

	Courses for INTERNAL Assessors, Implementors or Support Staff (Appropriate for those who will be conducting or supporting PCI assessments activities INSIDE their own company)			Courses for EXTERNAL Assessors, Consultants or Technicians/Installers (Appropriate for those who will be performing services OUTSIDE their own company for merchants or others)					
Course	Awareness	PCIP	ISA	Acquirer	QIR	ASV	QSA	PA-QSA	P2PE
Description	Entry-level course outlines payment card security issues and how PCI Standards can help protect cardholder data	Earn an individual credential for knowledge and understanding of PCI Standards	Receive instruction on how to perform internal assessments for PCI compliance	Understand the PCI DSS requirements to work with merchant clients and facilitate their journey toward PCI DSS compliance	Learn to install, configure, and maintain payment applications in a manner that facilitates PCI DSS compliance	Use security services and tools to validate adherence to the external scanning requirement of the PCI DSS	Learn to perform PCI DSS assessments of merchants and service providers	Provides tools to perform PA-DSS assessments and associated testing	Get a solid foundation to assess point-to-point encryption compliance with all six domains included in the P2PE standard
Key Benefits	<ul style="list-style-type: none"> Gain foundation of PCI knowledge Understand PCI DSS compliance before going through an assessment with a QSA Drive PCI DSS compliance across your business Satisfies PCI DSS requirement 12.6 for general security awareness 	<ul style="list-style-type: none"> Achieve industry recognized qualification that remains with you, throughout your career Supports your organization's or client's ongoing compliance efforts Enhances credibility with service partners Listing on PCI SSC website 	<ul style="list-style-type: none"> Enhance quality, reliability, and consistency of internal PCI DSS self-assessments Effectively facilitate interactions with QSAs Reduce compliance costs with development of ongoing security processes <i>* Cannot perform assessments external to Sponsor Company</i> 	<ul style="list-style-type: none"> Learn where acquirers fit into compliance in the payment process Apply PCI DSS security principles to your clients' specific situations Understand assessment process including Self-Assessment Questionnaire (SAQ), Report on Compliance (ROC) and Attestation of Compliance (AOC) 	<ul style="list-style-type: none"> Achieve industry-recognized qualification Ensure PA-DSS validated application is installed in compliance with the application vendor's <i>PA-DSS Implementation Guide</i> Produce the QIR Implementation Statement Listing on PCI SSC website 	<ul style="list-style-type: none"> Qualified to conduct vulnerability scans of internet-facing environments and validate adherence to PCI DSS requirement 11 Listing on PCI SSC website 	<ul style="list-style-type: none"> Qualified to conduct assessments and validate adherence to PCI DSS requirements Listing on PCI SSC website 	<ul style="list-style-type: none"> Qualified to conduct PAQSA assessments and validate a vendor's payment applications as adhering to the PADSS requirements Authorized to generate the final Report on Validation (RoV) Listing on PCI SSC website 	<ul style="list-style-type: none"> Qualified to test and assess P2PE solutions & components Authorized to generate the final P2PE Report on Validation (P-RoV) Listing on PCI SSC website PA-QSA (P2PE), all of the above, plus qualified to assess P2PE applications
Who Should Attend	Geared to a broad audience including executives, managers, and staff who are interested in learning more about PCI	IT and IT Security professionals; Entry level and mid-career professionals dedicated to excellence in payment security	Internal security assessment, risk management and audit staff	Acquirers and Processors	Integrators and Re-sellers, Software Developers and Engineers, Installers and Technicians	Security professionals at ASV companies	Security and audit professionals at QSA companies	Security and audit professionals at QSA companies	Security and audit professionals at QSA/PA-QSA companies
Necessary Experience	None	2 years experience in an IT or IT related role and knowledge of information technology, network security and architecture, and the payment industry	Security audit and assessment experience including but not limited to network security, application security and consultancy, system integration, and auditing	None	Experience in payment applications, system hardening, or network security, sufficient to conduct technically complex application installations	3 years of IT experience including 1 year vulnerability scanning or penetration testing OR CISSP, CISA, CISM certificate and 2 years of IT experience	See note 1 on page 2	Current QSA, must have completed 2 PCI DSS assessments	QSA(P2PE) – Current QSA and 2 PCI DSS assessments PA-QSA(P2PE) – Current PAQSA and 2 PCI DSS and 2 PADSS assessments
Course Format	<ul style="list-style-type: none"> 5 hour self-paced eLearning course or Hosted instructor-led at corporate site for employee group 	<ul style="list-style-type: none"> 1 day instructor-led class followed by exam or 8 hour eLearning course followed by exam Or Hosted instructor-led at corporate site for employee group followed by exam 	<ul style="list-style-type: none"> 5 hour self-paced online pre-requisite course followed by exam plus 2 day instructor-led class with exam or 8 hour self-paced eLearning course with exam or Hosted instructor-led at corporate site for employee group followed by exam 	<ul style="list-style-type: none"> 6 hour self-paced eLearning course or Hosted instructor-led at corporate site for employee group 	<ul style="list-style-type: none"> Self-paced online pre-requisite course and exam plus 5 hour self-paced eLearning course followed by final exam 	<ul style="list-style-type: none"> 6 hour self-paced eLearning course followed by exam 	<ul style="list-style-type: none"> 5 hour self-paced online pre-requisite course followed by exam plus 2 day instructor-led class with exam 	<ul style="list-style-type: none"> 6 hour self-paced eLearning followed by exam 	<ul style="list-style-type: none"> 2 hour online pre-requisite course with exam plus 2 day instructor-led class with exam

