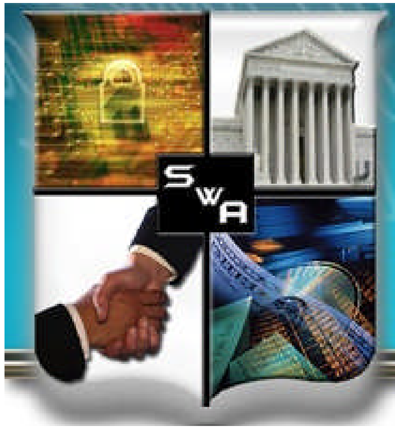


SOFTWARE ASSURANCE FORUM

BUILDING SECURITY IN

*4 November 2009*

# DoD-DHS-NIST
# Software Assurance Forum
# Evolution in SwA Processes
# Panel Briefing

Facilitator: Michele Moss, Booz Allen Hamilton

Co-Chair DHS SwA Processes and Practices Working Group

Mini-Keynote: Lynn Penn, Lockheed Martin

SOFTWARE ASSURANCE FORUM

BUILDING SECURITY IN

# *As a community we have created resources for those who want to wear "Security Goggles"*

Executive Dashboards

People

Policy and Mission/Business Goals

Risk Management

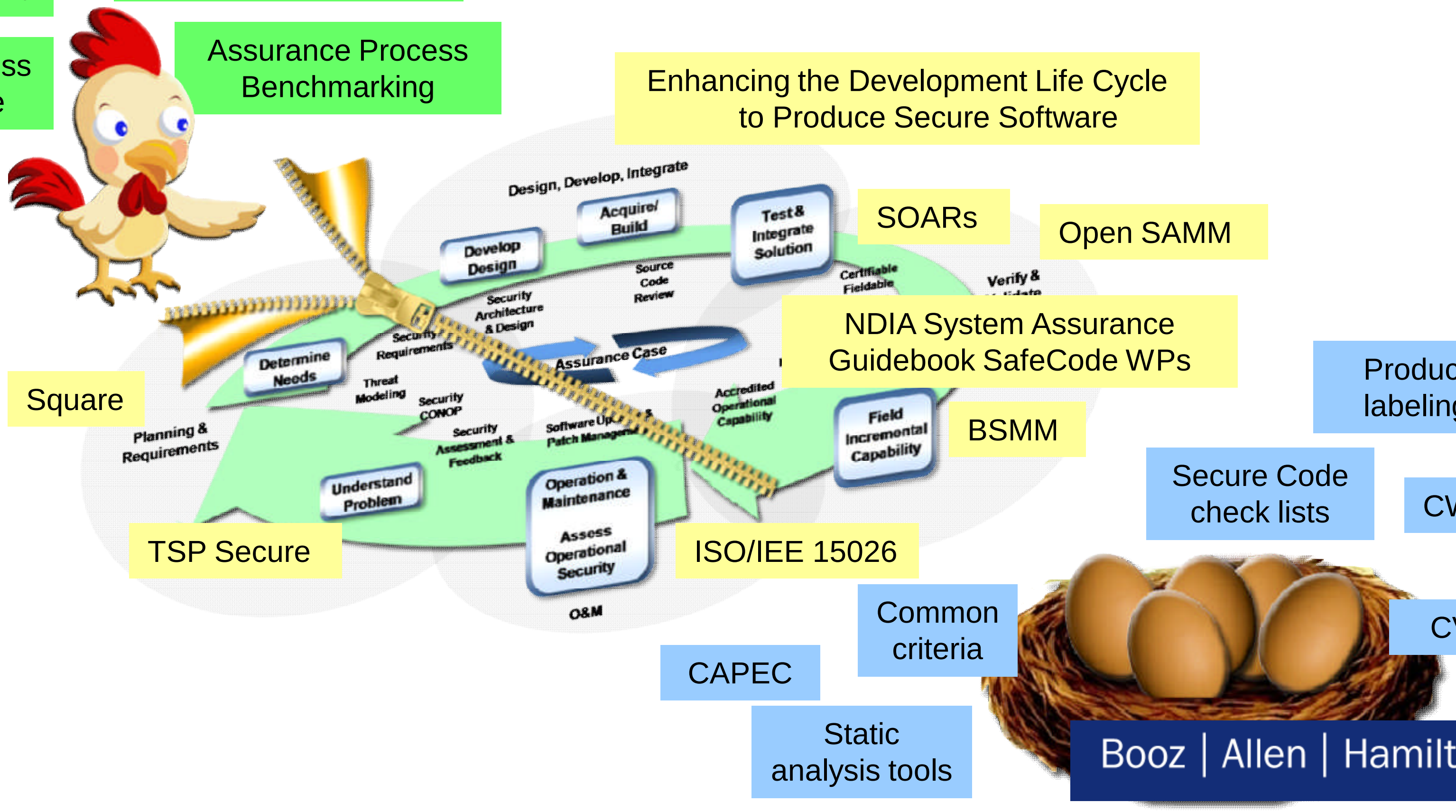
Acquisition Guidance

Business Case

Assurance Process Benchmarking

Tools to measure

Enhancing the Development Life Cycle to Produce Secure Software


Design, Develop, Integrate
Develop Design
Acquire/ Build
Test & Integrate Solution
Certifiable Fieldable
Verify & Validate
Source Code Review
Security Architecture & Design
Security Requirements
Assurance Case
Determine Needs
Threat Modeling
Security CONOP
Accredited Operational Capability
Field Incremental Capability
Planning & Requirements
Security Assessment & Feedback
