2025
NORTH
AMERICA
COMMUNITY
MEETING

Navigating PCI Compliance at Scale:

Managing Service Providers & Assurance

Simon Turner

CISSP, CISM, CISA, VCP, PCI ISA
Head of Security Governance & Compliance
British Telecommunications (BT Group)

BT Group

Managing PCI DSS Scope at Scale

The complexity of managing hundreds of service providers in a regulated environment

The risks of third-party dependencies in PCI DSS compliance

The challenge of balancing security, compliance, and business agility

Why this is a challenge for organisations of all sizes

The Scale of Our PCI DSS Environment

eCommerce

- BT Buynet - PSP
- iFrame
  15 Web Sites
- AWS Hosted
- On Prem Hosted

Contact Centres

- BT Buynet PSP
- DTMF Masking
- Pause & Resume
- 32 Contact Centres
- 18,000 Agents

Retail Stores

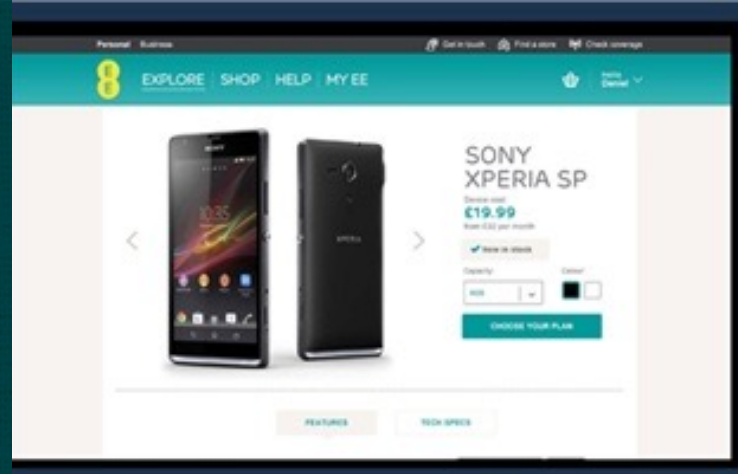
- BT Buynet PSP
- P2PE
- Pay by Link
- 450 Stores
- 3,500 Retail Staff

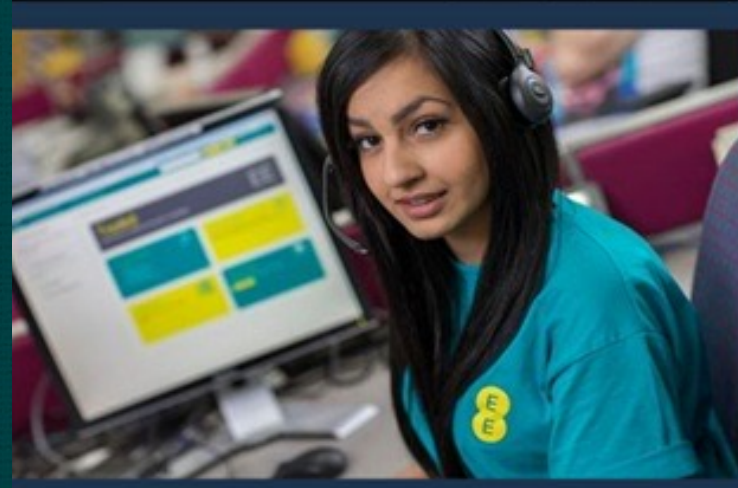
BT Business

- BT Buynet/BT Pay
- Cloud Contact PCI
- Cardway
- Data Center
- Managed Services
- BIDS/RFP/ITT

Service Provider Types

- PSPs
- Contact Centre Services
- Fraud Services
- Hosting
- Development
- Support
- DTMF Providers
- Insurance Services
- Financial Services
- Physical Storage
- Other





