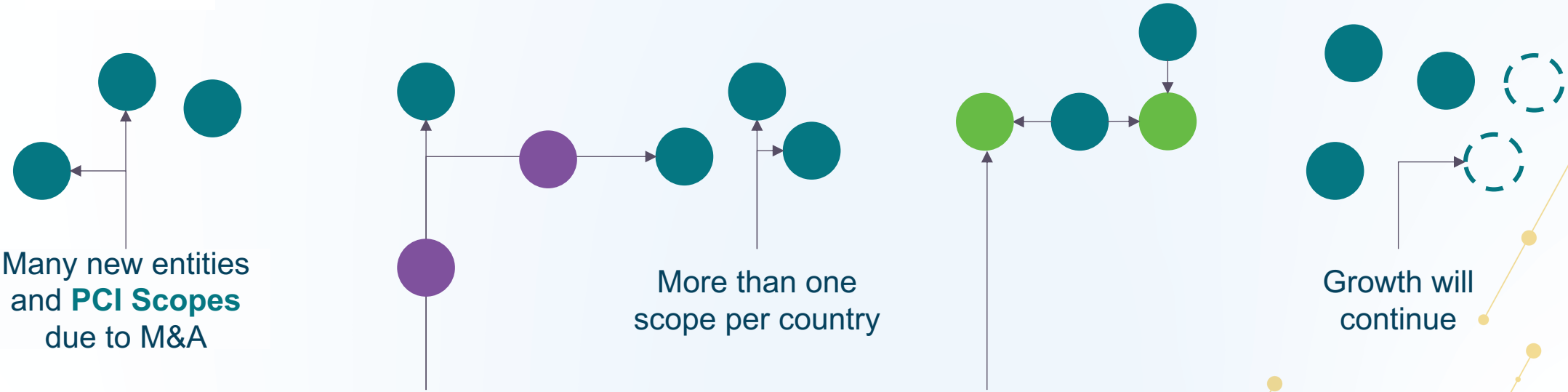
PCI Security Standards Council

Challenges of Global Growth

Why did we have to change anything?

WORLDLINE

GoPay → PAYONE → bambora (a Worldline brand) → cardlink (a Worldline brand) → Many more



Many new entities and **PCI Scopes** due to M&A

Different QSA Companies using various monitoring tools and different reporting standards

