Mature and Secure: Creating a CMMI® and ISO/IEC 21827 Compliant Process Improvement Program

Michele Moss
San Diego, CA
October 27, 2005

© CMMI is registered in the U.S. Patent and Trademark Office by Carnegie Mellon University.
Security needs are continuously evolving, which makes security implementation increasingly challenging

- Global interconnection
- Massive complexity
- Release of beta versions of software
- Evolutionary development
Addressing security is increasingly complex

You are here.

They are somewhere.

Any questions?
Business drivers help shape the integration of security into our systems/software efforts

- **Headline News**
  - Microsoft: "Code Red" Worm
  - Air Force: “Hacker Steals Air Force Officer’s Personal Information”

- **Legislation**
  - e-Gov Act
  - OMB A-11 Exhibit 300 Section II. B
  - FISMA

- **Market recognition**
  - Assurance that security is appropriately addressed
  - Security implementation should be transparent
Integrating security engineering into the systems engineering lifecycle enables successful information assurance implementation.
The CMMI is an existing business requirement that provides guidance for defining, implementing and improving the systems lifecycle.
The ISO 21827 SSE-CMM* provides guidance for defining, implementing and improving the security lifecycle.

* Systems Security Engineering Capability Maturity Model
DITSCAP defines the certification and accreditation lifecycle
Organizational Standard Processes leverage industry standards that support diverse clients

**Systems/SW Process Improvement Program**
WTB Systems Teams are pursuing CMMI Level 3 for systems and software development

**ISO-9001**
Ensure the process improvement programs are also compliant with ISO 9001

**Systems Security Engineering Process Improvement Program**
Standardize security engineering activities in compliance with the ISO/IEC 21827 and Integrate our standard security engineering activities into our Systems/SW processes

**Industry Best Practices**
Project Management Institute, National Institute of Standards (NIST), Software Engineering Institute (SEI), Information Assurance Technical Framework (IATF) and International Organization for Standardization

**Foundation:** Software centric programs that have attained SW-CMM Level 3

CMMI = Capability Maturity Model Integration
ISO = International Organization for Standardization
The ISO 21827 is based on the Systems Engineering CMM (SE-CMM), adding security engineering practices to enable improvement of security specific practices.
Our CMMI approach integrated security engineering processes with our systems/software processes

Integrating security engineering into the systems engineering lifecycle will enable successful information assurance implementation
There are different CMM Representations

- **Staged**\(^1\) - process areas are assessed using specific practices. Predefines the process areas required to attain each maturity level (1-5) and thereby provides a roadmap for institutionalizing best practices.

- **Continuous**\(^1\) – process areas are assessed using specific practices within an area and the generic practices required for a specific level. Based on its business objectives, an organization selects the process areas in which it wants to improve and to what degree.

The SSE-CMM is a continuous model and a target profile is used to scope the appraisal and prioritize the process areas

- A target profile is based on
  - An analysis of the “Business and Mission Imperatives” and an assessment of which Process Areas are most important to support them
  - Industry “best practices” for the type of product, project or service, published Industry sector profiles, or a published profile from another organization in the same or related industry

- Organizations may develop their own unique target profiles
  - The SSE-CMM does not mandate specific profiles
The ISO 21827 addresses the organization’s selected process areas from two dimensions or aspects:

- **Domain Aspect** – What We Do
  - Process Areas
    - Base Practices

- **Capability Aspect** – How Well We Do It
  - Capability Level
    - Common Features
      - Generic Practices

- The **domain aspect** includes process areas that include base practices for the domain of security engineering.

- The **capability aspect** addresses institutionalization of the process areas.
Sample Profile for a Security Product Developer

- For a security product developer, the process areas related to product development activities might target a higher level of maturity.
Sample Profile for a Systems Integrator

- In this case, the highest level of maturity is required in those process areas that contribute most significantly to fulfilling the customers' expectations.
CMMI processes provided the foundation for implementation of security practices

