Security Delivery Done Right: Turning Intent into Impact





Simon Turner
Head of Security Governance and Compliance (BT Group)

Brendan Keenan
Head of Cyber Strategy & Transformation (BT Group)

Opening perspective

Compliance as a Consequence

Compliance follows transformation delivery. It is not the starting point.

The objective is not to chase compliance.

The objective is to transform how the business works so the right controls, evidence and accountability become part of normal operations.

Well-designed security

Effective transformation

Clear accountability

Sustainable operating model

Fireside discussion question

How do we turn this principle into change that works at scale?

20 YEARS OF SECURING PAYMENT DATA
PCI Security Standards Council

The problem was bigger than security technology

The visible symptoms were technical. The root causes were ownership, alignment and repeatability.

Traceability
Risks needed to trace into controls, standards and measurable outcomes.

Alignment
Strategy needed to connect to roadmaps, investment and governed action.

Ownership
Delivery needed named accountable owners across organisational boundaries.

Without traceability, alignment and ownership, transformation becomes activity rather than outcome.

20 YEARS OF SECURING PAYMENT DATA
PCI Security Standards Council

Why traditional transformation struggles

The challenge wasn't a lack of activity. It was a lack of connection.

Projects

Lots of good initiatives, No single view of their combined impact.

Stakeholders

Responsibility was shared. Accountability wasn’t.

Reporting

Progress was visible. Outcomes weren’t.

Ownership

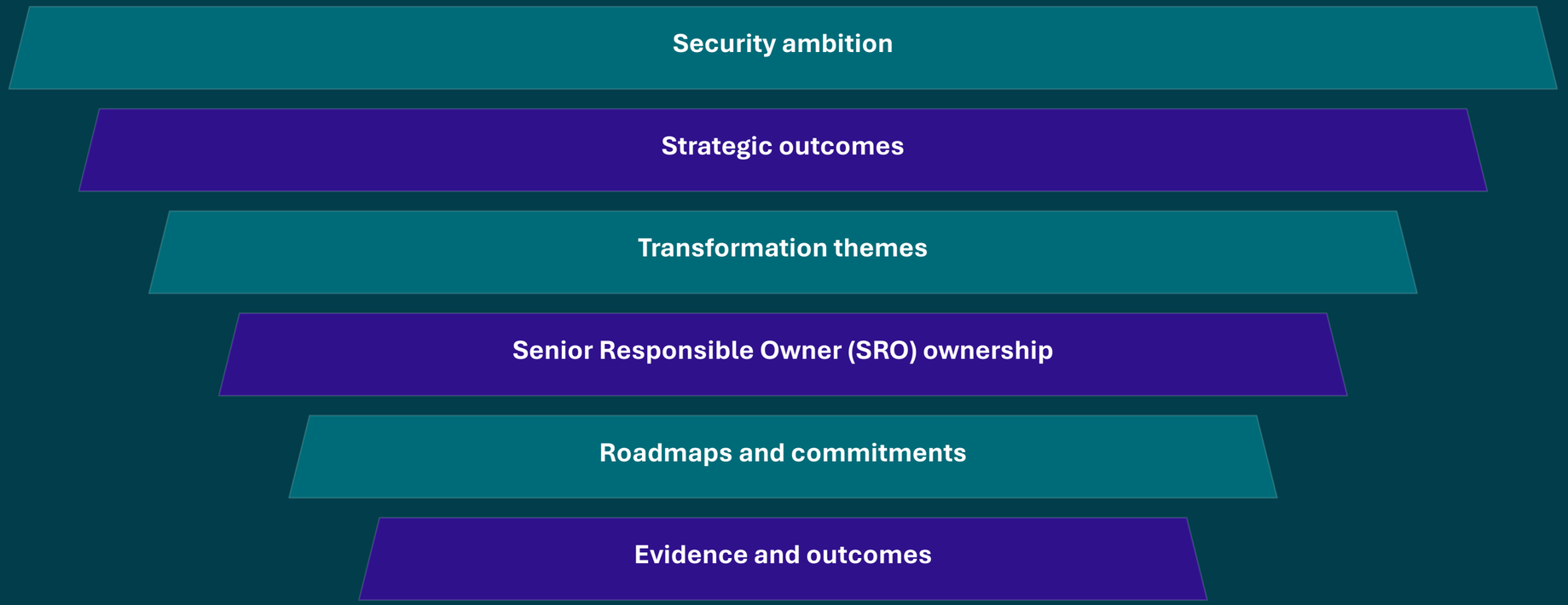
When delivery crossed organisational boundaries, ownership became blurred.

