# CSP106 - SECURE SOFTWARE ACCEPT/DEPLOY

## Course Learning Objectives

In the four modules of this course, we'll explore how to establish a secure software acceptance process, including methods to integrate software acceptance concepts throughout the development lifecycle and promote a strong security culture by safely generating test data, classifying bugs, finding undocumented functionality, using a bug bar to make release decisions, assessing risk in the production environment, automating security checks with a CI/CD pipeline, getting approval to operate, monitoring deployed applications, responding to security incidents, planning patch releases, and safely decommissioning old software.

## Description

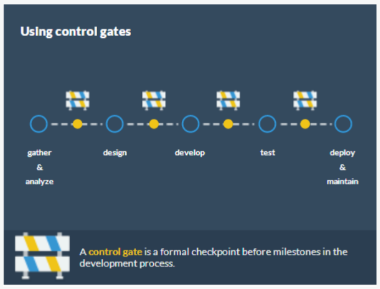
Secure Software Acceptance and Deployment is for software development professionals and security professionals who are responsible for securing different phases of the SDLC, including software engineers, architects, DevOps engineers, DevSecOps engineers, development managers, project managers, product managers, and QA analysts.

## Audience

Managers
DevOps
Engineers

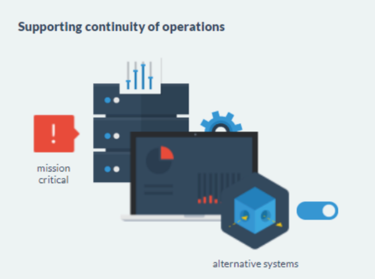
## Time Required

Tailored learning - 60 minutes total (approx.)

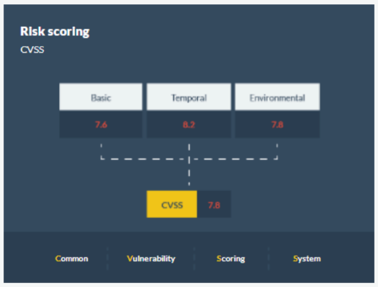


Using control gates

A control gate is a formal checkpoint before milestones in the development process.



Supporting continuity of operations



Risk scoring

CVSS

# CSP106 - SECURE SOFTWARE ACCEPT/DEPLOY

## Course Outline

### 1. Planning for Software Acceptance

- What is software acceptance?
- The secure SDLC
- The need for software acceptance
- The acceptance process
- Residual risk
- Using control gates
- Control gate example
- Control gate best practices
- Integrating with development practices
- Promote security culture in your organization
- Use metrics to make a quantifiable measure of code security
- Encourage continuous improvement
- Adopt a DevSecOps perspective
- Designate a security champion

### 2. Verification and Validation

- What is verification and validation?
- The test environment
- Testing with realistic data
- Production data
- Anonymized data
- Fake data
- Synthesized data
- Undocumented functionality
- Identifying bugs
- Bug classification
- Risk scoring
- DREAD
- CVSS
- Bug remediation
- Using a bug bar

### 3. Secure Deployment

- Secure deployment
- Assessing the environment
- Evaluate all parts of your environment
- Don’t reinvent the wheel
- Focus on threats
- Validate the recoverability of your system
- Training personnel
- Supplying secrets
- Securing secrets
- Continuous integration and deployment
- Benefits of CI/CD
- Automated tests
- Artifact verification
- Infrastructure as code
- Appropriate access control
- Approval to Operate

### 4. Monitoring and Maintenance

- Information Security Continuous Monitoring
- How to choose data
- Logging
- Identify the most important data sources
- Identify the most important event types
- Use analysis to aggregate data
- Use a log analysis tool
- Monitor log data continuously
- Incident response planning
- Goal of incident response plan
- Triaging
- Triaging security incidents
- Continuity of operations
- Supporting continuity of operations
- Patch management
- Prioritize patches by risk
- Version patches appropriately
- Perform regression testing
- Plan for the release of your patch
- Have a backout plan
- Decommissioning software

SecurityCompass