Achieving System and Software Assurance Through CMMI®-Compliant Processes

Paul R. Croll  
Chair, IEEE Software and Systems Engineering Standards Committee  
Convener, ISO/IEC JTC1/SC7 WG9, System and Software Integrity  
Computer Sciences Corporation  
pcroll@csc.com
Topics

- The Scope of System and Software Assurance
- Achieving System and Software Assurance Through CMMI®-Compliant Processes
- The CMMI® and Assurance
- Assurance in the Context of the Life Cycle
- Standards Supporting System and Software Assurance
- Implementing Assurance Processes
The Scope of System and Software Assurance

System and software assurance focuses on the management of risk and assurance of safety, security, and dependability within the context of system and software life cycles.

Terms of Reference: ISO/IEC JTC1/SC7 WG9, System and Software Integrity
Achieving System and Software Assurance Through CMMI®-Compliant Processes

1. Understand Your Business Requirements for Assurance

2. Look to the CMMI® for Assurance-Related Process Capability Expectations

3. Look to Standards for Assurance Process Detail

4. Build or Refine and Execute Your Assurance Processes
What are your business requirements for System and Software Assurance?

- Business process requirements
- Legal and regulatory requirements
- Marketplace requirements
- Customer-specific requirements
- Product-specific requirements
How does the CMMI® support System and Software Assurance?

2. Look to the CMMI® for Assurance-Related Process Capability Expectations
CMMI® Assurance Shortfalls

- Inconsistent treatment of safety and security concerns
- Insufficient assurance detail in required and expected components
  - Specific goals
  - Specific practices
- Insufficient traceability to assurance source standards
### CMMI® – Process Areas and Assurance

<table>
<thead>
<tr>
<th>Process Area</th>
<th>Explicit</th>
<th>Implicit</th>
<th>Supporting</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Process Management</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>OPF</td>
<td></td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>OPD</td>
<td></td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>OT</td>
<td></td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>OPP</td>
<td></td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>OID</td>
<td></td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td><strong>Project Management</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>PP</td>
<td>✓</td>
<td></td>
<td></td>
</tr>
<tr>
<td>PMC</td>
<td>✓</td>
<td></td>
<td></td>
</tr>
<tr>
<td>SAM</td>
<td>✓</td>
<td></td>
<td></td>
</tr>
<tr>
<td>IPM</td>
<td></td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>RSKM</td>
<td>✓</td>
<td></td>
<td></td>
</tr>
<tr>
<td>IT</td>
<td></td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>ISM</td>
<td></td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>QPM</td>
<td></td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td><strong>Engineering</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>REQM</td>
<td>✓</td>
<td></td>
<td></td>
</tr>
<tr>
<td>RD</td>
<td>✓</td>
<td></td>
<td></td>
</tr>
<tr>
<td>TS</td>
<td>✓</td>
<td></td>
<td></td>
</tr>
<tr>
<td>PI</td>
<td>✓</td>
<td></td>
<td></td>
</tr>
<tr>
<td>VER</td>
<td>✓</td>
<td></td>
<td></td>
</tr>
<tr>
<td>VAL</td>
<td>✓</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Support</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>CM</td>
<td>✓</td>
<td></td>
<td></td>
</tr>
<tr>
<td>PPQA</td>
<td>✓</td>
<td></td>
<td></td>
</tr>
<tr>
<td>MA</td>
<td>✓</td>
<td></td>
<td></td>
</tr>
<tr>
<td>DAR</td>
<td>✓</td>
<td></td>
<td></td>
</tr>
<tr>
<td>OEI</td>
<td>✓</td>
<td></td>
<td></td>
</tr>
<tr>
<td>CAR</td>
<td>✓</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
CMMI® – Project Management Process Areas and Assurance

- Project Planning (PP)
- Project Monitoring and Control (PMC)
- Supplier Agreement Management (SAM)
- Risk Management (RSKM)
CMMI® – Project Management Assurance Objectives - PP

**Project Planning**

- Determine the *technical approach* for the project, including the *functionality* expected in the final products, such as *safety and security*.
- Estimate *effort and cost* using models and/or historical data including *inputs related to level of security required* for tasks, work products, hardware, software, personnel, and work environment.
- *Plan for the management of project data* including *data supporting safety*.
- *Establish requirements and procedures* to ensure privacy and *security of the data*.

