

## SC MGR 101: APPLICATION SECURITY FOR MANAGERS

Taking this class will allow students to understand application security from a manager's perspective. They will gain a strong understanding of technical attacks, activities that constitute a secure Software Development Life Cycle, and ROI for these activities with analysis from case studies.

Developers and security analysts are increasingly becoming involved in application security initiatives. Managers need to understand both the technical nature of their teams' involvement with security initiatives as well as the business case for performing activities. This class arms managers with the knowledge necessary to make effective, risk-based decisions about application projects that balance business needs with security requirements. Security Compass brings extensive enterprise security assessment and prioritization experience to its highly successful training platform in this class.

### DURATION & INTENDED AUDIENCE

- Duration: 1 day
- Intended Audience:
  - Information security managers
  - Software development managers
  - Project managers who work on applications

### PRE-REQUISITE KNOWLEDGE

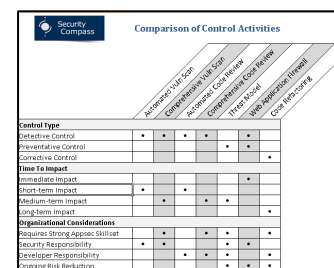
- Basic technical background, such as prior programming or network infrastructure experience
- Prior information security experience useful but not mandatory

### LEARNING OBJECTIVES

- Understand attacks that hackers use to break into applications
- Understand common activities used by organizations to secure their applications
- Articulate the Return on Investment and make perform tradeoff analysis on various application security review findings by risk)

### LEARNING ENVIRONMENT & TAKEAWAYS

- 4 GB bootable Backtrack Linux flash drive that students keep
- Video demonstrations of attacks
- Course book containing printouts of each slide along with detailed notes in paragraph form
- Hard-copy and soft copy of a source code review checklist to assist in performing source code reviews in the real world
- Hard-copy and soft copy of application security activity tradeoffs



	Technical Use Case	Comprehensive Use Case	Performance Cost Review	Integration Cost Review	Third Party	Web Application Control	Low Resource
<b>Control Type</b>							
Defensive Control	•	•	•	•	•	•	•
Preventative Control	•	•	•	•	•	•	•
Corrective Control	•	•	•	•	•	•	•
<b>Time To Impact</b>							
Immediate Impact	•	•	•	•	•	•	•
Short-term Impact	•	•	•	•	•	•	•
Medium-term Impact	•	•	•	•	•	•	•
Long-term Impact	•	•	•	•	•	•	•
<b>Organizational Considerations</b>							
Requires Strong Assess Skillset	•	•	•	•	•	•	•
Security Responsibility	•	•	•	•	•	•	•
Developer Responsibility	•	•	•	•	•	•	•
Ongoing Risk Reduction	•	•	•	•	•	•	•

### CONTACT INFO

- Phone: 1-888-777-2211 x 1
- Email: [training@securitycompass.com](mailto:training@securitycompass.com)

## DETAILED OUTLINE

### Introduction

- Application Security vs. Traditional Security

### Authentication

- Factors of Authentication
- User Enumeration
- Password Reset
- Brute Force
- Password Sniffing

### Session Management

- Session Hijacking
- Content Caching

### Input Validation

- Input Validation Overview
- Parameter Manipulation
- XSS
- CSRF
- SQL Injection
- XML Attacks

### Secure SDLC

- Security requirements
- Application security standards and guidelines
- Secure design & architecture
- Threat modeling
- Secure development
- Source code review, manual vs. static analysis
- Secure testing
- Secure quality assurance
- Secure deployment
- Web application firewalls
- Enterprise activities
- Training and awareness
- Remediation tracking

### Business Case

- Costs of application security activities
- Prioritizing multiple applications