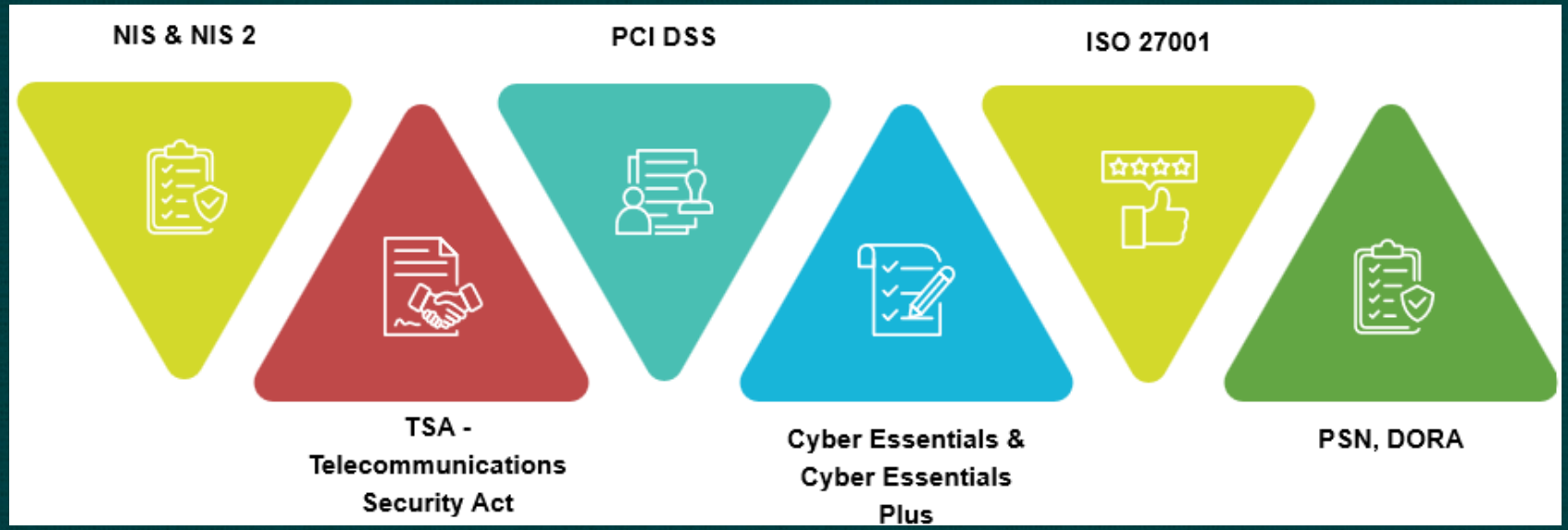
Compliance Obligations

NCSC Security Framework

Cyber Assess comprehensive set of principles, guidance, and best practice Framework

Key Controls

foundational to building a robust cybersecurity posture and align with the core principles of risk management, prevention, detection, and response



“Compliance As A Consequence”

The Evolution of Our Approach

(From Reactive to Proactive)

Initial challenges: Ad-hoc service provider assessments, fragmented visibility

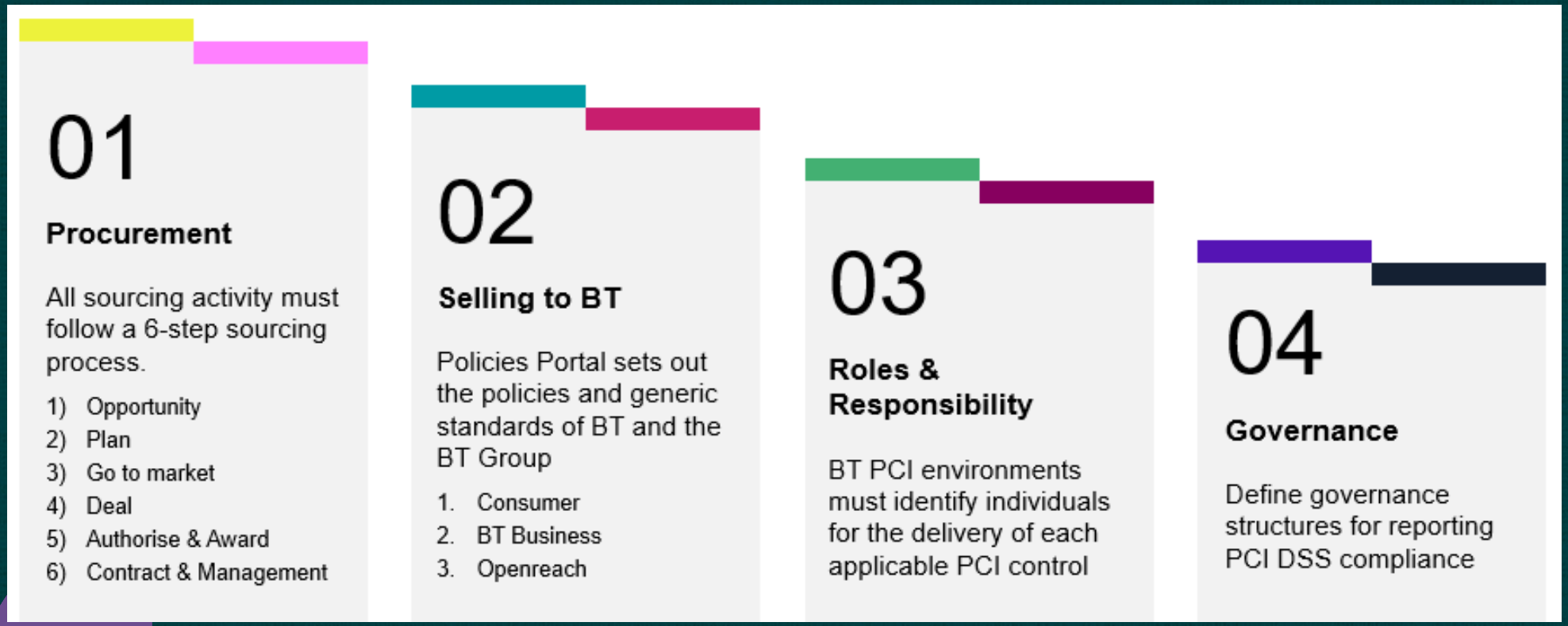
Lessons learned: The need for structured governance, automation, and engagement

