SOFTWARE ASSURANCE FORUM

BUILDING SECURITY IN

What can an Acquirer do to prevent developers from make dangerous software errors?

OWASP AppSec DC 2012

April 5, 2012

Key questions

- Do acquirers know why they need include requirements for secure code?
- How do acquirers articulate the requirements for secure code?
- What standards and best practices exist to communicate expectations?
- What are the critical success factors for developers developing secure code?
- How do acquires know their requirements for secure code have been met?
- How should acquirers communicate with other stakeholders?
- Next Steps?

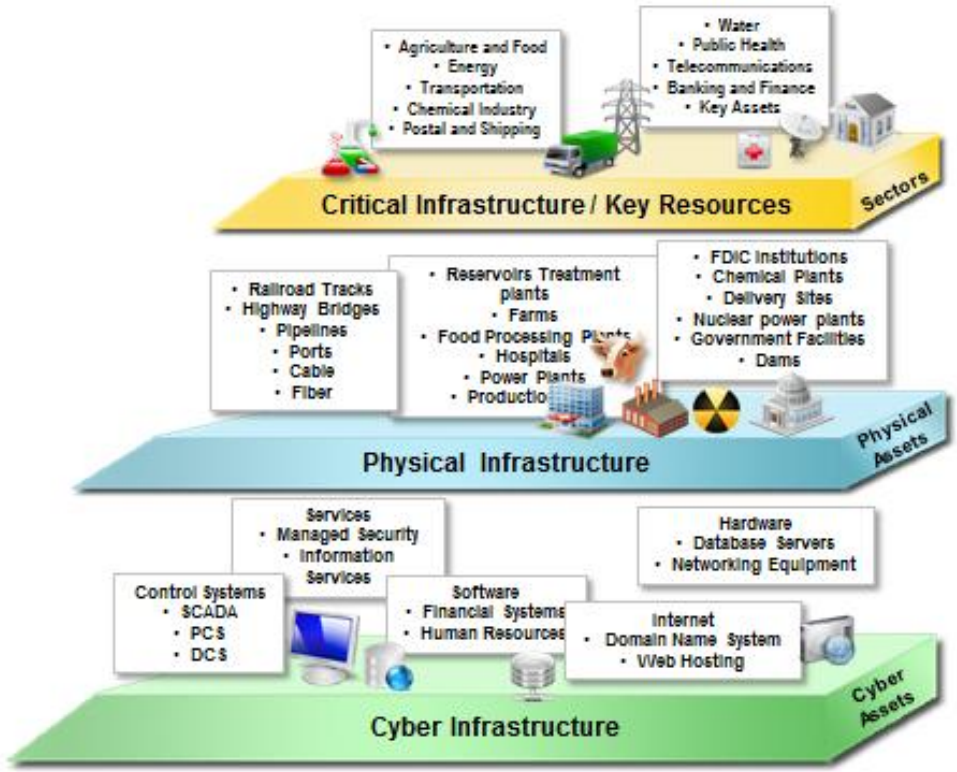
SOFTWARE ASSURANCE FORUM

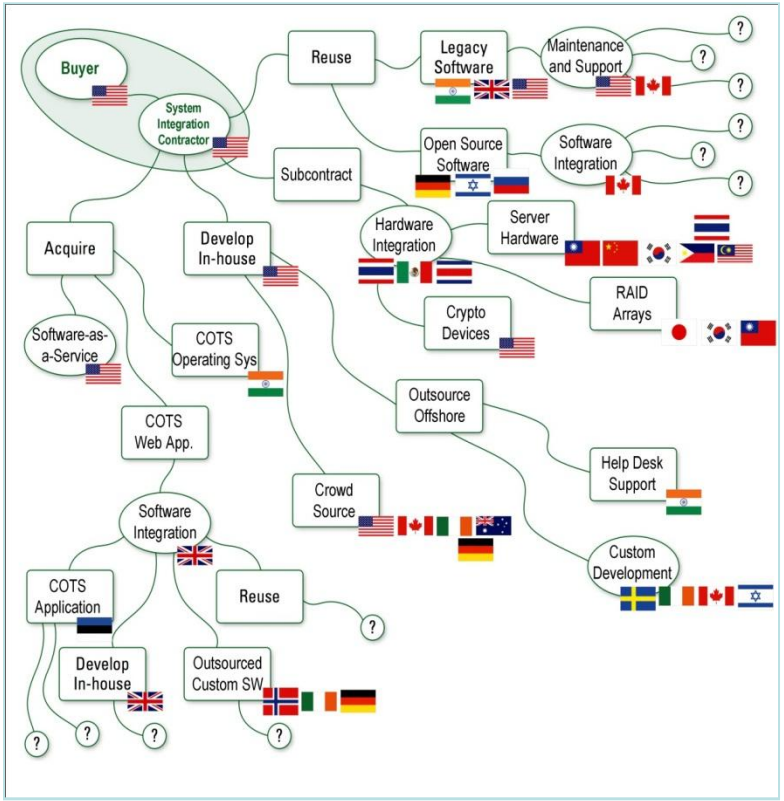
BUILDING SECURITY IN

Perspective on technology today

Technology is an integral part of our lives

IT and Communications products are assembled, built, and transported by multiple vendors around the





SOFTWARE ASSURANCE FORUM

BUILDING SECURITY IN

Acquirers of IT products and services trust that suppliers are addressing cyber security without validating