Software Update Patch Management
Understand Problem
Operation & Maintenance
Assess Operational Security
O&M

SOARs

Open SAMM

NDIA System Assurance Guidebook SafeCode WPs

Square

BSMM

Product labeling

Secure Code check lists

CWE

TSP Secure

ISO/IEE 15026

Common criteria

CVE

CAPEC

Static analysis tools

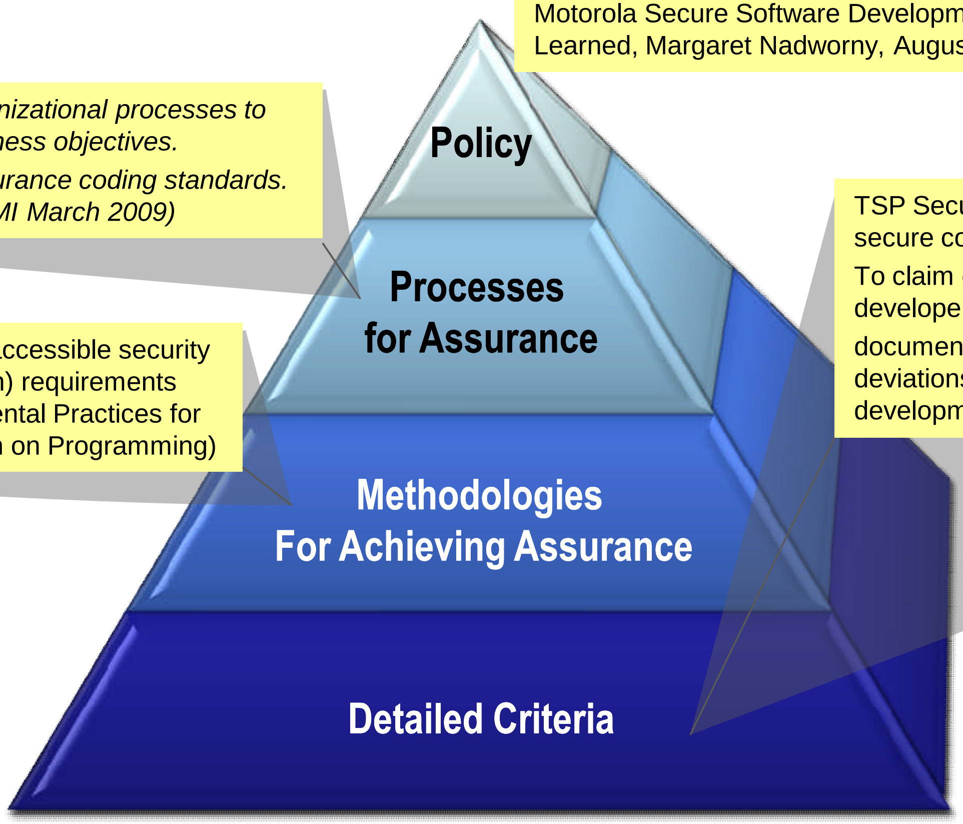
Booz | Allen | Hamilton

## *And are in the process of linking them together in a way that supports business/mission goals*

"It is the policy of Motorola to offer security solutions designed to protect the confidentiality, integrity and availability of information and other assets appropriate to their value to Motorola, and to service providers (and their customers) using Motorola products." (source: Motorola Secure Software Development Model (MSSDM) Lessons Learned, Margaret Nadworny, August 10, 2007)

*Establish and maintain organizational processes to achieve the assurance business objectives.*

*Identify deviations from assurance coding standards. (Source: Assurance for CMMI March 2009)*



TSP Secure CERT SCI provides language specific secure coding guidelines for C, C++, and Java.