Our mindset shift: Viewing service provider management as a continuous lifecycle, not a one-time checklist

Engaging with Business

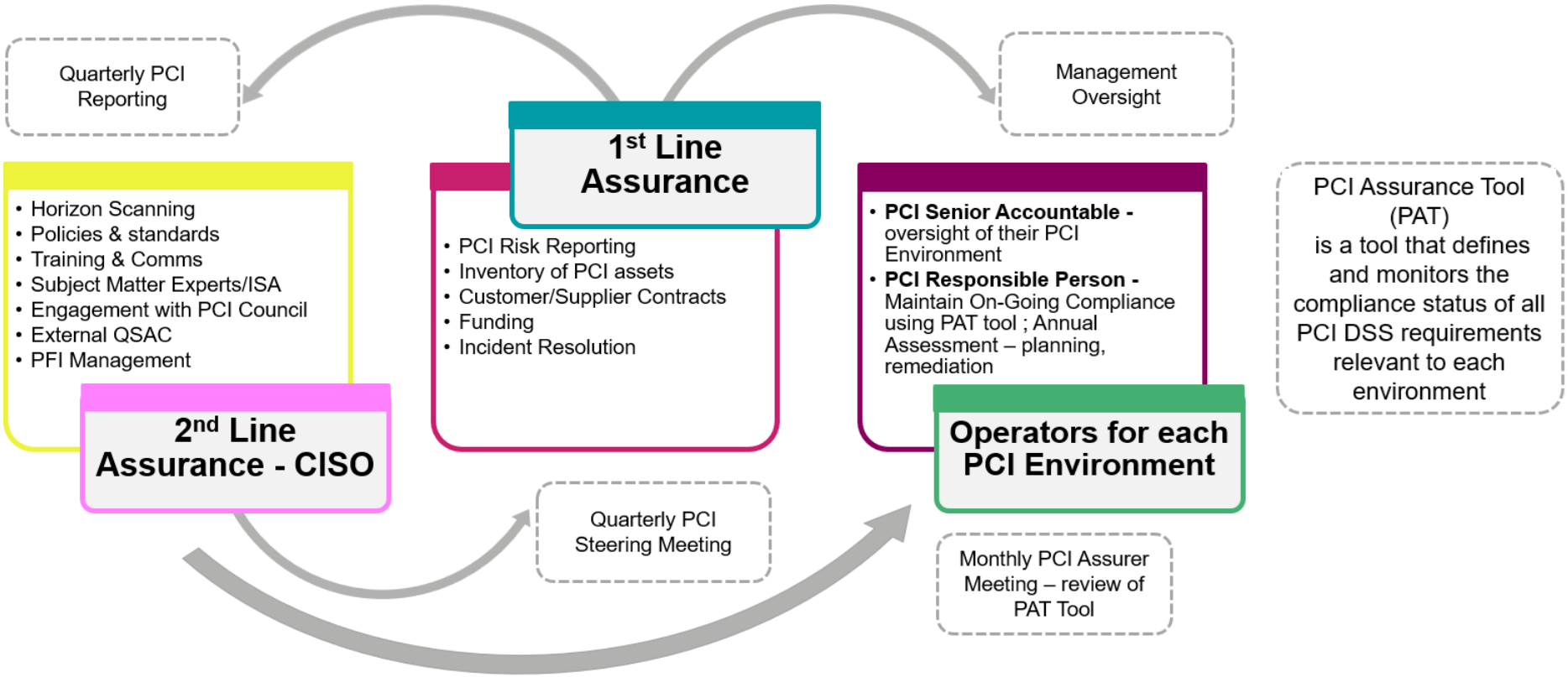
Howard Watson, CTIO is accountable for PCI security compliance on behalf of the Executive Committee (ExCo) – the executive management team for BT in support of the Group Chief Executive, Allison Kirkby.