Prepare for the acquisition	Advertise the acquisition and select the supplier	Initiate an agreement	Monitor the agreement	Accept the product or service

Product Development and Maintenance
- Requirements Management
- Design/Develop
- Test

47% do not perform acceptance testing of third-party code
30% do not use static analysis/manual code
27% do not practice secure design
19% do not carry out security requirement definition
46% use own development method, rather than SDL or CMM/CMMI
15% follow SDL
20% follow CMM/CMMI ®
61% had no special incentive program to get developers and testers to work together
More than 70% do not measure developers with security related metrics

ROI was greater for those who employed a coordinated, prescriptive approach

Source: Forrester, “State of Application Security,” January 2011

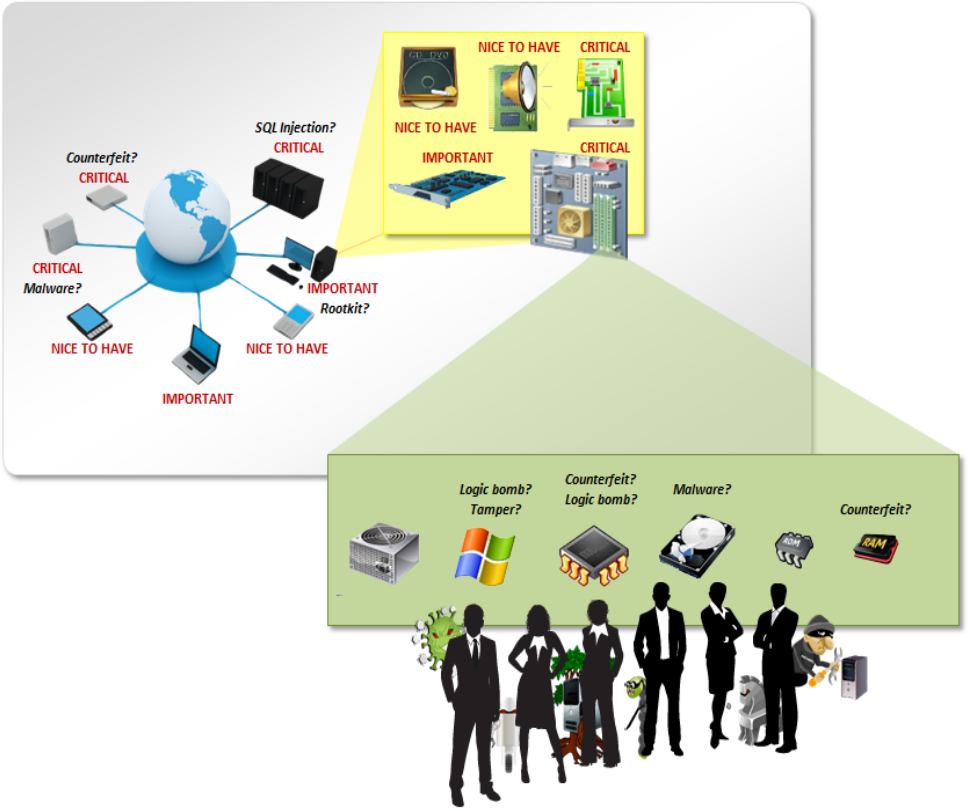
SOFTWARE ASSURANCE FORUM

BUILDING SECURITY IN

Malicious actors are taking advantage of abundant opportunities to tamper with and sabotage products …

