Security Extensions for CMMI

Doug Ashbaugh, CISSP, CISA, CSSLP

May 22, 2013

SEI CMMI LEVEL 3 Company

Software Engineering SERVICES

Doug Ashbaugh, CISSP, CISA, CSSLP

- 35 Years Software Development Experience
- 27 Years Project Management Experience
- 15 years information systems security experience
- Certified Information Systems Security Professional
- Certified Information Systems Auditor
- Certified Secure Software Lifecycle Professional
- Published Author: "Security Software Development – Assessing and Managing Security Risks" CRC Press, 2009

SEI CMMI LEVEL 3 Company

Software Engineering SERVICES

Outline

- What are security extensions?
- Why are security extensions necessary?
- A look at specific security extensions:
  - ISO/IEC 21827 (SSE-CMM)
  - +SAFE
  - +SECURE
- SES Security Offerings
- Questions

SEI CMMI LEVEL 3 Company

Software Engineering 3 SERVICES

What are Security Extensions?

- Additional practices intended for process improvement in several contexts:
  - **Strategically:** to support enterprise security services
  - **Program Level:** supporting the security of products and services including development, maintenance, operations and support
  - **Work Environment:** promoting a secure work environment
  - **Acquisition:** evaluating the ability of suppliers to provide secure products and services

Why are Security Extensions Necessary?

- Numbers
- Headlines
- Regulatory Requirements
- Cost
- Customer Confidence
- Changing hardware and software architectures

ISO/IEC 21827 (SSE-CMM)

- A basic set of security engineering practices which can be used as a:
  - Tool for provider organizations
  - Standard mechanism for customers to select providers
  - Basis for evaluation of organizations
  - Mechanism to measure and monitor the capability to deliver

HISTORY of ISO/IEC 21827

- 1993: NSA Initiated funding
- 1995: Working groups established
- 1996: SSE-CMM v1.0 Published
- 1996-98: Piloted in 7 organizations
- 1999: v2.0 Published
- 2002: Approved as ISO/IEC 21827
- 2004-05: Appraiser Certification Body under ISO/IEC 17024

SEI CMMI LEVEL 3 Company

Software Engineering SERVICES

CMMI – SSE-CMM

CMMI	SSE-CMM
Org Process Focus (L3) Org Process Definition (L3) Org Process Performance (L4) Org Innovation and Deployment (L5)	Define Org Sys Sec Eng (SSE) Process Improve Org SSE Process Manage Sys Eng Support Environment Manage Product Line Evolution
Organizational Training (L3)	Provide Ongoing Skills and Knowledge
Project Planning (L2) Project Monitoring & Control (L2) Supplier Agreement Mgt (L2) Integrated Project Mgt (L3) Risk Management (L3) Quantitative Project Mgt (L4)	Plan Technical Effort Monitor and Control Technical Effort Coordinate with Suppliers Coordinate Security Manage Project Risk Build Assurance Argument

SEI CMMI LEVEL 3 Company

Software Engineering SERVICES

CMMI – SSE-CMM

CMMI	SSE-CMM
Requirements Management (L2) Requirements Development (L3) Technical Solution (L3) Product Integration (L3) Verification (L3) Validation (L3)	Specify Security Needs Provide Security Input Verify and Validate Security Administer Security Controls Assess Impact Assess Security Risk Assess Threat Assess Vulnerability Monitor Security Posture
Configuration Management (L2)	Manage Configurations
Process & Product QA (L2)	Ensure Quality

SEI CMMI LEVEL 3 Company

Software Engineering SERVICES

+SAFE Background

- CMMI and iCMM interest in safety/security
- DoD and FAA decided to collaborate on developing safety/security extensions to both iCMM and CMMI
- Both CMMI and iCMM provide a framework in which safety and security activities can take place
- Safety and Security only mentioned in *informative* components not *required* or *expected* components

+SAFE

- Source Documents
  - Major, Essential, Widely Recognized
  - Used to Synthesize “Best Practice”
  - Bi-directonal Traceability
  - 3 for Safety
  - 4 for Security
    - ISO 17799 (Now ISO 27002)
    - ISO 15408
    - SSE-CMM
    - NIST 800-30

SEI CMMI LEVEL 3 Company

Software Engineering SERVICES

+SAFE

- Introduced Application Packages (AP)
- Looks like a Process Area
- Application Practices
- But… uses existing process areas and practices
- Visibility and Useability
- Appraisal

SEI CMMI LEVEL 3 Company

Software Engineering SERVICES

+SAFE Goals and APs

- Goal 1: An infrastructure for safety and security is established and maintained
  - AP 01.01 Ensure safety and Security Competency
  - AP 01.02 Established Qualified Work Environment
  - AP 01.03 Ensure Integrity of Safety and Security Information
  - AP 01.04 Monitor Operations and Report Incidents
  - AP 01.05 Ensure Business Continuity

+SAFE Goals and APs

- Goal 2: Safety and Security Risks are identified and managed
  - AP 01.06 Identify Safety and Security Risks
  - AP 01.07 Analyze and Prioritize Risks
  - AP 01.08 Determine, Implement and Monitor Risk Mitigation Plan

+SAFE Goals and APs

- Goal 3: Safety and Security Requirements are Satisfied
  - AP 01.09 Determine Regulatory Requirements, Laws and Standards
  - AP 01.10 Develop and Deploy Safe and Secure Products and Services
  - AP 01.11 Objectively Evaluate Products
  - AP 01.12 Establish Safety and Security Assurance Arguments

+SAFE Goals and APs

- Goal 4: Activities and products are managed to achieve safety and security requirements and objectives
  - AP 01.13 Establish Independent Safety and Security Reporting
  - AP 01.14 Establish a Safety and Security Plan
  - AP 01.15 Select and Manage Suppliers, Products, and Services
  - AP 01.16 Monitor and Control Activities and Processes

+SECURE

- Proposed security extension to CMMI-DEV v1.3 to describe practices to be used for defining processes for developing secure products.
- Process Areas
  - Organizational Preparedness for Secure Development
  - Security Management in Projects
  - Security Requirements and Technical Solution
  - Security Verification and Validation

SEI CMMI LEVEL 3 Company

Software Engineering SERVICES

+SECURE

- Organizational Preparedness for Secure Development (OPS)
  - Establish and maintain capabilities to develop secure products and react to product security incidents.
- Security Management in Projects (SMP)
  - is to establish, identify, plan and manage security activities for the project and to manage product security risks

+SECURE

- Security Requirements and Technical Solution (SRT)
  - Identify security requirements and then to design, develop and implement solutions that meet the security requirements to ensure the development of a secure product.
- Security Verification and Validation (SVV)
  - Ensure that selected work products meet their specified security requirements and to demonstrate that the product or product component fulfills the security expectations when placed in its intended operational environment and exposed to potential security threats

SES Capabilities

- Security Risk Assessment and Audit Services
- Remediation Services
- Training and Awareness Programs
- Governance and Oversight Programs
- Application Security Services
- BC/DR COOP/COG Services
- Compliance Services

SEI CMMI LEVEL 3 Company

Software Engineering SERVICES

Questions?

For further information contact:

Doug Ashbaugh
Director of Information Assurance
Software Engineering Services
(515) 226-9295
dashbaugh@sessolutions.com

SEI CMMI LEVEL 3 Company

Software Engineering SERVICES