

## **PCI-ISA (Payment Card Industry Internal Security Assessor).**

### **Introduction**

#### **PCI-ISA (Payment Card Industry Internal Security Assessor):**

- **Internal Role:** ISAs are employees of a PCI-compliant organization who have been trained and certified by the organization to conduct PCI DSS assessments internally.
- **Scope of Work:** ISAs are limited to conducting PCI DSS assessments solely for the organization that employs them. They assess the organization's compliance with PCI DSS requirements internally.
- **Responsibilities:** ISAs evaluate the organization's adherence to PCI DSS requirements, identify areas of non-compliance, and work with internal teams to implement remediation measures.

INTERNAL SECURITY ASSESSOR (ISA)<sup>™</sup> TRAINING day wise training curriculum

#### **Day 1: Introduction to PCI and Compliance Basics**

##### **Session:**

- Introduction to PCI DSS (Payment Card Industry Data Security Standard)
- Overview of the payment card industry: stakeholders, transaction flow, and relationships between organizations
- Importance of PCI compliance for companies handling cardholder data
- Key terminology and definitions in PCI compliance
- Overview of PCI DSS requirements and goals

#### **Day 2: Understanding PCI Requirements and Compliance Management**

##### **Session:**

- Deep dive into specific PCI DSS requirements (e.g., network security, encryption, access control)
- Understanding the testing procedures for each requirement
- Overview of PCI hardware and communications infrastructure requirements
- Best practices for securing payment card data in transit and at rest
- Overview of compliance issues and common challenges faced by organizations

#### **Day 3: Implementation Strategies and Policy Development**

##### **Session:**

- Strategies for implementing PCI requirements effectively
- Introduction to compensating controls and their role in achieving compliance
- Practical exercises and case studies to reinforce learning
- Workshop on creating and implementing policies and procedures to maintain compliance
- Strategies for modifying the cardholder data environment while maintaining compliance

#### **Day 4: Compliance Reporting and Ongoing Management**

##### **Session:**

- Overview of PCI reporting requirements and documentation
- Introduction to compliance management tools and resources
- Overview of ongoing compliance monitoring and assessment strategies
- Group discussions on compliance management challenges and solutions
- Q&A session and wrap-up

#### **Certification exam details**

##### **New Exam Specifics:**

- All exams are closed book.
- Exam is 60 multiple choice questions with a 90-minute time limit.
- Results of in person exams are delivered within 10 business days.
- Results of Pearson Vue exams are delivered upon completion of the exam.
- 75% or higher to pass the exam; the only information that can be released concerning exams is your grade.
- If you fail the exam, you are allowed one retake (within 30 days of failure notice) for a fee.

##### **Requalification exam:**

- Non-proctored remote exam
- 60 multiple choice questions with a 75-minute time limit.
- 75% or higher to pass the exam; the only information that can be released concerning exams is the grade.

- If you fail the exam, please have the primary contact email [administration@pcisecuritystandards.org](mailto:administration@pcisecuritystandards.org) for the next steps.