What commonalities exist?	**83%** of victims were targets of opportunity **92% of attacks were not highly difficult** **86%** were discovered by a third party **96% of breaches were avoidable through simple or intermediate controls**
How do breaches occur?	**50% utilized some form of hacking** 49% incorporated malware (lower percentages included physical attacks, privilege misuse, and social tactics)

**** Source – 2011 Verizon Data Breach Investigations Report***

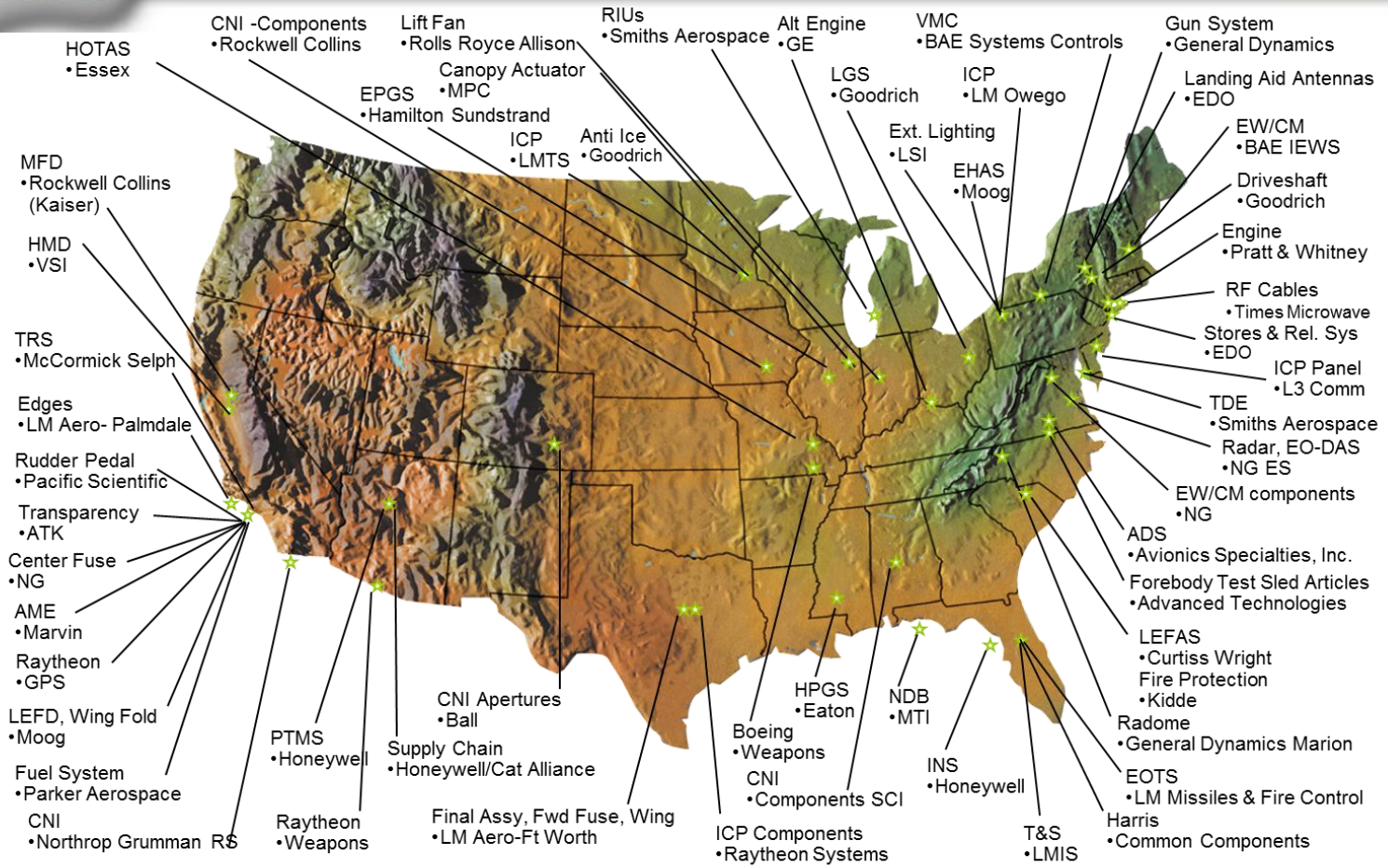


… ultimately compromising system integrity and operations

SOFTWARE ASSURANCE FORUM

BUILDING SECURITY IN

Joint Strike Fighter Extended Team – U.S.