		Courses for INTERNAL Assessors, Implementors or Support Staff (Appropriate for those who will be conducting or supporting PCI assessments activities INSIDE their own company)			Courses for EXTERNAL Assessors, Consultants or Technicians/Installers (Appropriate for those who will be performing services OUTSIDE their own company for merchants or others)					
Course		Awareness	PCIP	ISA	Acquirer	QIR	ASV	QSA	PA-QSA	P2PE
Snapshot of Course Content		Overview of PCI requirements Roles and responsibilities of the key players Brand specific reporting and validation requirements	Principles of PCI DSS, PA-DSS, PCI PTS, and PCI P2PE Compensating controls SAQs usage Effects of new technology on PCI	PCI Data Security Standard (DSS) assessment and test procedures PCI Reporting Network segmentation Hardware and Communications Infrastructure	Introduction to PCI DSS and review of requirements Compliance roles and responsibilities Assessment process (SAQs, ROCs, and AOCs) Quality control, using the acquirer checklist	Understanding the PCI Landscape Overview of PCI DSS, PA-DSS applications, requirements, and the PA-DSS Implementation Guide Preparing for and performing a Qualified Installation	Compliance validation, requirements and process ASV overview and quality assurance Requirements for scanning and reporting Scanning vendor testing and approval process	PCI Data Security Standard (DSS) assessment and test procedures PCI Reporting Network segmentation Hardware and communications infrastructure	Payment Application – Data Security Standard (PA-DSS) requirements PA-DSS laboratory testing PA-DSS reporting	P2PE requirements, sub-requirements and associated test procedures Basic cryptography, key management techniques, and solution specific assessment techniques P2PE Reporting
Qualification		NONE	YES Individual qualification (not tied to employer) Re-qualification required every 3 years	YES Re-qualification required annually via online course and exam	NONE	YES Re-qualification required every year	YES Re-qualification required annually via online course/exam	YES Re-qualification required annually via online course/exam	YES Re-qualification required annually via online course/exam	YES Re-qualification required annually via online course/exam
Continuing Professional Education (CPE) hours		5–6	6–7	16	6	9	5	16	6	12–13
Cost	PO rate	\$500	\$1,550	\$1,800	\$995	\$100	NA	NA	NA	NA
	Non PO rate	\$500	\$2,500	\$3,100	\$1,495	\$100	\$1,200	\$2,750-\$3,550	\$1,375	\$3,000

1 Necessary Experience for QSA Candidates

Candidate possesses at least one of the following industry-recognized professional certifications:

- Certified Information System Security Professional (CISSP)
- Certified Information Security Manager (CISM)
- Certified Information Systems Auditor (CISA)
- GIAC Systems and Network Auditor (GSNA)
- Certified ISO 27001, Lead Auditor, Internal Auditor
- International Register of Certificated Auditors (IRCA)
- Information Security Management System (ISMS) Auditor
- Certified Internal Auditor (CIA)

Candidate possesses a minimum of one year of experience in each of the following information security disciplines:

- Application security
- Information systems security
- Network security
- IT security auditing
- Information security risk assessment or risk management

**Maximize Knowledge.
Minimize Risk.**

For more information on any of these PCI training courses, please visit our website: www.pcissc.org/training, call us at: +1-781-876-6295, or email us at: training@pcisecuritystandards.org.