Faculty Workshops

Curriculum Alignment Governance, Risk Management and Compliance (GRC)

This workshop addresses the knowledge and skills need to students to be prepared for the Qualified Security Assessor (QSA) exam. A Qualified Security Assessor is a person who has been certified by the PCI Security Standards Council to audit merchants for Payment Card Industry Data Security Standard (PCI DSS) compliance.

The GRC workshop will teach you how to perform assessments of merchants and service providers who must comply with the PCI Data Security Standard. The course focuses on the 12 high level control objectives and corresponding sub-requirements that are required for compliance. Split into two parts, the course consists of an online component and a two-day instructor-led session.

# The 12 requirements of the PCI DSS

|  |
| --- |
| Lab 1 – Build, Maintain and Test Network and Workstation FirewallsInstall, maintain and test a firewall configuration to protect cardholder dataFirewalls control the transmission of data between an organization’s trusted internal networks and untrusted external networks, as well as traffic between sensitive areas of the internal networks themselves. Requirement 1 of the PCI DSS requires systems to use firewalls to prevent unauthorized access. Where other system components provide the functionality of a firewall, they must also be included in the scope and assessment of this requirement. |
| Lab 2 - Password Security Implementation and Testing Do not use vendor-supplied defaults for system passwords and other security parametersThe default settings of many commonly used systems are well known, easily exploitable and often used by criminal hackers to compromise those systems. Vendor-supplied default settings must, therefore, be changed, and unnecessary default accounts disabled or removed before any system is installed on a network. This applies to all default passwords, without exception. If firewalls are correctly implemented according to Requirement 1, they should also comply with Requirement 2. |
| Lab 3 – Data Encryption and Decryption Protect and test security of stored cardholder dataThe storage of cardholder data should be kept to a minimum, and appropriate data retention and disposal policies, procedures and processes should be implemented. Certain data – such as the full contents of the chip or magnetic strip, the CVN (card verification number) or the PIN (personal identification number) – should never be stored. When data is stored, it should be stored securely. Encryption, truncation, masking and hashing are critical components of cardholder data protection. Without access to the proper cryptographic keys, encrypted data will be unreadable and unusable by criminal hackers, even if they manage to circumvent other security controls. Cryptographic keys should therefore be stored securely and access restricted to the fewest custodians necessary. Other data protection methods should also be considered. |
| Lab 4 – Virtual Private Network (VPN) Configuration and Testing Encrypt and test the encryption of transmission of cardholder data across open, public networksStrong cryptography and security protocols (e.g. TLS, IPSec, SSH, etc.) should be used to safeguard sensitive cardholder data during transmission over open, public networks that could easily be accessed by malicious individuals. Examples of open, public networks include the Internet, wireless technologies (e.g. Bluetooth), GPRS (general packet radio service) and satellite communications. Industry best practices must be followed to implement strong encryption for authentication and transmission. Security policies and procedures for encrypting the transmission of cardholder data must be documented and made known to all affected parties. |
| Lab 5 – Antivirus and Malware Scanning and ComplianceProtect and test all systems against malware and regularly update antivirus software or programsAntivirus software capable of detecting, removing and protecting against all known types of malware (e.g. viruses, worms and Trojans) must be used on all systems commonly affected by malware to protect them from threats. For systems not commonly affected by malware, evolving malware threats should be periodically evaluated to determine if antivirus software is needed. Antivirus mechanisms must be maintained and kept actively running, and should only be disabled if formally authorized for a specific purpose. |
| Lab 6 – Systems Updates, Patching and Compliance Develop, maintain and test secure systems and applicationsMany security vulnerabilities are fixed by patches issued by software vendors. Organizations should establish a process to identify security vulnerabilities and rank them according to their level of risk. Relevant security patches should be installed within a month of their release to protect against cardholder data compromise. All software applications developed internally or externally, should be developed securely in accordance with the PCI DSS. They should also be based on industry standards and/or best practices, and incorporate information security throughout their entire development lifecycle. |