Source: Lockheed Martin Aeronautics Company

SOFTWARE ASSURANCE FORUM

BUILDING SECURITY IN

F-35 Extended Team –
International Industrial Participation

U.K.

BAE SYSTEMS
Goodrich Adv. Sys
Helmet
Integrated Sys.
Martin Baker
Hambles Sturc.
Smiths +Others
Beaufort
Smiths
GKN
Microfiltrex
HS Claverham
HS Marston
QinetiQ
Didsbury Engr
Kennard
+ Others

Turkey

TAI
Ayesas
Havelsan
KaleKalip
TAI
Aselsan
MIKES
Hema
KaleKalip
ALP
Parsans

Gate Elektronic
ALP Aviation
Aselsan
AYESAS
Gate Elektronic
Havelsan
Hema/Alp
Kale Kalip
Marconi
Mikes
Parsan Steel
Forging
TAI
TEI
+ Others

Netherlands

ATS Kleizen
Fokker Elmo, Aero, Defense
Sun Electronic
Philips Aerospace
SP Aerospace
Thales Cyrogenics
DAP
Thales Optronics
Sun Electronic
Phillips Aerospace
Thales Cyrogenics + Others
Axxiflex
Senior Aerospace Bosman
PHM Group
Urenco
+ Others

Norway

Kongsberg
Metronor
Techni
NERA
Kongsberg
Kitron
3D Perception
Applica
Ericsson
Kitron

Metronor
Nammo
Natech
NERA
Presens
SensoNor AS
SINTEF
T & G Elektro
Thales Comm.
+Others

Australia

Micro LTD
Ferra Engineering
Hovitt
Cablex
Varley
Production Parts
Calytrix Technologies
+ Others
Micreo
Cablex
Lovitt + Others
Compucat
Rosebank Eng
+ Others

Denmark

Terma AS
GPV
SSE
IFAD
HiQ Wise
Corena
Terma
SSE
GPV
E.Falk Schmidt
Maersk Data Def
Elbo Production
Danish Aerotech
Hamann Electronics
+ Others

Italy

Alenia
Marconi Sirio Panel
Galileo
Piaggio
Moog- Caselle
UOP
Secondo Mona
Samputensilli
Marconi Selenia
York
+Others

OMA
Mecaer
Aerea
Aermacchi
Galileo
ASE
Forgital
Inossman
Logic
+ Others

Canada

Herovx-Devtek
Magellan-Chicopee
Honeywell Eng. Sys
DY4
Mindready
Howmet
Virtek +Others
Mustang Surv. Co
Bristol Aerospace
Graphico
Novatronics
DMG + Othes
Bombardier
Air Data Inc
CMC Electronics
Noranco + Others

