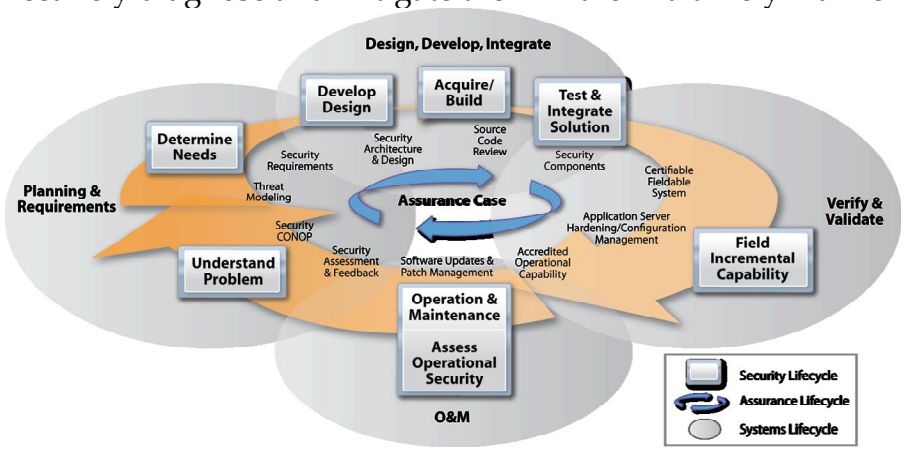
Summary of Assurance for CMMI® Efforts

System and Software Assurance is defined as

- The level of confidence that software is free from vulnerabilities, either intentionally designed into the software or accidentally inserted at anytime during its lifecycle, and that the software functions in the intended manner. *CNSS Instruction No. 4009, "National Information Assurance Glossary," Revised 2006*
- Grounds for confidence that an entity meets its relevant needs, goals or objectives for safety, security and dependability or other characteristics deemed to be critical, and possesses the related required properties. *ISO/IEC CD 15026, 2007, Systems and Software Assurance*

Current problems in achieving System and Software Assurance include:

- Assurance-related risks have dramatically increased due to the simultaneous growth in software vulnerabilities and threats
- Commonly used risk management processes inadequately address these threats and risks
- Government and industry are being confronted by risks presented by suppliers of software products and services
- Current development and acquisition processes inadequately address System and Software Assurance
- There is a fundamental lack of both the scientific understanding of software risks, and the capabilities to effectively diagnose and mitigate them in the in a timely manner



To solve this problem a blend of process (CMMI, ISO 9000) and product (Certification and Accreditation, Common Criteria, static code analysis) solutions is required. To address the process portion, the Assurance Working Group has created two work products

1. A draft set of assurance goals and practices that harmonize and enhance existing Security Capability Maturity Models (MSSDM, SSE-CMM)
2. A mapping of the draft set of assurance goals and practices to the CMMI-DEV v1.2

The mapping of the practices to CMMI-DEV v1.2 can serve as the basis for creating an Assurance Focus Topic as a third work product. The Focus Topic would document the assurance thread within the CMMI practices in a format similar to the CMMI for Acquisition Primer. This document can assist organizations with making progress in the integration of systems and software assurance as part of their continuous process improvement efforts.

Material adapted from "Leveraging CMMs and Standards for Assurance" Paul Croll and Michele Moss SSTC 2008, Track 6, Wednesday, April 30