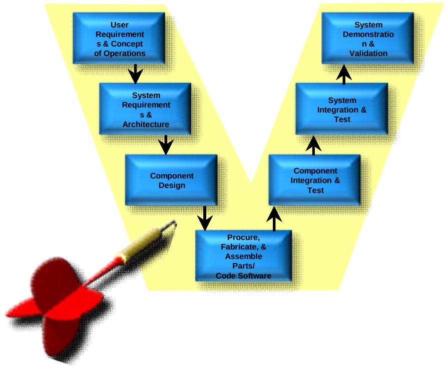
To claim compliance with a standard, software developers must be able to produce on request documentation as to which systematic and specific deviations have been permitted during development.

BSIMSR Level 1: Provide easily accessible security standards and (compliance-driven) requirements Safecode Whitepaper - Fundamental Practices for Secure SW Development (section on Programming)

SOFTWARE ASSURANCE FORUM

BUILDING SECURITY IN

# Operationalizing includes addressing challenges


User Requirements & Concept of Operations

System Requirements & Architecture

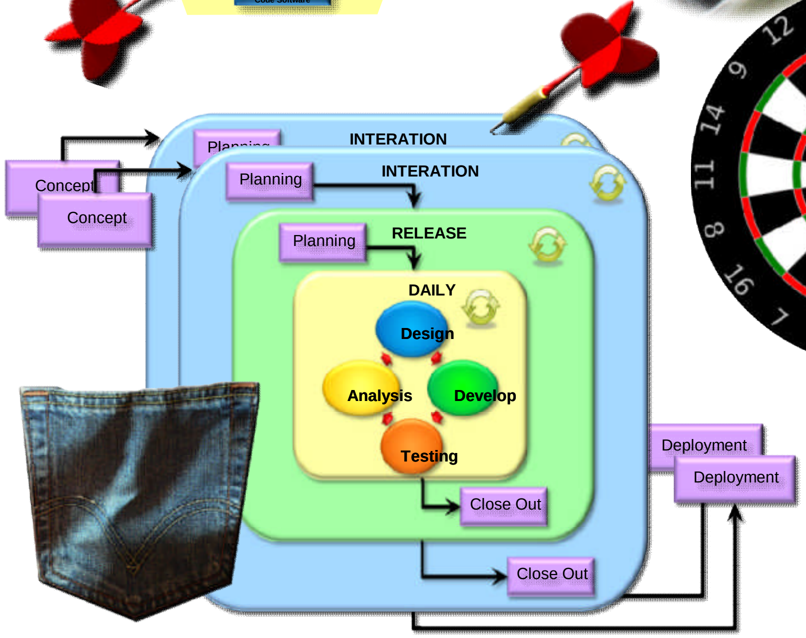
Component Design

Procure, Fabricate, & Assemble Parts/ Code Software

Component Integration & Test

System Integration & Test

System Demonstration & Validation


Concept

Concept

Planning

INTERATION

Planning

INTERATION

Planning

RELEASE

DAILY

Design

Analysis

Develop

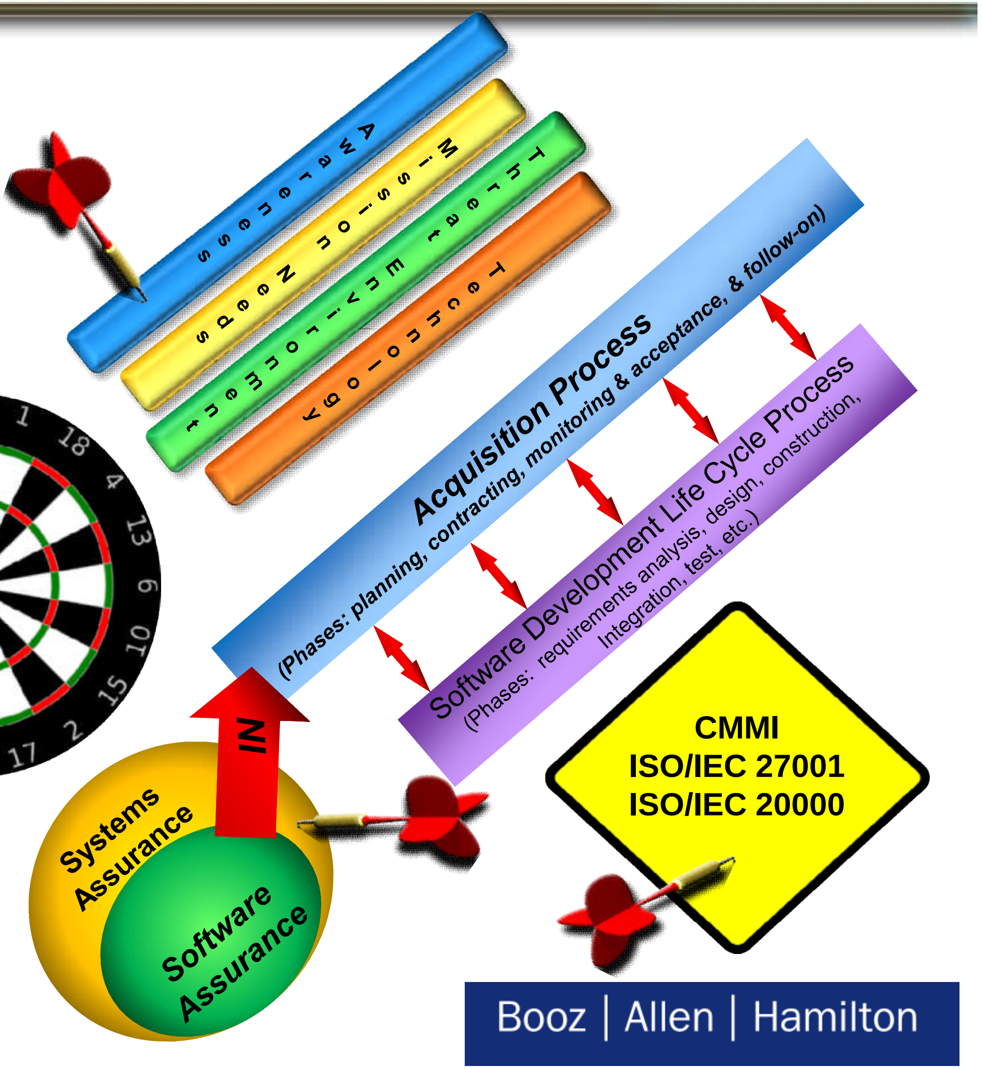
Testing

Close Out

Close Out

Deployment

Deployment


Awareness

Mission Needs

Threat Environment

Technology

Acquisition Process

(Phases: planning, contracting, monitoring & acceptance, & follow-on)

Software Development Life Cycle Process

(Phases: requirements analysis, design, construction, Integration, test, etc.)

IN

Systems Assurance

Software Assurance

CMMI
ISO/IEC 27001
ISO/IEC 20000

Booz | Allen | Hamilton

# *Participants*

- Facilitator: Michele Moss, Booz Allen Hamilton
- Mini Keynote: Lynn Penn, Lockheed Martin
- Janne Uusilehto, Vice Chairman of the Board / SAFECode
- David White, SEI/CERT
- Jeffrey Ritter, Esq., Water’s Edge

Note to self: Our stakeholder community includes the end user who in today’s technology enabled environment relies on software to have accurate and protected information ready when needed to support their business or personal efforts.
How do we help them help us? How do they help us?