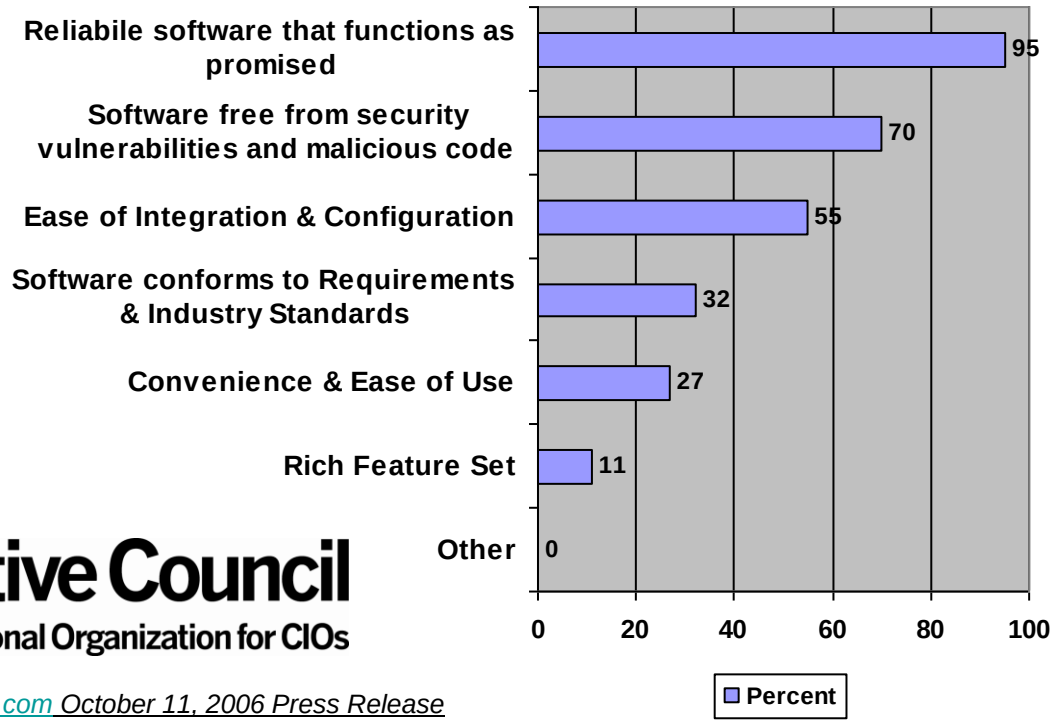
Global Development and Production

Source: Lockheed Martin Aeronautics Company

Key questions

- Do acquirers know why they need include requirements for secure code?
- How do acquirers articulate the requirements for secure code?
- What standards and best practices exist to communicate expectations?
- What are the critical success factors for developers developing secure code?
- How do acquires know their requirements for secure code have been met?
- How should acquirers communicate with other stakeholders?
- Next Steps?

Requirements for secure code are implicitly and not explicitly stated



CIO Executive Council
The Professional Organization for CIOs

https://www.cioexecutivecouncil.com October 11, 2006 Press Release

Contract requirements in recent SOWs is vague

- “Document and track security flaws and flaw resolution”.
- The Contractor certifies that at least one member of its staff assigned to this project working on any software code to be delivered under this effort has earned the Global Information Assurance Certification for Secured Software Programming or equivalent.
- The government intends to modify the contract as National Institute for Science and Technology (NIST) SCRM guidelines and standards evolve, and the contractor shall update its SCRM Plan to include such modifications at no cost to the government.
- What provisions are taken to ensure there is no malware on any hardware, firmware and/or software components?
- Define your approach for Software Assurance
- Present a plan for conducting security engineering/software assurance support

SOFTWARE ASSURANCE FORUM

BUILDING SECURITY IN

Current DOD RFP Content Considerations

- Section A: Solicitation Contract Form
- Section B: Supplies or services and prices/costs
  - Statement of Work (SOW)
  - System Requirements Document (SRD)
  - Compliance and Reference Document List (CDRLs)
- Section D: Packaging and marking
- Section E: Inspection and Acceptance
- Section F: Deliveries or performance
- Section G: Contract administration data
- Section H: Special contract requirements
- Section I: Contract Clauses
- Section J: List of Documents, Exhibits, and other Attachments
- Section K: Representations, Certification, and Other Statements of Offerors
- Section L: Instructions, conditions, and notice to offerors
- Section M: Evaluation factors for award

SOW to Include, but not Limited to:

- Conduct of Criticality Analysis (CA)
  - Identification of mission-critical functions that may result in Level 1 or Level 2 protection failures
  - Identification of logic-bearing elements of Level 1/2 failures
- Demonstration of visibility into supply chain and Software Assurance (SwA) for critical components
- Update of CA results and Program Protection risks and mitigations at each SETR

SRD to Include, but not Limited to:

- Detect and record incidents; sends alert
- Prevent onset of threat/ vulnerability that results in catastrophic or critical failure
- Return system to a normal operational state

CDRL DIDs to Include, but not Limited to:

- CA results 30 days before each SETR
- Design trade studies for selection of Level 1/2 logic bearing components
- Supply chain risk analysis for supplier selection