| Lab 7 - Implement System Access Control and Intrusion DetectionImplement and test access control systems to cardholder and sensitive data by business need to knowExploiting authorized accounts and abusing user privileges is one of the easiest ways for criminal hackers to gain access to a system. It is also one of the most difficult types of attack to detect. Documented systems and processes should therefore be put in place to limit access rights to critical data. Access control systems should deny all access by default, and access should be granted on a need-to-know basis and according to the clearly defined job responsibilities of authorized personnel. ‘Need to know’ is defined in the PCI DSS as “when access rights are granted to only the least amount [sic] of data and privileges needed to perform a job”. |
| Lab 8 - Implement Access Control Systems and Compliance*Identify and authenticate access to system components:*The ability to identify individual users not only ensures that system access is limited to those with the proper authorization; it also establishes an audit trail that can be analyzed following an incident. Documented policies and procedures must therefore be implemented to ensure proper user identification management for non-consumer users and administrators on all system components. All users must be assigned a unique ID, which must be managed according to specific guidelines. Controlled user authentication management (e.g. the use of passwords, smart cards or biometrics) should also be implemented and, as three-quarters of all network intrusions exploit weak or stolen passwords, 2FA (two-factor authentication) must be used for remote network access. |
| Lab 9 - Implement strong Physical Access Control and Compliance*Restrict physical access to cardholder data*Electronic data breaches are not the only source of data loss; physical access to systems should also be limited and monitored using appropriate controls. Procedures should be implemented to distinguish between on-site personnel and visitors, and physical access to sensitive areas (e.g. server rooms and data centers) should be restricted accordingly. All media should be physically secured, and its storage, access and distribution controlled. Media should be destroyed in specific ways when no longer required. Devices that capture payment card data via direct physical interaction with the card must be protected from tampering and substitution, and should be periodically inspected. An up-to-date list of these devices should be maintained. |
| Lab 10 – Log Management and Compliance (Michael Masino)Regularly record, track, monitor and test all access logs to network and workstations The use of logging mechanisms is critical in preventing, detecting and minimizing the impact of data compromise. If system usage is not logged, potential breaches cannot be identified. Secure, controlled audit trails must therefore be implemented that link all access to system components with individual users and log their actions. This includes access to cardholder data, actions taken by individuals with root or administrative privileges, access to audit trails, invalid logical access attempts, use of and changes to identification and authentication mechanisms, the initializing, stopping or pausing of audit logs, and the creation and deletion of system-level objects. An audit trail history should be retained for at least a year, with a minimum of three months’ logs immediately available for analysis. Logs and security events should be regularly reviewed to identify anomalous or suspicious activity. |
| 11 - Regularly Monitor and Test NetworksRegularly monitor, evaluate and test security systems and processesNew vulnerabilities are regularly found and exploited, so it is essential that system components, processes and custom software are regularly tested. Documented processes must be implemented to detect and identify all unauthorized wireless access points on a quarterly basis. Internal and external network vulnerability scans must be performed by qualified personnel at least quarterly and after any significant change in the network (e.g. new system component installations, changes in network topology, firewall rule modifications and product upgrades). Intrusion detection/prevention techniques should be used to identify and/or prevent unauthorized network activity, and a change detection mechanism should be employed to perform weekly critical file comparisons, and to alert personnel to unauthorized system modifications. |
| Lab 12 – Develop, Maintain and Test Information Security Policy (John Sands)Develop, maintain and test a policy that addresses information security for all personnelTo comply with the PCI DSS, organizations must establish, publish, maintain and disseminate a security policy, which must be reviewed at least annually and updated according to the changing risk environment. A risk assessment process must be implemented to identify threats and vulnerabilities, usage policies for critical technologies must be developed, security responsibilities for all personnel must be clearly defined and a formal awareness program must be implemented. Organizations must also implement an incident response plan so that they can respond immediately to any system breach.  |