Homeland Security

4 November 2009

# DoD-DHS-NIST Software Assurance Forum Mini-Keynote on Process

Mary Lynn Penn, Lockheed Martin

LOCKHEED MARTIN

# *Mini-Keynote Agenda*

- Where Are We?
  - The Problem
  - The Need
- Where Are We Going?
  - Critical Success Factors and Drivers
  - Process Definition Drivers
- Challenges
  - Choosing the “Right” Process, Standard and Scope
  - Management

# Where Are We? – The Problem

- Adopted Industry Standards do not include a robust description or requirements for software assurance
  - ISO 9001
  - CMMI
  - AS 9100
- Projects have been forced to use their own initiatives to accommodate the risks
  - When they see them
  - If they see them
  - Ad Hoc and not institutionalized
- Because the focus has been at the project level, the organization/ enterprise has remained “uninvolved”

# Where Are We? – The Problem

- A mature project team needs a defined project process
  - Each project will likely have its own Standard Process
    - Most will assume Quality Assurance implies security
    - Most will assume Risk implies security
  - Formulating a brand new process, never deployed by any team member, is always risky

# Where Are We – The Need

- Well-defined comprehensive project processes are critical to a project team’s success
  - Processes must address all aspects of software development – this includes security
- Customers increasingly expect team processes to be common, integrated and mature
- A mature project approach to a comprehensive process enables “proactive” management

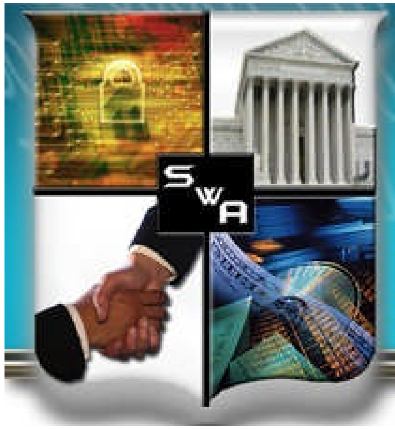
# Where Are We Going?

***Critical Success Factors for Comprehensive Team Processes***

- Project **process definition** based on
  - Shared objectives
  - Shared process needs
  - Shared vision
  - Clearly defined roles and responsibilities
- Common **process infrastructure**
  - Industry standard
  - Organization Standard Process
- Project **process measurement** in areas critical to software security

# *Software Security Definition Drivers*

- Project specific needs and objectives
- Project risks and opportunities
- Organizational structure and security needs
- Program management needs
  - Project security reporting (cost, schedule, etc.)
  - Measurement (performance, productivity, phase specific, etc.)
- Work environment



# Challenges - Process

The “right” security process is one that

- Meets requirements, including standards
  - From the customer
  - From the individual organizations
- Is appropriately suited to the domain and project
- Contains necessary and sufficient process elements
- Is integrated across the disciplines
- Is measurable
- Supports development of a quality work product

# *Challenges – Standard*

- Support current process infrastructure to leverage common processes
  - ISO 27001 complements ISO 9001 and ISO 20000
    - Focused on the management system
    - Shared process for management review, document/records control, corrective and preventive action
    - Aligned with NIST risk management and security control guidance
  - CMMI-SVC complements CMMI-DEV
    - Focused on capability and process improvement
    - Shared core of 16 process areas
    - Security Process Reference Model (PRM) to elaborate

# *Challenges – Standard*

- Support current process infrastructure to leverage common processes (contd.)
  - Government customers often require specific standards for system certification and accreditation
  - Less formal, but more specific models and practice lists can provide detailed guidance to support formal frameworks

# *Challenges – Scope*

- Software assurance extends beyond the SDLC
- Resilience
  - As an Engineering goal may increase complexity
  - As an Organizational goal may extend dependencies
    - Supply Chain Management
    - Organizational risk management
- SEI CERT – Resiliency Maturity Model (RMM)
  - New process areas within a capability and maturity framework
  - Operational focus

# *Challenges – Management*

- Increased requirements and complexity
- Interoperability expectations
- Continually changing threat landscape
- Emerging technology disruptors

# Summary

- Existing frameworks and practices form the foundation for security processes
- SW assurance needs extend beyond the SDLC into operational and organizational matters
- Array of standards options are emerging and blend well with existing process technology
- Challenges include maintaining focus and fostering innovation within an evolving scenario

# Contact Information

**Mary Lynn Penn**

**Lockheed Martin Information Systems & Global Services**

**mary.lynn.penn@lmco.com**

# *Participants*

- Facilitator: Michele Moss, Booz Allen Hamilton
- Mini Keynote: Lynn Penn, Lockheed Martin
- Janne Uusilehto, Vice Chairman of the Board / SAFECode
- David White, SEI/CERT
- Jeffrey Ritter, Esq., Water’s Edge

# *What is needed next?*

We have gained an understanding of many secure development practices and are having success with broader adoption. Are there any areas of the SDLC where more work is urgently needed? What are the challenges with implementing a secure development lifecycle? How do business objectives fit into the picture?