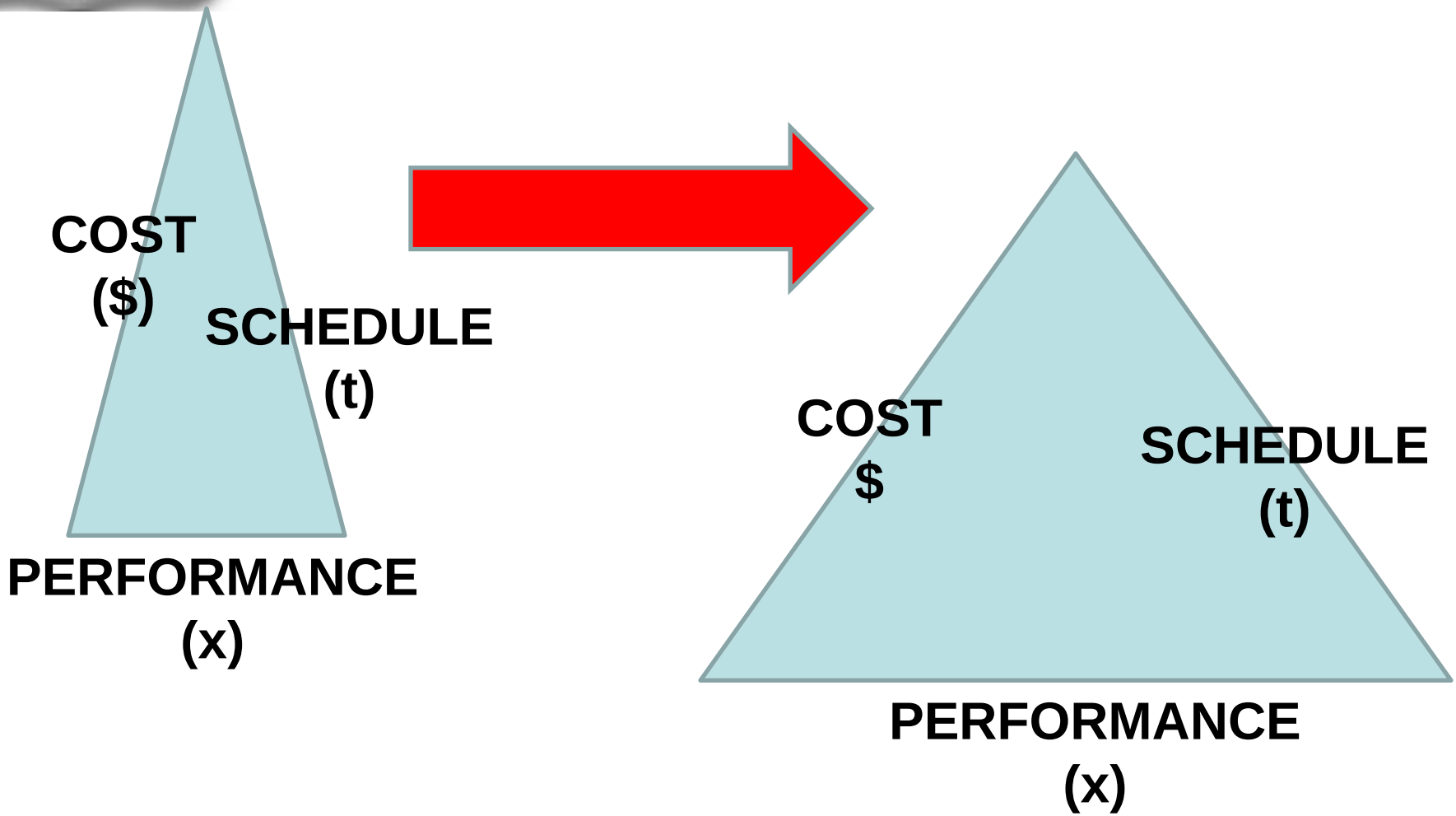
Section L, to Include, but not Limited to:

Request a description of Supply Chain Risk Management and SwA processes and techniques that will be used to achieve system protection and mission effectiveness

Section M, to Include, but not Limited to:

Evaluate proposed processes, including SCRM and SwA use in system specification and design, to mitigate threats and vulnerabilities to system mission effectiveness

Balancing risk when making trades



"Defacto" security requirements in NIST 800-53 rev 3 do not explicitly require secure code

- AC-2 Account Management
- AC-3 Access Enforcement
- AC-4 Information Flow Enforcement
- RA-5 Vulnerability Scanning
- CM-7 Least Functionality
- SI-3 Malicious Code Protection
- SI-10 Information Input Validation

Draft NIST SP 800-53 rev 4 has SwA controls for low, moderate, and high systems

- AT-3 Security Training
- CM-3 Configuration Change Control
- CM-7 Least Functionality
- SA-3 System Development Life Cycle
- SA -4 Acquisition Process
- SA -11 Developer Security Testing
- SA -15 Development Process, Standards, and Tools
- SA – 16 Developer-Provided Training
- SA – 17 Developer Security Architecture and Design