We didn't need another programme. We needed a way to connect strategy, ownership and delivery.

20 YEARS OF SECURING PAYMENT DATA
PCI Security Standards Council

The breakthrough: strategy became a system

We created a visible chain from intent to outcome.



If you cannot trace the work back to strategy, it is probably activity, not transformation.

20 YEARS OF SECURING PAYMENT DATA
PCI Security Standards Council

The golden thread created confidence

Every discussion could move from strategy to ownership to evidence.



20 YEARS OF SECURING PAYMENT DATA
PCI Security Standards Council

From Programme to movement

The moment people ask “what am I doing?” instead of “what is the Programme doing?” the change has started to embed.

Ownership

Visibility

Accountability

20 YEARS OF SECURING PAYMENT DATA
PCI Security Standards Council

The SRO model made ownership visible

Accountability sat with senior owners; execution was supported through responsible owners; delivery leads and a lean Centre.

1

Senior Responsible Owner

Accountable for outcomes, governance and benefits.

2

Responsible Owners + Delivery Leads

Translate outcomes into roadmaps, dependencies and evidence.

3

Lean transformation Centre

Creates the rhythm: governance, reporting, escalation and visibility.

20 YEARS OF SECURING PAYMENT DATA
PCI Security Standards Council

We scaled accountability, not bureaucracy

The centre created clarity. The organisation delivered the transformation.

Common trap

- Large Centre owns plans
- Status reporting dominates
- Business units are recipients
- Escalation becomes the culture

What we chose

- Lean Centre creates rhythm
- SROs own outcomes
- Teams deliver roadmaps their way
- Escalation removes blockers

20 YEARS OF SECURING PAYMENT DATA
PCI Security Standards Council

The rhythm mattered as much as the model

Governance did not exist to admire progress. It existed to unblock it.

Monthly STB (Security Transformation Board)
progress, decisions and items needing support

Jira visibility
delivery, risks, issues and dependencies in one place

Quarterly commitments
look forward, look back and reset where needed

20 YEARS OF SECURING PAYMENT DATA
PCI Security Standards Council

Embedding starts before the ending

The test of transformation is not the final board pack. It is what still works when the programme stops.

Transfer the ownership
Capabilities, controls and improvement backlogs move into BAU teams.

Keep the evidence visible
Metrics and assurance keep colleagues connected to the risk they manage.

Make improvement continuous
Lessons, roadmaps and governance continue outside programme closure.

If it only lives in the Programme, it has not landed.

20 YEARS OF SECURING PAYMENT DATA
PCI Security Standards Council

Five lessons I would share externally

Make these feel like hard-won lessons, not a methodology sales pitch.

1. **Start with the outcome, not the org chart**
2. **Make the strategy traceable to delivery**
3. **Give accountability a named owner**
4. **Use governance to remove friction**
5. **Design the handover before the finish line**

20 YEARS OF SECURING PAYMENT DATA
PCI Security Standards Council

Most organisations think transformation is about changing technology.

We learned it is about changing ownership.

When ownership changes, behaviour changes.

When behaviour changes, culture changes.

And when culture changes... transformation sticks.

Build the model so the work can outlive the programme.

20 YEARS OF SECURING PAYMENT DATA
PCI Security Standards Council

Transformation delivery makes compliance inevitable

Brendan’s delivery perspective is the mechanism that makes the principle real.

1

Align stakeholders

Create shared ownership and a reason to act.

2

Remove friction

Make the secure route easier to deliver.

3

Measure progress

Track changed outcomes, not just completed activity.

4

Embed the change

Move ownership into BAU processes and operational teams.

Closing message

When transformation is delivered effectively, controls become embedded, evidence becomes repeatable and compliance becomes a consequence of how the organisation operates.

20 YEARS OF SECURING PAYMENT DATA
PCI Security Standards Council

COMPLIANCE AS A CONSEQUENCE”

“Compliance is not something you chase, retrofit, or prepare for - it is the natural outcome of well-designed security, architecture, governance, and operating models.”

BT Group

20 YEARS OF SECURING PAYMENT DATA
PCI Security Standards Council