PCI Security Standards Council

Third-Party Service Providers – Forging a Quality Relationship

Peter O'Sullivan
Principal Information Security Consultant, Nettitude Ltd.

Who am I?

“Why is he talking about this?”

LRQA NETTITUDE

Peter O’Sullivan

- Principal Information Security Consultant
- LRQA Nettitude
- QSA since 2015
- 3DS-QSA since 2019
- GEAR Representative

Have too many conversations about Service Providers

Had a full head of hair when I qualified in 2015

PCI Security Standards Council

Who are LRQA Nettitude?

Trusted leaders in cybersecurity

Helping clients prioritise and mitigate cybersecurity risk

- QSA Company since May 2009
- Award-winning organisation with over 20 years of experience.
- Quality, highly sophisticated technical capabilities, backed by demonstrable industry accreditations and certifications.
- The only organisation in the world with a full suite of CREST accreditations.
- Active participation in financial & government-led cybersecurity-regulated frameworks.
- Dedicated research & innovation team focused on developing and exploring ideas including core tooling, honey traps, zero-day exploits, blockchain, and SOC maturity.

PCI Security Standards Council

LRQA NETTITUDE

Agenda

- The Effects upon Compliance
- The Demanding Client
- Going to the shops
- PCI DSS v4.0 and TPSP

PCI Security Standards Council

PCI Security Standards Council

The Effects upon Compliance

A Third-Party Service Provider causing a problem – is that really fair to say?

There a gap in compliance

“Do you realise what this means to me?”

Impact of this outcome:

- Assessment result
- Conversations with banks
- Reassessment costs
- Scope change
- Pain and anxiety
- Cessation of service

PCI Security Standards Council

The QSA says you're Non-Compliant

"How on earth did that happen?"

Reasons seen:

- Puffing
- Attestation of Compliance mismatch
- Contract challenges
- Misunderstanding of Responsibilities
- Service Provider push-back
- SAQ Type ≠ SAQ D-SP

PCI Security Standards Council

The QSA says you're Non-Compliant

"Prevention is better than a cure"

Quality Due Diligence Processes:

- ✓ NDA/Confidentiality BEFORE signing/buying
- ✓ Comprehensive Contract
- ✓ Responsibility Matrix
- ✓ Service Provider Attestation of Compliance
- ✓ QSA Support (as necessary)
- ✓ Ongoing service management
- ✓ Business as Usual
- ✓ Stay in your lane

PCI Security Standards Council

PCI Security Standards Council

The “Demanding” Client

“Is that a me problem or a you problem?”

The “Demanding” Client

“Is that a me problem or a you problem?”

Impact of this outcome:

- Poor customer relationships
- Lost of trust and reputation
- Increased cost and effort
- Limited business opportunities
- Competitive disadvantage

PCI Security Standards Council

The “Demanding” Client

“Is that a me problem or a you problem?”

Reasons Seen:

- Education and awareness
- Situational context and the PCI DSS
- Descriptions in Attestation of Compliance
- Vagueness in Responsibility Matrix
- Being blinkered by the client
- Perpetuation of Misinformation

PCI Security Standards Council

The “Demanding” Client

“Fixing my problems”

Your compliance offering:

- ✓ Service Provider Attestation of Compliance
- ✓ Ignore FAQ 1331 – you are not a merchant
- ✓ Contracts containing relevant PCI DSS terminology
- ✓ Service names, descriptions and BAU
- ✓ Responsibility Matrix
  - ✓ For your client
  - ✓ For scoping your own assessment
  - ✓ Shared responsibilities
- ✓ Acknowledge responsibility; commit to compliance.
- ✓ Transparent and easily available

PCI Security Standards Council

PCI Security Standards Council

Let Go Shopping!

Selecting a Third-Party Service Provider

Selecting a Third-Party Service Provider

Creating a partner relationship not finding a supplier”

What do you need:

- See “*Prevention is better than a cure”*
- Sequencing
- Functional vs Non-functional requirements
- NDAs to complete rigorous due-diligence
- Risk Management
- General Vendor and Service Management
- Recognise transparency or blocking
- Engage with your QSA

PCI Security Standards Council

PCI Security Standards Council

The Impact of PCI DSS v4.0

For Merchants and Service Providers

The Impact of PCI DSS v4.0

Requirement 12.8 and 12.9

Factors and Actions:

- Contract Wording and Reviews
- Different versions between merchants and service providers
    - Mapping between versions
    - Responsibility Matrix
- Future dated requirements
    - Anniversary dates
    - Implementation impact
- Customer Journeys and TPSP
- Start a dialogue sooner than later

PCI Security Standards Council

Conclusions and Takeaways

““What have we learned?”

Observations, Top Tips and Tricks

- ✓ Complete all due-diligence before you sign
- ✓ Service Provider Attestation of Compliance only
- ✓ Read the small print and big print
- ✓ Ensure documentation shows the TPSPs responsibilities
- ✓ Helping achieve compliance vs Responsible for compliance
- ✓ Responsibility Matrix is valuable for both parties – make them count
- ✓ Transparency of compliance is an enabler
- ✓ Establish a common goal – *protecting cardholder data*.

PCI Security Standards Council