# *What is needed next?*

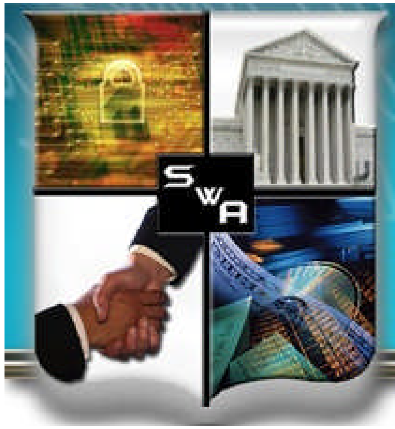
- How to ensure suppliers skills for SW security engineering
- How to ensure 3rd party SW security engineering skills
- How to ensure good SW security verification/testing
- How to ensure reasonable expectations towards to SW security
- How to utilize platform HW security for security critical apps
- How to keep regulation in level it enables/supports innovation
- Fair and reasonable liability sharing between players
- Proper curriculum available for universities, but also for schools

# *What is needed next?*

- How to verify security from binaries as well
- How to keep reactive SW security in right limits (80/20 -rule)
- What is the right role for certification (the true value of it)
- How to keep “logical” mistakes away from SW & services
- Business management involvement to requirements settings
- Reasonable global harmonization of SW security (US,China,EU...)
- Lawful interception related issues harmonization globally
- How to measure SW security and ensure the right level

# *Participants*

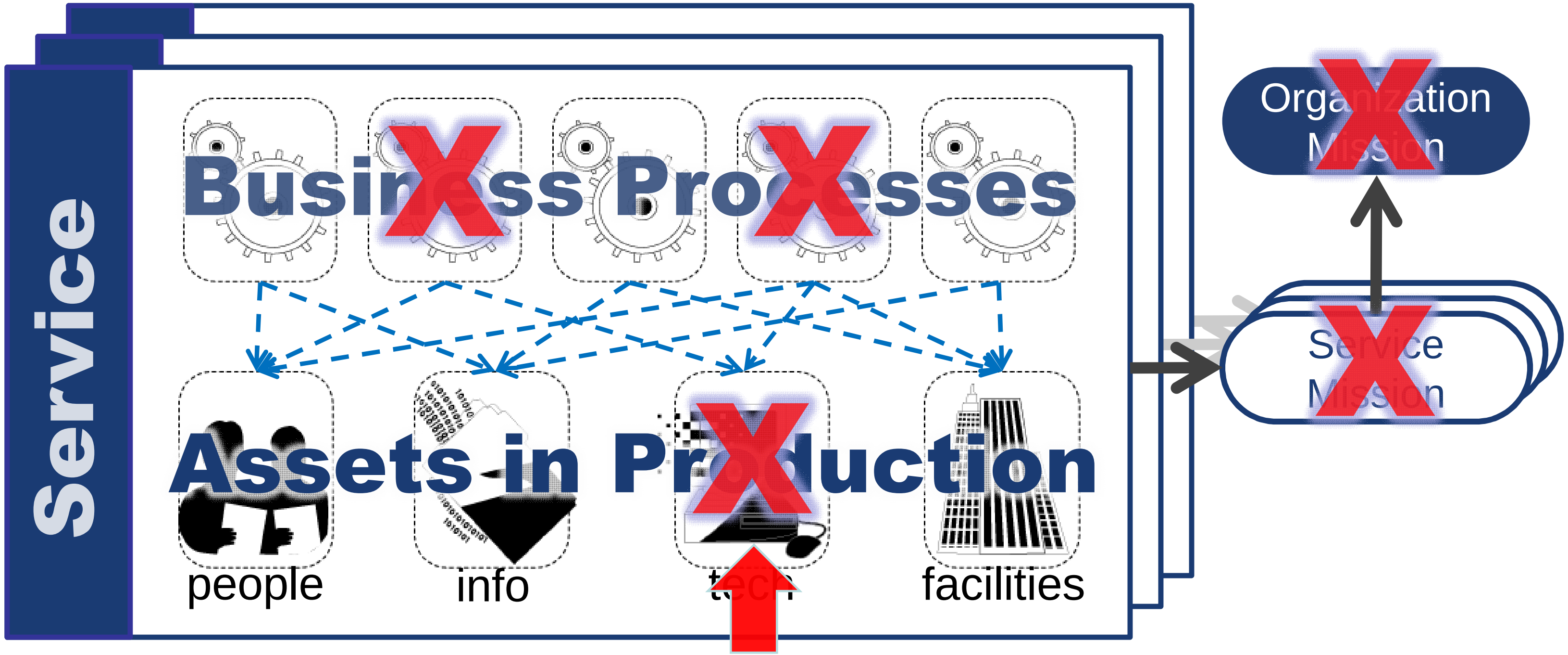
- Facilitator: Michele Moss, Booz Allen Hamilton
- Mini Keynote: Lynn Penn, Lockheed Martin
- Janne Uusilehto, Vice Chairman of the Board / SAFECode
- David White, SEI/CERT
- Jeffrey Ritter, Esq., Waters Edge