*Source: CMMI® -SE/SW/IPPD/SS, V1.1, Continuous Representation, © CMU SEI, 2002.*
Project Monitoring and Control

- *Monitor resources provided and used*, including the *security environment*
- *Collect and analyze issues* and *determine the corrective actions* necessary to address the issues, *including security issues*.

Supplier Agreement Management

- Evaluate the impact of candidate COTS products on the project's plans and commitments, including security requirements

Risk Management

- *Identify the risks* associated with cost, schedule, and performance in all appropriate product life-cycle phases, *including risks associated with maintaining safety and security performance.*

CMMI® – Engineering Process Areas and Assurance

- Requirements Development (RD)
- Technical Solution (TS)
- Product Integration (PI)
- Verification* (VER)
- Validation* (VAL)

*Implicit
Requirements Development

- Analyze needs and requirements for each product life-cycle phase, including factors that reflect overall customer and end-user expectations and satisfaction, such as safety, security, and affordability.

- Ensure that the design adheres to applicable design standards and criteria, including safety standards.

Technical Solution

- Design comprehensive product-component interfaces in terms of established and maintained criteria, including safety and security.

- Adhere to applicable standards and criteria, including safety standards.

- Train the people performing or supporting the technical solution process as needed, including safety standards.

Product Integration

- *Satisfy the applicable requirements and standards for packaging and delivering the product*, including those for *safety and security*.

Verification*

- **Establish and maintain the environment** needed to support verification. For example, a product test may require simulators, emulators, scenario generators, data reduction tools, environmental controls, and interfaces with other systems.

- **Establish and maintain verification procedures and criteria** for the selected work products.

*Implicit*
**Validation**

- *Establish and maintain the environment* needed to support validation.
- *Establish and maintain procedures and criteria for validation* to ensure that the product or product component will fulfill its intended use when placed in its intended environment.

*Implicit*

CMMI® – Support Process Areas and Assurance

- Configuration Management (CM)
- Product and Process Quality Assurance* (PPQA)
- Measurement and Analysis* (MA)
- Decision Analysis and Resolution (DAR)
- Organization Environment for Integration (OEI)
- Causal Analysis and Resolution (CAR)

*Implicit
Configuration Management

- Perform reviews to ensure that changes have not compromised the safety and/or security of the system.
CMMI® – Support Assurance Objectives - PPQA

Product and Process Quality Assurance*

- *Objectively evaluate the designated work products and services against the applicable process descriptions, standards, and procedures.*

*Implicit

Measurement and Analysis*

- **Establish and maintain measurement objectives** that are derived from identified information needs and objectives. The sources for measurement objectives may be management, technical, project, product, or process implementation needs.

- **Specify measures** to address the measurement objectives. Measurement objectives are refined into precise, quantifiable measures.

*Implicit

Decision Analysis and Resolution

- Establish and maintain guidelines to determine which issues are subject to a formal evaluation process. For example, on design-implementation decisions when technical performance failure may cause a catastrophic failure (e.g., safety of flight item).

Organizational Environment for Integration

- Plan, design, and implement an integrated work environment, including tradeoff of safety and security costs and benefits.