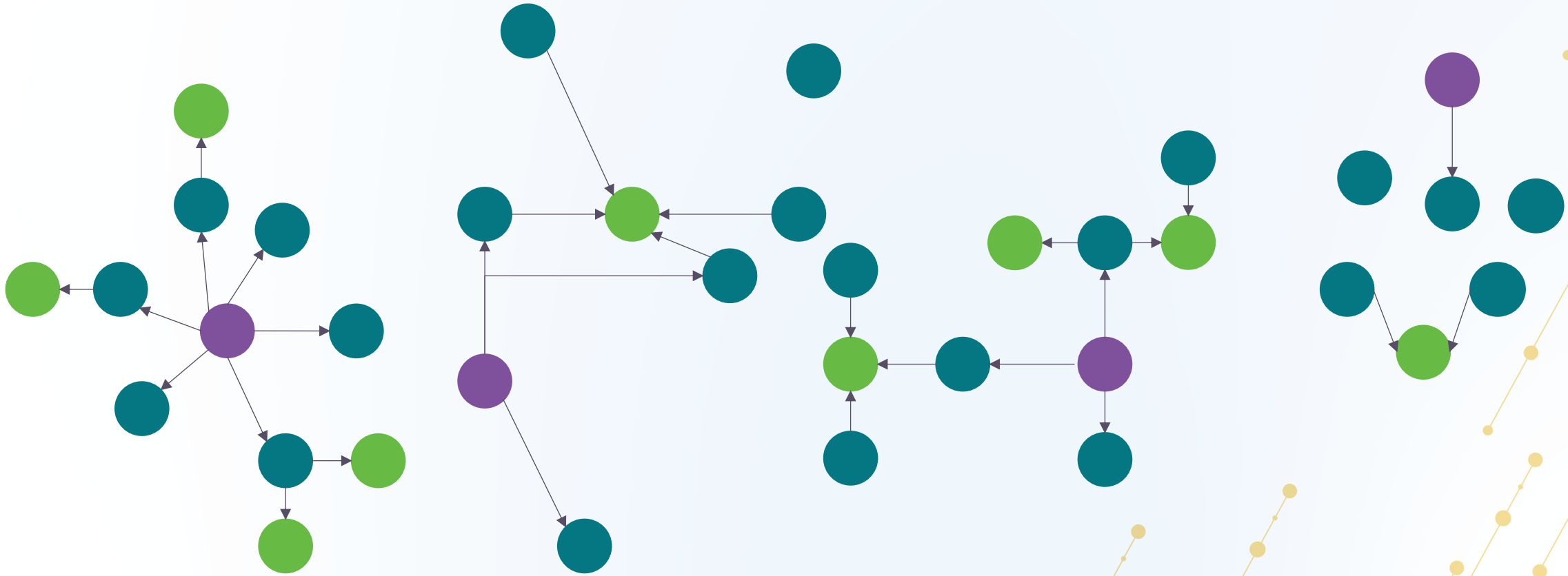
More than one scope per country

Local controls, methods, approaches in every country

Growth will continue

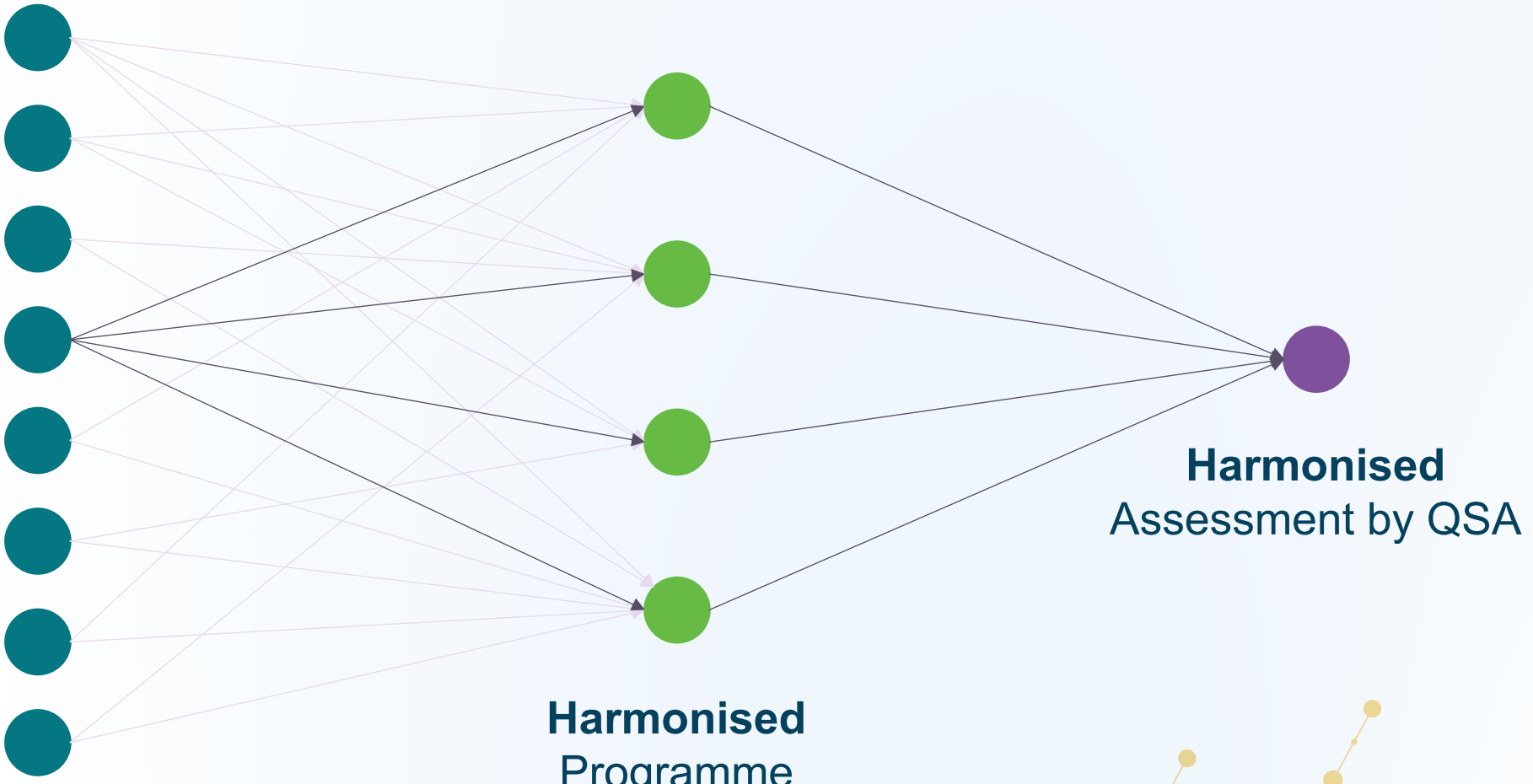
PCI Security Standards Council

So, Our Aim Was to Transform This…



PCI Security Standards Council

…Into This:



PCI Security Standards Council

PCI Security Standards Council

Our Vision

How did we envision our journey to harmonisation?

