CSP108 – SUPPLY CHAIN AND SOFTWARE ACQUISITION

Course Learning Objectives

Understand the complexity and issues surrounding supply chain security. Describe the industry standards that are used to in securing the supply chain. Take the steps necessary for assessing a supplier's security practices. Describe a process for ensuring the software from a supplier is securely delivered and deployed. Gain the confidence to certify supplier delivered software.

Description

The goal of this Supply chain and software acquisition domain is to provide the learner knowledge to ensure that the software developed in a supply chain is secure. The learner will learn some of the industry standards and practices that must applied to provide a high level of assurance that the supply chain is secure – both upstream and downstream. In addition to the practices discussed in previous modules the learner will understand how to assess supplier practices, installation and deployment, monitoring considerations for suppliers, identify risks, and understand the use of contractual obligations for suppliers.

Audience

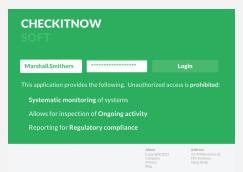


Time Required









CSP108 – SUPPLY CHAIN AND SOFTWARE ACQUISITION

Course Outline

- 1. Supplier risk assessment
- Components to software
- Supply chain
- Software assurance
- Three aspects to software assuran<u>ce</u>
- Providing assurance
- Acquisition lifecycle phases
- About outsourcing
- Risks to outsourcing
- Code reuse

2. Intellectual property and legal compliance

- About IP
- Patents
- Copyright
- Trade secrets
- Trademarks
- Contracts
- Non-disclosure agreements
- Service level agreements
- Completing the deal

3. Supplier sourcing

- Supplier selection
- Auditing deliverables
- Contractual integrity controls
- Vendor technical controls
- Managed security services
- Service level agreements
- Terms of service
- Service levels are based on requirements

4. Software development and test

- About
- Supplier risks
- Technical controls
- Code testing and verification
- Software testing and verification
- Trojans
- Maintenance hook
- Logic bombs

5. Software delivery, operations and maintenance

- Software maintenance
- Risk in software delivery
- Chain of custody
- Publishing controls
- Software authenticity and integrity controls
- Systems-of-systems
- Sustainment process
- Operations and maintenance
- Monitoring
- Validate systems
- Service levels
- Compliance
- Metrics for suppliers
- · Vulnerability management

6. Supplier transitioning

- About code escrow services
- How code escrow works
- Code escrow benefits
- Final considerations
- About code escrow services
- How code escrow works
- Code escrow benefits
- Final considerations