<table>
<thead>
<tr>
<th>CMMI</th>
<th>ISO/IEC 21827 SSE-CMM</th>
</tr>
</thead>
<tbody>
<tr>
<td>Org Process Focus (L3)</td>
<td>Define Organization’s Systems Security Engineering Process</td>
</tr>
<tr>
<td>Org Process Definition (L3)</td>
<td>Improve Organization’s Systems Security Engineering Process</td>
</tr>
<tr>
<td>Org Process Performance (L4)</td>
<td>Manage Systems Engineering Support Environment</td>
</tr>
<tr>
<td>Org Innovation and Deployment (L5)</td>
<td>Manage Product Line Evolution</td>
</tr>
<tr>
<td>Organizational Training (L3)</td>
<td>Provide Ongoing Skills and Knowledge</td>
</tr>
<tr>
<td>Project Planning (L2)</td>
<td>Plan Technical Effort</td>
</tr>
<tr>
<td>Project Monitoring and Control (L2)</td>
<td>Monitor and Control Technical Effort</td>
</tr>
<tr>
<td>Supplier Agreement Management (L2)</td>
<td>Coordinate with Suppliers</td>
</tr>
<tr>
<td>Integrated Project Management (L3)</td>
<td>Coordinate Security</td>
</tr>
<tr>
<td>Risk Management (L3)</td>
<td>Manage Project Risk</td>
</tr>
<tr>
<td>Quantitative Project Management (L4)</td>
<td>Build Assurance Argument</td>
</tr>
<tr>
<td>Requirements Management (L2)</td>
<td>Specify Security Needs</td>
</tr>
<tr>
<td>Requirements Development (L3)</td>
<td>Provide Security Input</td>
</tr>
<tr>
<td>Technical Solution (L3)</td>
<td>Verify and Validate Security</td>
</tr>
<tr>
<td>Product Integration (L3)</td>
<td>Administer Security Controls</td>
</tr>
<tr>
<td>Verification (L3)</td>
<td>Assess Impact</td>
</tr>
<tr>
<td>Validation (L3)</td>
<td>Assess Security Risk</td>
</tr>
<tr>
<td></td>
<td>Assess Threat</td>
</tr>
<tr>
<td></td>
<td>Assess Vulnerability</td>
</tr>
<tr>
<td></td>
<td>Monitor Security Posture</td>
</tr>
<tr>
<td>Configuration Management (L2)</td>
<td>Manage Configurations</td>
</tr>
<tr>
<td>Process &amp; Product Quality Assurance (L2)</td>
<td>Ensure Quality</td>
</tr>
<tr>
<td>Measurement and Analysis (L2)</td>
<td></td>
</tr>
<tr>
<td>Decision Analysis and Resolution (L3)</td>
<td></td>
</tr>
<tr>
<td>Causal Analysis and Resolution (L5)</td>
<td></td>
</tr>
</tbody>
</table>
An integrated team to advocates process implementation

- Appraisers
  - Role: Provide CMMI model and OSP subject matter expertise
- Process Engineers
  - Role: Mentor and assist project personnel in implementing project processes
- Security Process Engineers
  - Role: Provide SME support and guidance for security process implementation
The SCAMPI and ISO/IEC 21827 Appraisal Method have similar steps

SSE-CMM Appraisal Method

Planning Phase
- Scope Appraisal
- Plan Appraisal

Preparation Phase
- Prepare Appraisal Team
- Administer Questionnaire
- Consolidate Evidence
- Analyze Evidence/Questionnaire

Onsite Phase
- Executive Brief/Opening Meeting
- Interview Leads/Practitioners
- Analyze Data
- Establish Findings
- Develop Rating Profile
- Manage Records
- Conduct Wrap Up

Reporting Phase
- Develop Findings Report
- Report Appraisal Outcomes to Sponsor
- Manage Appraisal Artifacts
- Report Lessons Learned

CMMI SCAMPI

Plan and Prepare for Appraisal
- Analyze Requirements
- Develop Appraisal Plan
- Select and Prepare Appraisal Team
- Obtain and Analyze Initial Objective Evidence
- Prepare for Collection of Objective Evidence

Conduct Appraisal
- Examine Objective Evidence
- Verify and Validate Objective Evidence
- Document Objective Evidence
- Generate Appraisal Results

Report Results
- Deliver Appraisal Results
- Package and Archive Appraisal Assets

SM SCAMPI is a service mark of Carnegie Mellon University
Integrating security into a Process Improvement Program results in increased assurance and transparency of security implementation.
For More Information

- ISO/IEC 21827
  - www.sse-cmm.org
  - www.issea.org

- CMMI
  - http://www.sei.cmu.edu/cmmi/Information

- Assurance
  - http://iase.disa.mil/
  - http://www.iatf.net/
  - http://www.sei.cmu.edu/programs/nss/nss.html
Back up slides
History of ISO/IEC 21827

- 1993  NSA initiated funding for development of a CMM for security engineering
- 1995  Working groups established to develop the SSE-CMM
- 1996  SSE-CMM v1.0 published
- 1996-98 SSE-CMM piloted in 7 organizations
- 1999  SSE-CMM v2.0 published

The International System Security Engineering Association (ISSEA) was established as a non-profit professional membership organization to be a liaison with ISO for standardization, model maintenance, and appraiser certification

- 2002  SSE-CMM approved as ISO/IEC 21827
- 2004-05 ISSEA submitting application for approval as ISO/IEC 21827 Appraiser Certification Body under ISO/IEC 17024, General Requirements For Bodies Operating Certification Schemes For Persons
The ISO 21827 facilitates achieving several of security engineering goals

- Tool for provider organizations to evaluate their security practices and focus improvements
- Basis for evaluation of organizations (e.g., certifiers, evaluators) to establish organizational capability-based confidence in results
- Mechanism to measure and monitor an organization’s capability to deliver a specific security engineering capability
- Standard mechanism for customers to select appropriately qualified security engineering providers