Our Vision

What goals did we want to achieve?

WORLDLINE

more security. usd

Strengthen the central certification approach that is oriented towards the major business lines

Improve the overall security to be prepared for the future

Adapt new PCI controls into separate Worldline entities and become ready for PCI DSS v4.0

PCI Security Standards Council

Roadmap to PCI DSS Harmonised Programme

Preparation

- From local teams to cross-country teams
- Control & scope inventory

usd provided assessments only for specific countries

Setup

- Domain approach introduced
- PCI DSS Harmonised Programme launched
- Central assessment sessions conducted

usd conducted first harmonised assessment at Worldline

Global Rollout

- Central PCI team built
- Global PCI DSS v4.0 transition project has started

usd as global assessor for all DSS audits

PCI Security Standards Council

Worldline's Global PCI Programme

Complex compliance programme due to global growth

PCI Security Standards Council

BoA & Communication with PCI SSC

PCI Central Team

Coordination of Internal PCI Training Programme

Certification Strategy

Coordination of 100 Assessments

PCI DSS

PCI DSS v4.0 Transition

Non-DSS

PCI Security Standards Council

PCI Security Standards Council

Our Assessment Strategy

How did we do it?

usd as a Partner

A perfect match for the harmonisation programme

more security. usd

Experience

PCI DSS since 2005

Worldline since 2009

Large Clients

medavis · PAYONE · PAGATEO · PHOENIX group · invia · zalando · MYRA · Getnet · GK · bp · Eurowings · METZLER · DOHOP · e-shelter security · VR Payment · RS2 · operations[1] · Miles & More · KRIEGER · NTT · Bizzon · DB · noris network · Keppel Data Centres · unzer · CASHPOINT

