

ETAU LEVEL II: DATA SECURITY ESSENTIALS COURSE OUTLINE

Learning Objectives:

At the end of the course, participants should be able to:

- Define “compliance” and “validation” within PCI
- Understand the various card brand compliance requirements and technical aspects of the PCI Data Security Standard
- Identify how the payment card security standards apply to their environment and how to address shortcomings

I. Importance of Data Security

- ❖ Public relations
- ❖ Regulatory
- ❖ Effects of a compromise

II. Card Company Policies vs. PCI

- ❖ PCI and the PCI-SSC
- ❖ Data Security Standard changes
- ❖ Compliance vs. validation

III. Card Company Requirements

- ❖ Compliance statements
- ❖ Merchant levels, validation and reporting
- ❖ Service provider levels, validation and reporting
- ❖ Additional resources/tools

IV. PCI Data Security Requirements

- ❖ Data to protect
- ❖ How to protect
- ❖ Details of the Data Security Standard
 - Build and maintain a secure network
 - Protect cardholder data
 - Maintain a vulnerability management program
 - Implement strong access control measures
 - Regularly monitor and test networks
 - Maintain an information security policy

V. Case Study Review and Best Practices

- ❖ Covers a typical security breach, including remediation steps