

Framework Solution for Life Cycle Security

This two day workshop outlines a comprehensive approach to building and maintaining secure information systems. It assists IT organizations in understanding and preparing for regulatory compliance with HIPAA, Sarbanes-Oxley and other regulatory mandates.

This workshop teaches organizations how to increase security in their applications without costly security skills training and without adversely affecting project timelines or budgets.

The Information Assurance workgroup revising IEEE P1074 *Standard for Developing Software Life Cycle Processes* has concluded:

Efforts that do not treat security as an integral part of systems engineering and architecture fail to provide security.

It no longer makes any business sense to spend any money, apply any resources and proceed with any Software Development project unless corporate assets and private customer data will be sufficiently secure.

These findings fundamentally alter when and how security concerns should be addressed during development, at deployment, and during maintenance over the lifetime of a software application.

This seminar presents a practical framework that integrates security practices embodied in ISO 17799 *Code of Practice for*

Framework Solution for Life Cycle Security

Information Security Management and ISO 15408 *Common Criteria for Information Technology Security Evaluation* into the the typical Project Life Cycle. It covers IT security and regulatory awareness, secure management techniques, security risk analysis, product certification, secure coding and testing methods, and secure systems maintenance and operations.

Seminar Summary

- frames the IT security problem
- introduces a practical process framework that integrates seamlessly into any enterprise security model
- explores organizational gaps that make developing secure software challenging
- teaches effective risk analysis and threat modeling
- demonstrates how and when to address security on projects
- provides strategies for judging how much security should be built into a product
- offers an approach for immediately improving the security of software that does not involve developer security training
- provides flexible templates and an overview of powerful free or low cost tools

Intended Audience

Directly benefits IT Project Managers, Technical Architects and Leads, QA Leads and Security Professionals. Also appropriate for technology managers, developers & testers who seek to better understand their security responsibilities and to CIOs, CISOs and Executives as an introductory overview of the full curriculum.

QualityIT presents

SESSION 1: Framing the Secure Software Problem

- ✓ Security incident impacts
- ✓ The detection/response fallacy
- ✓ Defense in depth concept
- ✓ Commercial product trends
- ✓ Legal, privacy, and financial implications
- ✓ Security trends
- ✓ Overview of available standards guidance
- ✓ LAB: Security Context, Awareness & Perception

SESSION 2: Finding the Security Goal

- ✓ Understanding customer security concerns
- ✓ What information assurance means
- ✓ Exploring the secure development life cycle
- ✓ The acceptability problem
- ✓ Identifying product security objectives
- ✓ Security objectives inputs and influence
- ✓ Confidentiality, Integrity, and Availability
- ✓ Monitoring threat and liability trends
- ✓ Formulating threat responses
- ✓ Relationship to Business Continuity
- ✓ LAB: Case Study: Determining Security Objectives

SESSION 3: Available Guidance and Powerful Tools

- ✓ ISO 17799 Security Management
- ✓ ISO/IEC 15408 Common Criteria Evaluation
- ✓ Common Criteria terminology and concepts
- ✓ Protection profiles and benefits
- ✓ Seven evaluation levels
- ✓ LAB: Applying Common Criteria assets and principles

Framework Solution for Life Cycle Security

SESSION 4: Threat Modeling: Key to Security Coding

- ✓ Where threat modeling fits in the SDLC
- ✓ Overview of modeling method
- ✓ CC threat roles and categories
- ✓ OSI, Zones, STRIDE and STRIDER
- ✓ LAB: Effective Threat Modeling

SESSION 5: Writing Secure Code

- ✓ Demystifying secure coding
- ✓ Security strategies based on current trends
- ✓ Exploring the universe of secure checklists
- ✓ 40 of the top Java, C, C++ coding issues
- ✓ Microsoft's Trustworthy Computing Initiative
- ✓ 15 of the best C/C++ coding guidelines
- ✓ Revelations
- ✓ LAB: Setting Code Inspection Goals

SESSION 6: Security Testing

- ✓ Measuring against security target
- ✓ Seeking accreditation
- ✓ Demystifying penetration testing
- ✓ Contrasting security and penetration testing
- ✓ Tips and tools for black-box testers
- ✓ Assuring secure product upgrade and integrity
- ✓ LAB: Communicating Security Risk

SESSION 7: Back to Work

- ✓ Adjusting awareness quotients
- ✓ Threat monitoring strategies
- ✓ Preferred websites and books
- ✓ Review of key points and principles
- ✓ LAB: Back to work plans

Framework Solution for Life Cycle Security

Benefits of Attending

- Gaining a comprehensive understanding of how and why traditional software development must change to meet contemporary security challenges
- Understanding why it is difficult—but not impossible—to build secure software that satisfies customer expectations
- Understanding the legal implications of security in software
- Understanding how product security affects project management
- Understanding how to communicate security risk effectively
- Understanding how to define product security requirements and how to measure against them
- Understanding how secure coding and security testing are different from functional coding and testing
- Learning what guidance documents are available and how to apply them effectively to limit security liability.

For public or onsite workshops contact

Quality IT
15805 NE 83rd Ct. Redmond, WA 98052

425.241.5391

barbis@qualityit.net

or

Construx Software

<http://www.construx.com/training/onsite/>

For other services, see our website:

<http://www.qualityit.net>

QualityIT
presents

Framework Solution for Life Cycle Security

A two day workshop
for building and maintaining
secure information systems

Quality IT
15805 NE 83rd Ct.
Redmond, WA 98052
425-241-5391
<http://www.qualityit.net>

IT Quality & Security Assurance in action