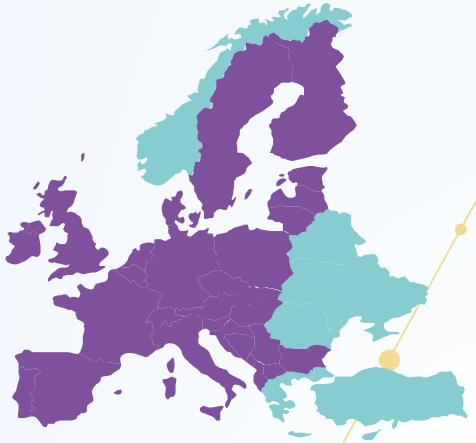
Experience in harmonisation projects

Team

Company 200

PCI 40

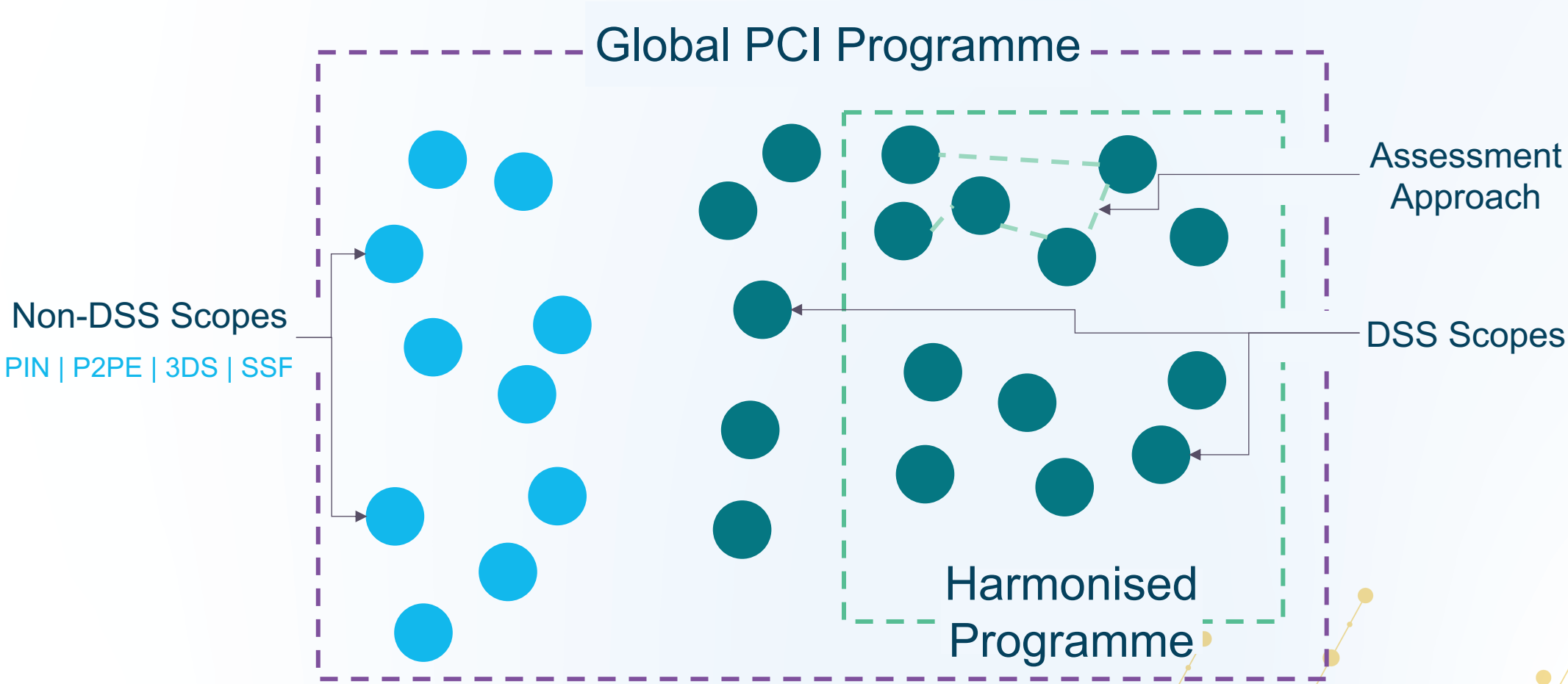
Centre of Europe



Security Standards Council

Big Picture

Global PCI DSS assessment strategy



PCI Security Standards Council

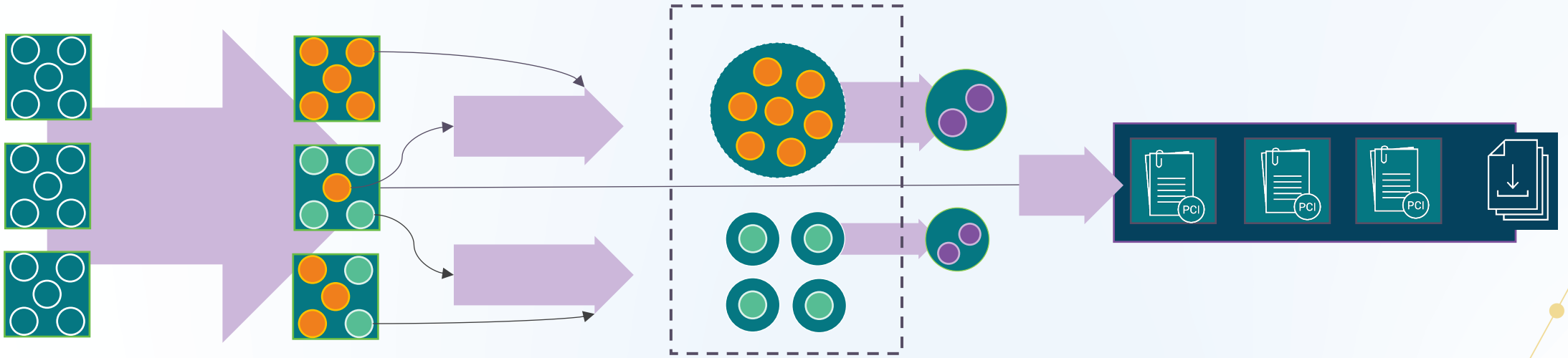
Central PCI DSS Assessment Planning

Overview

1. Planning

2. Assessment

3. Reporting



Entity

Harmonised

Non-harmonised

Central Assessment

Assessment sessions

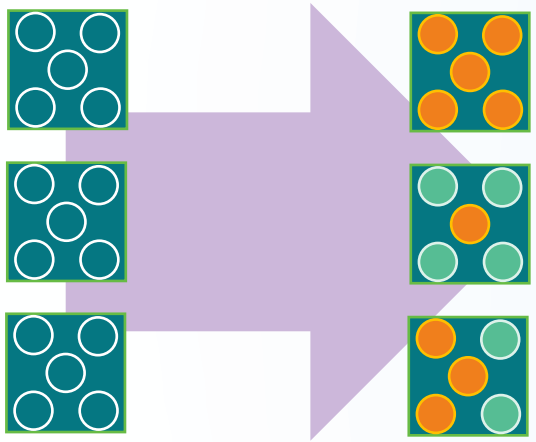
Sample

Separate RoC

Frame RoC (FRoC)

PCI Security Standards Council

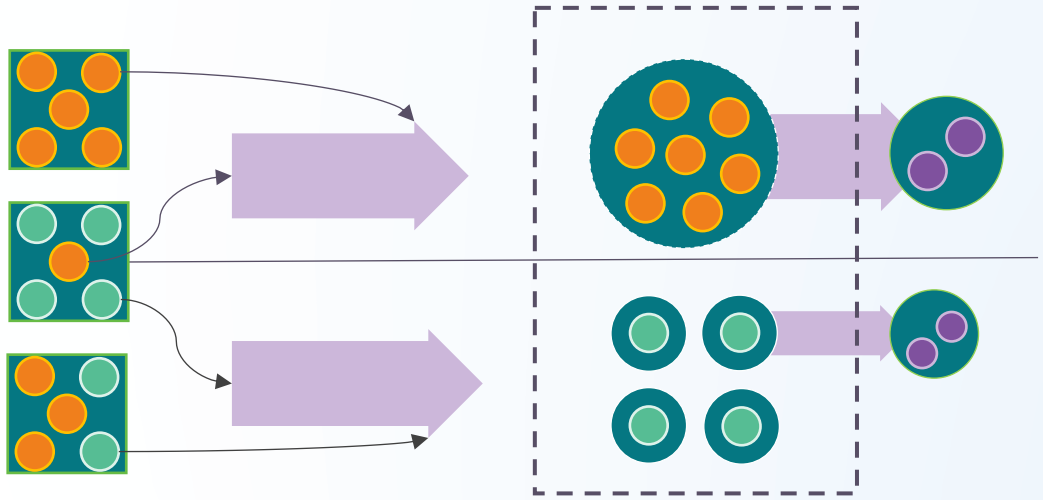
Process Phase 1: Planning



- All entities are listed **centrally**
- For **each entity**, assessment sessions are defined based on the existing DSS scope
  1. Fully harmonised sessions are moved to **central assessment sessions**
  2. For only partly harmonised topics, **dedicated sessions** are planned
- Result is a large table containing all global entities and assessment sessions

PCI Security Standards Council

Process Phase 2 (1/2): Assessments



- There is **one single assessment session for each topic** which covers all entities with fully harmonised processes
- For each topic, the assessor chooses **samples from all entities** covered by this assessment session
- All other entities have their own, **separate** assessment sessions for each topic

PCI Security Standards Council

Process Phase 2 (2/2): Evidence Collection & Findings Management

Use the **customer's** issue tracking tool if possible!

Advantages:

- Cross-references between tickets and different assessments
- Provides central dashboards and management reports
- Follow-up on business-as-usual (BAU) activities
- Have all historical data in one tool

