PCI-DSS ver. 3.2.1 (Payment Card Industry Data Security Standard) Implementation Training

Course Details

Course Outline

Day – 1

- What is PCIDSS 3.2.1 and its purpose
- Payment Transaction Flow
- Merchant levels and Service provider levels
- SAQ types and reporting requirements
- Card holder data discovery
- Scoping the Cardholder Data Environment
- Segmentation
- Req.1 – Install and maintain a firewall configuration
- Req.2 – Do not use vendor – supplied defaults for system passwords
- Req. 3 – Protect stored card holder data
- Req. 4 – Encrypt transmission of card holder data across open and public networks

Day – 2

- Quiz
- Req. 5 - Protect all systems against malware and regularly update anti-virus
- Req. 6 - Develop and maintain secure systems and applications
- Req. 7 - Restrict access to cardholder data by business need to know
- Req. 8 - Identify and authenticate access to system components
- Req. 9 - Restrict physical access to cardholder data
- Req. 10 - Track and Monitor all access to network resources and cardholder data
- Req. 11 - Regularly test security systems and processes
- Req. 12 - Maintain a policy that addresses information security for all personnel
- Q and A Session
- Appendix A
- Exam