Process Improvement
Assurance
Risk Management
Capability Evaluation
There are 129 bases practices categorized into either Security Engineering Process Areas or Project and Organizational Process Areas

<table>
<thead>
<tr>
<th>Security Engineering Process Areas</th>
<th># of Base Practices</th>
<th>Project and Organizational Process Areas</th>
<th># of Base Practices</th>
</tr>
</thead>
<tbody>
<tr>
<td>1) Administer Security Controls</td>
<td>4</td>
<td>Ensure Quality</td>
<td>8</td>
</tr>
<tr>
<td>2) Assess Impact</td>
<td>6</td>
<td>Manage Configurations</td>
<td>5</td>
</tr>
<tr>
<td>3) Assess Security Risk</td>
<td>6</td>
<td>Manage Project Risk</td>
<td>6</td>
</tr>
<tr>
<td>4) Assess Threat</td>
<td>6</td>
<td>Monitor and Control Technical Effort</td>
<td>6</td>
</tr>
<tr>
<td>5) Assess Vulnerability</td>
<td>5</td>
<td>Plan Technical Effort</td>
<td>10</td>
</tr>
<tr>
<td>6) Build Assurance Argument</td>
<td>5</td>
<td>Define Organization’s Security Engineering Process</td>
<td>4</td>
</tr>
<tr>
<td>7) Coordinate Security</td>
<td>4</td>
<td>Improve Organization’s Security Engineering Process</td>
<td>4</td>
</tr>
<tr>
<td>8) Monitor Security Posture</td>
<td>7</td>
<td>Manage Product Line Evolution</td>
<td>5</td>
</tr>
<tr>
<td>9) Provide Security Input</td>
<td>6</td>
<td>Manage Systems Engineering Support Environment</td>
<td>7</td>
</tr>
<tr>
<td>10) Specify Security Needs</td>
<td>7</td>
<td>Provide Ongoing Skills and Knowledge</td>
<td>8</td>
</tr>
<tr>
<td>11) Verify and Validate Security</td>
<td>5</td>
<td>Coordinate with Suppliers</td>
<td>5</td>
</tr>
</tbody>
</table>
Systems Security Certification & Accreditation

- **Certification**
  - Provides a comprehensive **evaluation** of technical and non-technical security features of an information system
  - Establishes the **extent to which** a particular design and implementation meets a set of specified security requirements
  - Provides **proof** of compliance with security requirements
  - **Leads** to accreditation

- **Accreditation**
  - Formal **declaration** by the designated approving authority (DAA):
    - An information system is approved to operate in a particular security mode at an **acceptable level of risk**
    - Based on the implementation of an **approved set of** technical, managerial, and procedural **safeguards**
  - Approval is granted to operate the system with the identified residual risk
  - Upon accreditation, the DAA formally accepts full responsibility for the security of the system
Staged vs. Continuous Models

**Staged Model**

1. **Initial**
   - Process Area Base Practices Performed

2. **Repeatable**
   - Configuration Management
   - Process and Product Quality Assurance
   - Supplier Agreement Management
   - Project Monitoring and Control
   - Project Planning
   - Requirements Management
   - Measurement and Analysis

3. **Defined**
   - Requirements Development
   - Technical Solution
   - Product Integration
   - Verification
   - Validation
   - Organizational Process Focus
   - Organizational Process Definition

4. **Managed**
   - Organizational Process Performance
   - Quantitative Project Management

5. **Optimizing**
   - Organizational Innovation and Deployment
   - Causal Analysis and Resolution

**Continuous Model**

1. **Performed Informally**
   - Process Area Base Practices Performed

2. **Planned and Tracked**
   - Planning Performance
   - Disciplined Performance
   - Verifying Performance
   - Tracking Performance

3. **Well-Defined**
   - Defining a standard process
   - Perform the defined process
   - Coordinate practices

4. **Quantitatively Controlled**
   - Establishing Measurable Quality Goals
   - Objectively Managing Performance

5. **Continuously Improving**
   - Improving Organizational Capability
   - Improving Process Effectiveness

**Process Areas**

**Generic Practices**
## Staged and Continuous Model Comparison

<table>
<thead>
<tr>
<th></th>
<th>Staged</th>
<th>Continuous</th>
</tr>
</thead>
<tbody>
<tr>
<td>Less Flexible</td>
<td>More Flexible</td>
<td></td>
</tr>
<tr>
<td>Provides a definitive direction for improvement</td>
<td>Organizations can chart their own direction for improvement</td>
<td></td>
</tr>
<tr>
<td>Applies to only specific type of organization</td>
<td>Applies across all industries or types of organizations</td>
<td></td>
</tr>
<tr>
<td>All processes addressed at each level</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>