PCI Security Standards Council

Process Phase 3 (1/2): Reporting

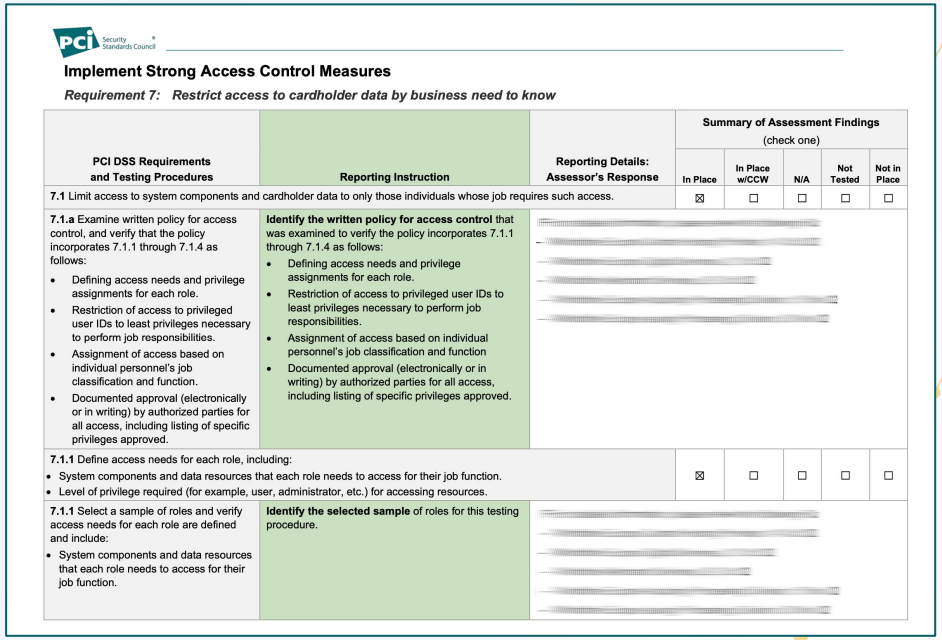
- Worldline harmonised entities are covered by **central / business line** RoCs and AoCs.
- RoCs contain **cross-references** to the central hosting RoC where needed.
- All entities will also be covered in a **frame RoC** with an overall AoC.

PCI Security Standards Council

Process Phase 3 (2/2): Frame RoC / AoC

The PCI DSS Frame RoC / AoC covers the following entities:

1. Entities that were assessed in the central assessment
2. Entities that were validated independently during the year and were chosen to be integrated into the central assessment for the following year (no separate listing required)



Implement Strong Access Control Measures

Requirement 7: ***Restrict access to cardholder data by business need to know***

PCI DSS Requirements and Testing Procedures	Reporting Instruction	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)				
			In Place	In Place w/CCW	N/A	Not Tested	Not in Place
7.1 Limit access to system components and cardholder data to only those individuals whose job requires such access.			☒	☐	☐	☐	☐
7.1.a Examine written policy for access control, and verify that the policy incorporates 7.1.1 through 7.1.4 as follows: • Defining access needs and privilege assignments for each role. • Restriction of access to privileged user IDs to least privileges necessary to perform job responsibilities. • Assignment of access based on individual personnel's job classification and function. • Documented approval (electronically or in writing) by authorized parties for all access, including listing of specific privileges approved.	**Identify the written policy for access control** that was examined to verify the policy incorporates 7.1.1 through 7.1.4 as follows: • Defining access needs and privilege assignments for each role. • Restriction of access to privileged user IDs to least privileges necessary to perform job responsibilities. • Assignment of access based on individual personnel's job classification and function • Documented approval (electronically or in writing) by authorized parties for all access, including listing of specific privileges approved.	[redacted]					
7.1.1 Define access needs for each role, including: • System components and data resources that each role needs to access for their job function. • Level of privilege required (for example, user, administrator, etc.) for accessing resources.			☒	☐	☐	☐	☐
7.1.1 Select a sample of roles and verify access needs for each role are defined and include: • System components and data resources that each role needs to access for their job function.	**Identify the selected sample** of roles for this testing procedure.	[redacted]					