“Compliance As A Consequence”



Business As Usual PCI DSS Governance Structure and Processes

BT operates a 3 Lines of Assurance Model, and this has been applied to our PCI DSS Environments

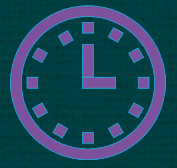


Effective Service Provider Management

Onboarding & Risk Categorisation

Due Diligence & Validation

Ongoing Monitoring & Compliance Assurance



Collaboration & Continuous Improvement

Governance & Oversight

Onboarding & Risk Categorisation

It’s important to classify service providers by risk, ensuring contractual security clauses and compliance validation match their risk level from onboarding onward.

01

Risk-based Classification

- Critical
- Significant
- Platform
- Gorilla
- Ancillary

02

Supplier Categories

- Skilled Resource Provider
- Technical Services Support
- Development and Maintenance
- Contract / Channel Partner
- Ethical

03

Contractual Security Clauses

- BT Legal
- BT PCI Supplier Policy (Extranet)
- BT QSA/ISA Review

Due Diligence & Validation

We use **standard security questionnaires** and **AOCs**, escalating to deeper assessments based on risk.

04

Standardised Security Questions

- BT Procurement
- Supply Chain Security Process

05

PCI Certification Requirements

- QSA Validated AOC
- Service Provider AOC – L1
- Responsibility Matrix
- ASV Scans
- Contractual Committal to Annual AOC Submission

06

BT PCI Team Validation

- Front Door Request
- BT QSA/ISA Review
- Tracking

Ongoing Monitoring & Compliance Assurance

We combine **continuous monitoring tools** for compliance drift detection with **annual validation cycles** to ensure real-time assurance

07

PCI Responsibilities (BAU)

- PCI Assurance Tool (PAT)
- PCI Supplier Tracker
- 1st Line – PCI Responsible
- 2nd Line – PCI Assurer (ISA)
  - Responsible for tracking
- 2nd Line – PCI QSA

08

Security Risk Assessment

- Right to Audit
- Frequency based on Risk Category
- Custom set of controls
- Validate AOC vs Offerings
- Follow up on Remediation

09

Governance

- Quarterly PCI Return
- List of 3rd Parties
- Certification Dates
- Services Provided

Governance & Oversight

Our governance framework includes **board-level reporting, KPIs, and structured oversight.**

10

Key Governance Reporting

- PCI Merchant Forum (1/4)
- BT Security Forum (monthly)
- BT Quarterly Returns (1/4)
- CFU CTIO - Escalation

11

Key Performance Indicators

- % of Complaint Service Providers
- Number of Security Incidents
- Time taken for Risk Remediation
- Assessment Pass Rate

12

Governance Structure

- 3 Lines of Defence
- CISO / CTO
- BT ExCO

A Real-World Example

Example 1 – 3rd Party Contact Centre

- Third-party contact center manages incoming calls for EE's sales and services
- BT Telephony for inbound calls.
- Outbound calls own telephony
- Ensuring seamless customer interactions and efficient call handling

Example 2 – UCaaS & CCaaS Provider

- White-labeled for a BT Business Service
- Third-party UCaaS & CCaaS Provider - delivers VoIP & Contact Centre Solutions
- Supports DTMF masking for secure payment processing
- Enhanced Data Protection

Final Thoughts

Final Thoughts

Visibility: Gaining a Clear Picture

- Complex ecosystem of providers, making PCI DSS scope hard to track.
- Limited transparency into providers' real-time security posture.

Assurance: Beyond Tick-Box Compliance

- Providers may be compliant on paper but weak in practice.
- Challenges enforcing PCI DSS requirements through contractual agreements.

Ongoing Monitoring: From Static to Dynamic Risk Management

- Annual compliance checks don't account for daily evolving risks.
- Manual processes slow response – need for automation & continuous monitoring

A Centralised PCI DSS-Managed Service Provider Registry – A Game Changer

A Proposed Solution: PCI Council-Managed Service Provider Registry

- PCI Council-managed third-party listing - apply for listing.
- PCI Council reviews and validates AOCs, ensuring the description of services is accurate.
- RMs are standardised and reviewed, clarifying shared responsibilities between merchants and providers.
- Merchants can search for listed providers, similar to how they find QSAs, ISAs, and P2PE solutions today.

Any Questions

simon.p.turner@bt.com

PCI Security Standards Council®

2025 NORTH AMERICA COMMUNITY MEETING