PCI Data Security Standard: Advanced - Training Overview

Session 1: Fitting PCI Into Your Security Program	
Subject: What is Real Security *To 'operationalise' PCI compliance, we must first agree of what a security program actually looks like.* Session Objective: To put security and PCI into a *business* context.	09:00 – 10:30
Subject: Scoping and Descoping *Regardless of how you approach PCI, there will be in-scope and out of scope systems. How you treat these is critical.* Session Objective: To understand why the scope of your systems is driven by a data classification policy, not by the DSS.	
Subject: Compensating Controls *Behind every requirement is an intent, and the only way to NOT follow the DSS is to write a compensating control.* Session Objective: To understand how compensating controls can negate almost every DSS requirement as written.	
Morning Break	10:30 – 10:45

Session 2: Outsourcing and Due Diligence	
Subject: Outsourced Service Providers *Unless taking payment is core to your business, why do it yourselves?* Session Objective: To understand the many benefits (and risk reduction) of outsourcing your payments channels.	10:45 – 12:15
Subject: Assessing Cloud Infrastructure *The PCI DSS was not written for virtualisation/cloud, but that's the way the industry is going.* Session Objective: To understand how to 'translate' the PCI DSS into as-a-service options.	
Subject: Using PCI Assessment as 'Certification' Evidence *There's no reason PCI assessment validation evidence cannot count as ISO 27001 certification 'records'.* Session Objective: How to treat PCI validation no differently from standard operational auditing.	
Lunch Break	12:15 – 13:15

PCI Data Security Standard: Advanced - Training Overview

Session 3: Requirements - Part 1	
Subject: Requirements 1 ('Networking') & 2 ('Configuration Standards') *Deep-dive into the alternatives to and operationalisation of requirements 1 and 2.* Session Objective: How to operationalise requirements 1 & 2 to demonstrate real-world security.	13:15 – 14:45
Subject: Requirements 3 ('Storage Encryption') & 4 ('Transmission Encryption') *Deep-dive into the alternatives to and operationalisation of requirements 3 and 4.* Session Objective: How to operationalise requirements 3 & 4 to demonstrate real-world security.	
Subject: Requirements 5 ('Anti-Malware') & 6 ('Vulnerability Management / Secure Coding') *Deep-dive into the alternatives to and operationalisation of requirements 5 and 6.* Session Objective: How to operationalise requirements 5 & 6 to demonstrate real-world security.	
Afternoon Break	14:45 – 15:00

Session 4: Requirements - Part 2	
Subject: Requirements 7 ('Access Control') & 8 ('Credentials') *Deep-dive into the alternatives to and operationalisation of requirements 7 and 8.* Session Objective: How to operationalise requirements 7 & 8 to demonstrate real-world security.	15:00 – 16:30
Subject: Requirements 9 ('Physical Security') & 10 ('Logging & Monitoring') *Deep-dive into the alternatives to and operationalisation of requirements 9 and 10.* Session Objective: How to operationalise requirements 9 & 10 to demonstrate real-world security.	
Subject: Requirements 11 ('Testing') & 12 ('Policy') *Deep-dive into the alternatives to and operationalisation of requirements 11 and 12.* Session Objective: How to operationalise requirements 11 & 12 to demonstrate real-world security.	
Subject - Discussion, Q&A	