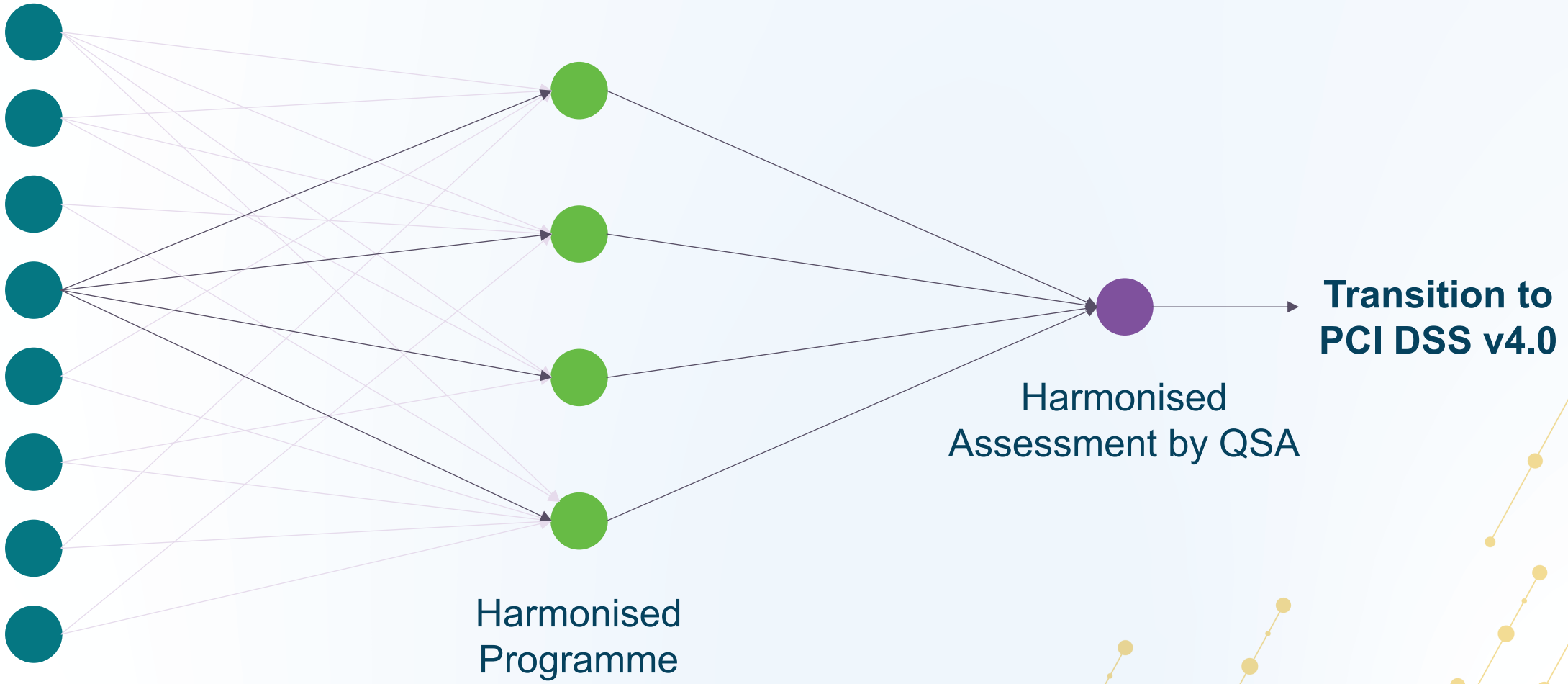
PCI Security Standards Council

PCI Security Standards Council

PCI DSS v4.0 Transition

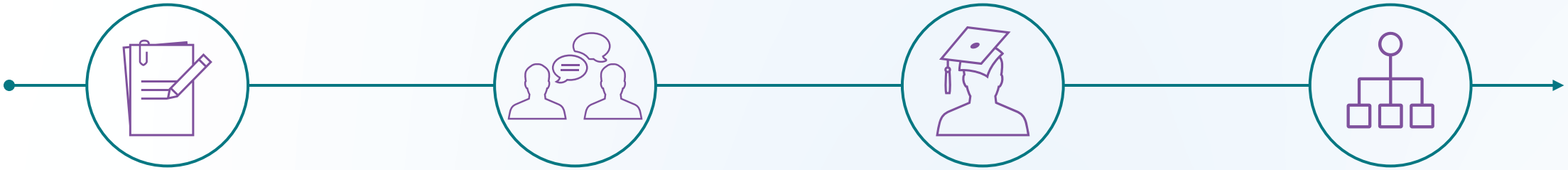
How do we move forward with PCI DSS v4.0?