# *Resiliency Perspective*

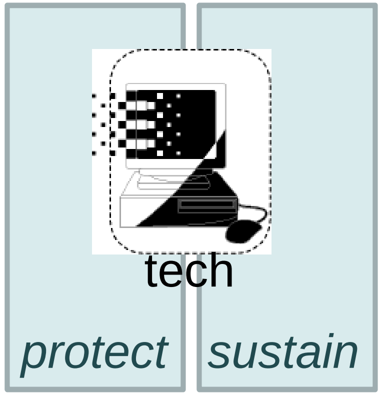
- Resiliency defined:
  - *The emergent property of an organization that can continue to carry out its mission after a disruption that does not exceed its limit*
  - Disruptions come from realized risk; sources of risk include software defects and vulnerabilities
- CERT® Resiliency Management Model (RMM)
  - Process improvement model
  - Addresses convergence of security, business continuity, and IT operations to manage operational risk and establish operational resiliency
  - www.cert.org/resiliency

# Asset view of resiliency

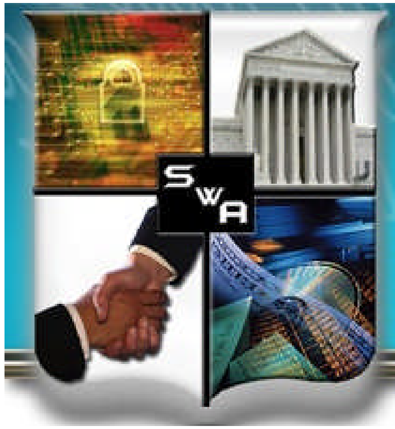


Software issues can impact availability and suitability of assets on which the organization depends

# *Resiliency begins at the asset level*



- Resiliency requirements form basis for protection and sustainment of an asset
- Resiliency requirements are informed by
  - Organization’s mission and strategy
  - Role of the asset in the service
  - Asset interdependencies
- Resiliency requirements must be addressed in development & acquisition of new software assets



# *SDLC issues*

Building security in clearly supports resiliency, but how do we

- Build-in continuity support for continued operation under extreme stress from realized risk? What if the risk is unforeseen?
- Develop to support resilient operation in the cloud?
- Identify and manage risks that stem from unmet requirements in development or acquisition?
- Build for dynamic asset-service interdependencies throughout the operation lifecycle?

# *Participants*

- Facilitator: Michele Moss, Booz Allen Hamilton
- Mini Keynote: Lynn Penn, Lockheed Martin
- Janne Uusilehto, Vice Chairman of the Board / SAFECode
- David White, SEI/CERT
- Jeffrey Ritter, Esq., Water’s Edge

# *The Value of Certification*

- Globally, standards-based business design and operation is accelerating as a foundational requirement for doing business.

- Software development has standards available against which to certify the development process.
  - Self-certification.
  - Third-party certification.

- Certification will not enhance competitive advantage *if* traditional contractual limitations on liability are permitted to persist.

*Questions?*

SOFTWARE ASSURANCE FORUM
BUILDING SECURITY IN

# *Join us at the SwA Working Groups*

Paul R. Croll
CSC
5166 Potomac Drive
King George, VA  22485-5824

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

Michele Moss
Booz Allen Hamilton
8283 Greensboro Drive
McLean, VA  22102

Phone:  +1 703.377.1254
Fax:  +1 703.902.3595
e-mail:  moss_michele@bah.com