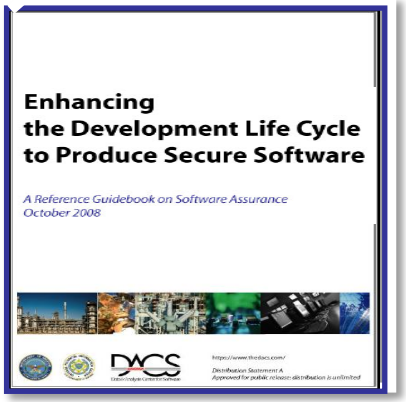
Key questions

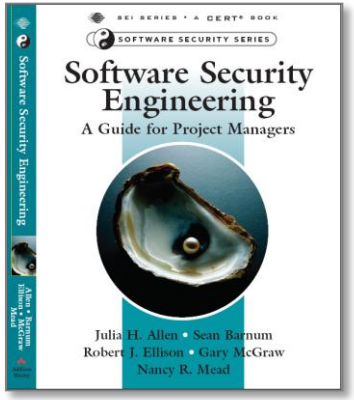
- Do acquirers know why they need include requirements for secure code?
- How do acquirers articulate the requirements for secure code?
- What standards and best practices exist to communicate expectations?
- What are the critical success factors for developers developing secure code?
- How do acquires know their requirements for secure code have been met?
- How should acquirers communicate with other stakeholders?
- Next Steps?

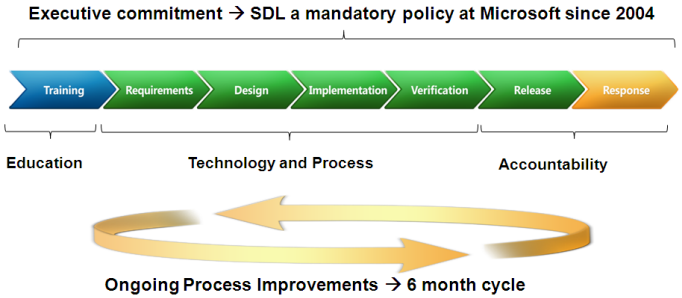
SOFTWARE ASSURANCE FORUM

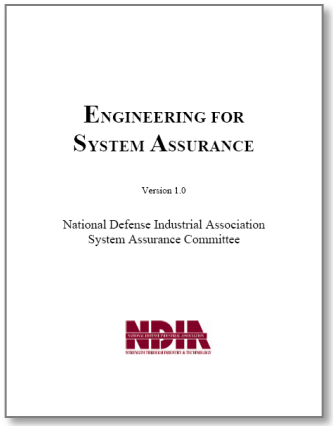
BUILDING SECURITY IN

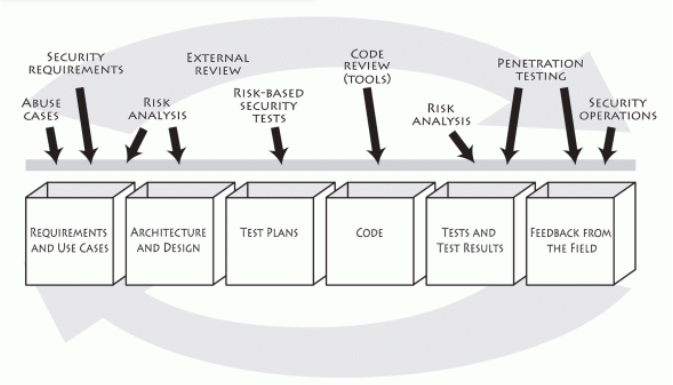
A majority of SwA best practices focus on developer-centric audiences from a security point of view



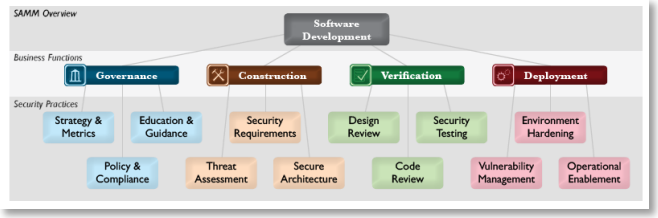








Assurance for CMMI ®



SOFTWARE ASSURANCE FORUM

BUILDING SECURITY IN

Application Security resources are available through industry efforts and relationships with industry leaders