Journey Continues: Transition to PCI DSS v4.0



PCI Security Standards Council

PCI DSS v4.0 Transition: Initial Phase



Being involved in the RfC Period

GAP Analysis / Workshops

Training Experts & Stakeholders

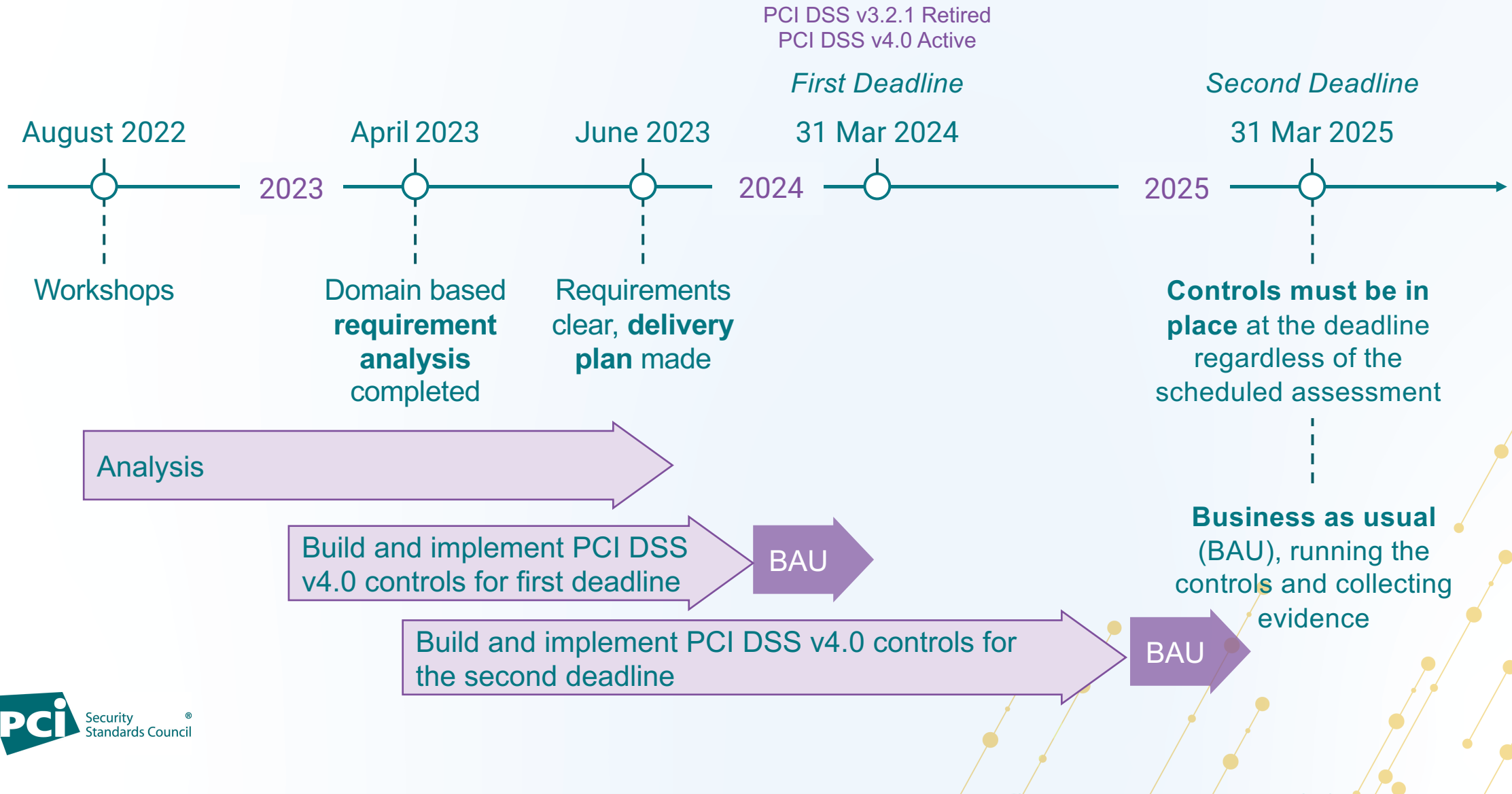
Grouping the Requirements & Controls

Total number of requirements with relevant changes: 76 (30 %)

High-impact changes:	Effective 04/24	Effective 04/25
	6	27

PCI Security Standards Council

PCI DSS v4.0 Transition: Project Phase



PCI Security Standards Council

PCI DSS v4.0 Transition: Practical Insights

Continuous training & workshops to raise awareness and leverage expertise

Regular Q&A sessions for all entities

Close contact to PCI SSC

Use Global PCI Progamme initiatives and tools

Monitoring the status with QSA

PCI Security Standards Council

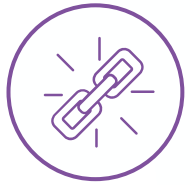
Key Take-Aways

How harmonisation can help to improve your PCI DSS strategy

Harmonised controls help reduce the assessment effort and increase efficiency

Increased IT security level through standardisation and best practice implementations

Use a business-centric PCI organisation to leverage PCI expertise. Supports scalability and adaptability



Centralised approach helps manage big transitions such as the one to PCI DSS v4.0

Any organisation can benefit from a PCI DSS harmonisation programme. Large organisations can't do without.

THANK YOU