Certified Information Systems Security Tester (CISST)

Introduction

Certified Information Systems Security Tester (CISST) is designed exclusively for information security professionals who want to enhance their skill set in the testing of different security phases. CISST training course enables the candidate to modify, inspect, record, and secure the data that might be in any form e.g electronic or physical. Moreover, the certification tests the capabilities of individuals to identify different security vulnerabilities in their technology infrastructure. Hence, inhibiting different elements of work ethics including confidentiality, integrity, authentication, availability, and authorization.

Course Highlights

This course teaches you about core aspects such as:

- Security Risks
- Asset Identification
- Assessing Risk Analysis Effectiveness
- Information Security Policies and Procedures
- Analysis of Information Security Policies and Procedures
- Lifecycle Alignment and Security Testing Tasks
- Security Test Designing & Planning
- Implementing Policy-Based Security Tests
- Security Test Reporting
- Reporting Security Test Status
- Reporting Security Test Results
- Types and Purposes of Security Test Tools
- Tool Selection
- Open-Source Tools
- Benefits of Standards

Course Outline

Module Information - 1	● Module 1 - Security Risks ● Module 2 - Asset Identification ● Module 3 - Assessing Risk Analysis Effectiveness ● Module 4 - Information Security Policies and Procedures ● Module 5 - Analysis of Information Security Policies and Procedures ● Module 6 - Security Auditing and Its Role in Security Testing ● Module 7 - Security Risk Assessment ● Module 8 - Security Triad ● Module 9 - Introduction to Security Testing ● Module 10 - The Purpose of Security Testing ● Module 11 - The Organizational Context ● Module 12 - Security Testing Objectives ● Module 13 - The Difference between Information Assurance and Security Testing ● Module 14 - The Scope and Coverage of Security Testing Objectives ● Module 15 - Analysis of Security Approaches ● Module 16 - Analysis of Failures in Security Test Approaches

	● Module 17 - Stakeholder Identification
Module Information - 2	● Module 18 - Improving the Security Testing Practices ● Module 19 - Security Test Process Definition ● Module 20 - Lifecycle Alignment and Security Testing Tasks ● Module 21 - Security Test Planning ● Module 22 - Security Test Design ● Module 23 - Implementing Policy-Based Security Tests ● Module 24 - Security Test Execution ● Module 25 - Security Test Evaluation ● Module 26 - Security Test Maintenance ● Module 27 - Role of Security Testing in a Lifecycle ● Module 28 - The Role of Security Testing in Design ● Module 29 - The Role of Security Testing in Implementation Activities ● Module 30 - Component Test Analysis & Design ● Module 31 - Analyzing Component Test Results ● Module 32 - Component Integration Test Analysis & Design ● Module 33 - The Role of Security Testing in System and Acceptance Test Activities ● Module 34 - Definition of Security-Oriented Acceptance Criteria
Module Information - 3	● Module 35 - The Role of Security Testing in Maintenance ● Module 36 - Testing the Effectiveness of System Hardening ● Module 37 - Authentication and Authorization ● Module 38 - Firewalls and Network Zones ● Module 39 - Encryption, Intrusion Detection, Malware Scanning, and Data Obfuscation ● Module 40 - Training ● Module 41 - Security Awareness ● Module 42 - Attack Motivations ● Module 43 - Social Engineering and Security Awareness ● Module 44 - Revising Security Expectations ● Module 45 - Security Test Reporting ● Module 46 - Reporting Security Test Status ● Module 47 - Reporting Security Test Results ● Module 48 - Types and Purposes of Security Test Tools ● Module 49 - Tool Selection ● Module 50 - Open Source Tools ● Module 51 - Benefits of Standards ● Module 52 - Applying Security Standards

Prerequisites

The Certified Information Systems Security Tester (CISST)® Certification has no pre-requisites.

Target Audience

- This certification is the most advanced information systems testing training in the Information Security industry for IT managers, security consultants, security analysts, IT professionals, network engineers, and anyone having prior ethical hacking knowledge.

- People in managerial positions related to PCI DSS compliance, Project managers, Fraud management and prevention staff, Information security managers and officers, payment application vendors.

Duration

30 to 35 Hours