PCI Data Security Standard: Beginners - Training Overview

Session 1: Background	
Subject: A Brief History of the PCI DSS *The PCI DSS was first published by Visa on December 15th, 2004 and was a total of 12 pages in length. Version 3.2.1 is 139 pages in length, how did it get here?* Session Objective: To provide context for the training by briefly touching on what where the PCI DSS came from.	09:00 – 10:30
Subject: The Security Standards Council (SSC) and Other PCI Security Standards *Founded in 2006, the SSC was paid for by the 5 major card brands (Visa, Mastercard, Amex, Discover, JCB) and they now 'own' all of the PCI standards. Of which there are several.* Session Objective: How the PCI 'ecosystem' all fits together.	
Subject: What is a Payment? *The PCI standards cover every aspect of a payment, what are they.* Session Objective: To understand how a payment works between all of the industry player and intermediaries.	
Morning Break	10:30 – 10:45

Session 2: Reporting	
Subject: Merchant and Service Provider Levels *Depending on what you do, and how many transaction you process, you need to do slightly different things.* Session Objective: To understand your PC obligations based on your business type and transaction volume.	10:45 – 12:15
Subject: Report on Compliance (RoC) vs Self Assessment Questionnaires (SAQ) *How you report your compliance varies considerably, from RoC to one of 9 SAQs.* Session Objective: To understand exactly which report you'll be filling out.	
Subject: Scoping and Compliance Validation *Once you know how to report, what do you have to do to validate your compliance. This varies dramatically.* Session Objective: To understand exactly how to validate you compliance to relevant interested parties.	
Lunch Break	12:15 – 13:15

PCI Data Security Standard: Beginners - Training Overview

Session 3: Requirements - Part 1	
Subject: Requirements 1 (‘Networking’) & 2 (‘Configuration Standards’) *High-level review of requirements 1 and 2.* Session Objective: To understand the *intent* of requirement 1 & 2 and what they mean in the real-world.	13:15 – 14:45
Subject: Requirements 3 (‘Storage Encryption’) & 4 (‘Transmission Encryption’) *High-level review of requirements 3 and 4.* Session Objective: To understand the *intent* of requirement 3 & 4 and what they mean in the real-world.	
Subject: Requirements 5 (‘Anti-Malware’) & 6 (‘Vulnerability Management / Secure Coding’) *High-level review of requirements 5 and 6.* Session Objective: To understand the *intent* of requirement 5 & 6 and what they mean in the real-world.	
Afternoon Break	14:45 – 15:00

Session 4: Requirements - Part 2	
Subject: Requirements 7 (‘Access Control’) & 8 (‘Credentials’) *High-level review of requirements 7 and 8.* Session Objective: To understand the *intent* of requirement 7 & 8 and what they mean in the real-world.	15:00 – 16:30
Subject: Requirements 9 (‘Physical Security’) & 10 (‘Logging & Monitoring’) *High-level review of requirements 9 and 10.* Session Objective: To understand the *intent* of requirement 9 & 10 and what they mean in the real-world.	
Subject: Requirements 11 (‘Testing’) & 12 (‘Policy’) *High-level review of requirements 11 and 12.* Session Objective: To understand the *intent* of requirement 11 & 12 and what they mean in the real-world.	
Subject - Discussion, Q&A	