Causal Analysis and Resolution

- **Determine which defects and other problems will be analyzed further**, including **safety impact considerations**.
Beyond The CMMI®
Safety and Security Extensions for Integrated Capability Maturity Models

1. Ensure Safety and Security Competency
2. Establish Qualified Work Environment
3. Ensure Integrity of Safety and Security Information
4. Monitor Operations and Report Incidents
5. Ensure Business Continuity
6. Identify Safety and Security Risks
7. Analyze and Prioritize Risks
8. Determine, Implement, and Monitor Risk Mitigation Plan
10. Develop and Deploy Safe and Secure Products and Services
11. Objectively Evaluate Products
12. Establish Safety and Security Assurance Arguments
13. Establish Independent Safety and Security Reporting
14. Establish a Safety and Security Plan
15. Select and Manage Suppliers, Products, and Services
16. Monitor and Control Activities and Products

Source: United States Federal Aviation Administration, Safety and Security Extensions for Integrated Capability Maturity Models, September 2004

www.faa.gov/ipg
What Standards Support System and Software Assurance?
Dependability Standards

Safety and Security Standards

**IEC 61508**
Functional Safety

**IEC 60880**
SW in nuclear power safety systems

**DO 178B**
SW considerations in airborne equip certification

**ISO/IEC 9796**
Digital Security Schemes

**ISO/IEC 10181**
Security frameworks for open systems

**ISO/IEC 15408**
Common Criteria for IT Security Evaluation

**ISO/IEC 17799**
Code of Practice for Information Security Management

**ISO/IEC 21827**
Systems Security Engineering CMM

**ISO/IEC 17799**
Code of Practice for Information Security Management

**ISO/IEC 21827**
Systems Security Engineering CMM

**IEEE P1619**
Standard Architecture for Encrypted Shared Storage Media

**IEEE P1700**
Security Architecture for Certification and Accreditation of Information

**IEEE P2200**
Baseline Operating System Security

**MIL-STD-882D**
Standard Practice for System Safety

**DEF STAN 00-56**
Safety Management Requirements for Defence Systems

**IEEE P1228**
SW safety plans

**IEEE 1228**
SW in nuclear power safety systems

**IEEE P2200**
Baseline Operating System Security

**IEEE CS**
Military

**RTCA**

**ISO**

**IEC**

**IEEE CS**

**RTCA**

**CMMI Technology Conference, Track 6, Thursday, 18 November 2004, 0855**

Paul R. Croll

Slide 31
“Each Federal agency shall develop, document, and implement an agency-wide information security program to provide information security for the information and information systems that support the operations and assets of the agency, including those provided or managed by another agency, contractor, or other source…”

- Federal Information Security Management Act of 2002

Source: FISMA Implementation Project, Dr. Ron Ross, NIST, April 2004
NIST FISMA Implementation Project Standards and Guidelines

- FIPS Publication 199 (Security Categorization)
- NIST Special Publication 800-37 (Certification & Accreditation)
- NIST Special Publication 800-53 (Security Controls)
- NIST Special Publication 800-53A (Assessment)
- NIST Special Publication 800-59 (National Security)
- NIST Special Publication 800-60 (Category Mapping)
- FIPS Publication 200 (Minimum Security Controls)

Source: FISMA Implementation Project, Dr. Ron Ross, NIST, April 2004
Have you addressed the assurance implications of your CMMI®-compliant processes?

Do your assurance processes meet your business requirements?

- Business process requirements
- Legal and regulatory requirements
- Marketplace requirements
- Customer-specific requirements
- Product-specific requirements
Achieving System and Software Assurance Through CMMI®-Compliant Processes

1. Understand Your Business Requirements for Assurance

2. Look to the CMMI® for Assurance-Related Process Capability Expectations

3. Look to Standards for Assurance Process Detail

4. Build or Refine and Execute Your Assurance Processes
For More Information . . .

Paul R. Croll
Computer Sciences Corporation
5166 Potomac Drive
King George, VA  22485-5824

Phone:    +1 540.644.6224
Fax:       +1 540.663.0276
e-mail:   pcroll@csc.com

For IEEE Standards:
http://computer.org/standards/sesc/
http://ieeelia.org/iasc/
http://computer.org/cspress/CATALOG/st01110.htm

For ISO/IEC Standards:
http://saturne.info.uqam.ca/Labo_Recherche/Lrgl/sc7/