Organizations **People**

Secure Coding Libraries

Secure Development Lifecycles

SwA Implementation Roadmaps

Supplier — Executive

Acquirer — Practitioner

Contract Language

Acceptance Testing Resources

Secure Development Guides

Open Source SwA Validation Tools

OWASP The Open Web Application Security Project http://www.owasp.org

www.owasp.org

BSIMM3

http://bsimm.com/

Homeland Security — Build Security In — Setting a higher standard for software assurance — Sponsored by DHS National Cyber Security Division

BuildSecurityIn.us-cert.gov

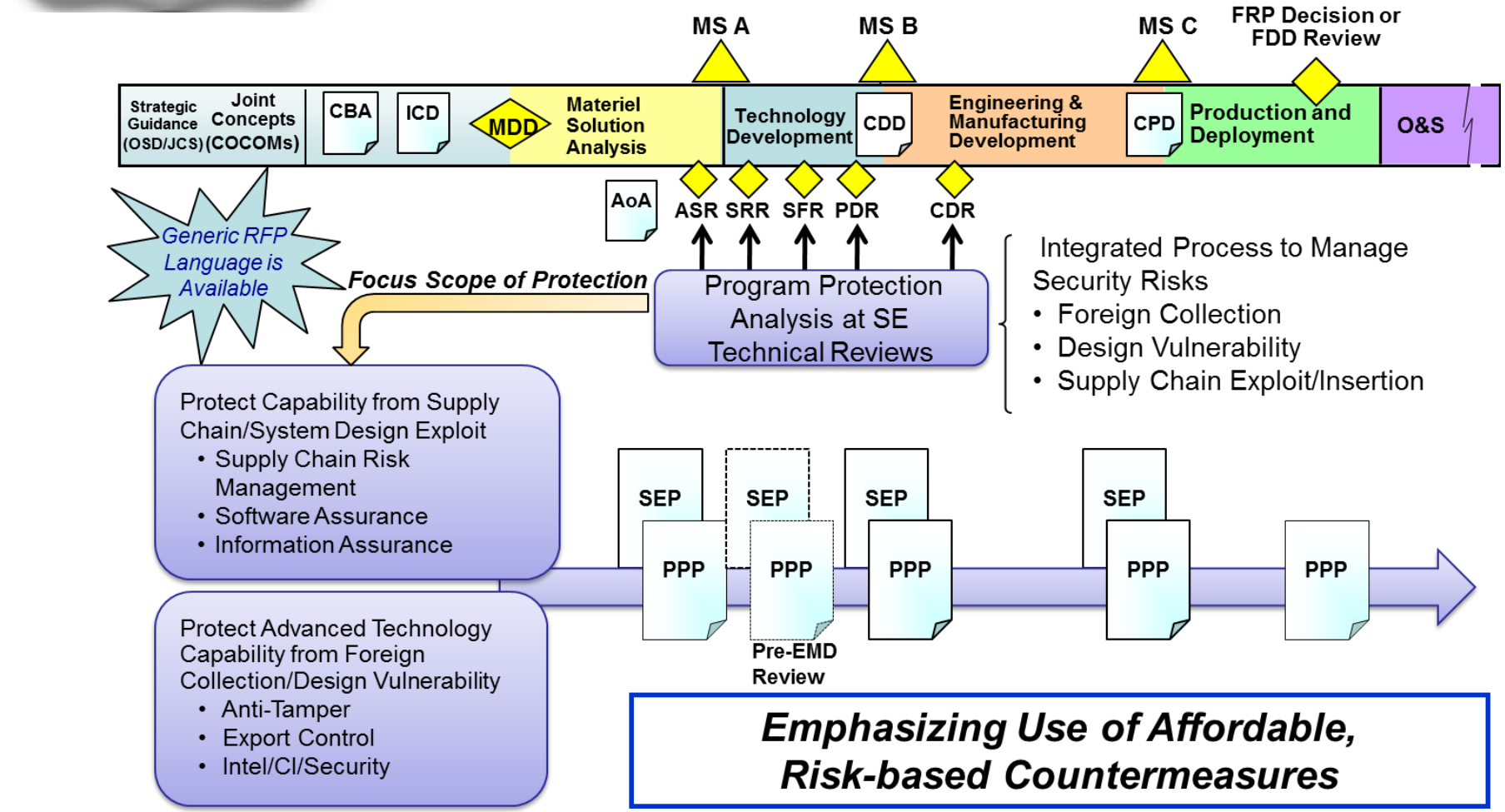
www.microsoft.com/sdl

www.safecode.or

SOFTWARE ASSURANCE FORUM

BUILDING SECURITY IN

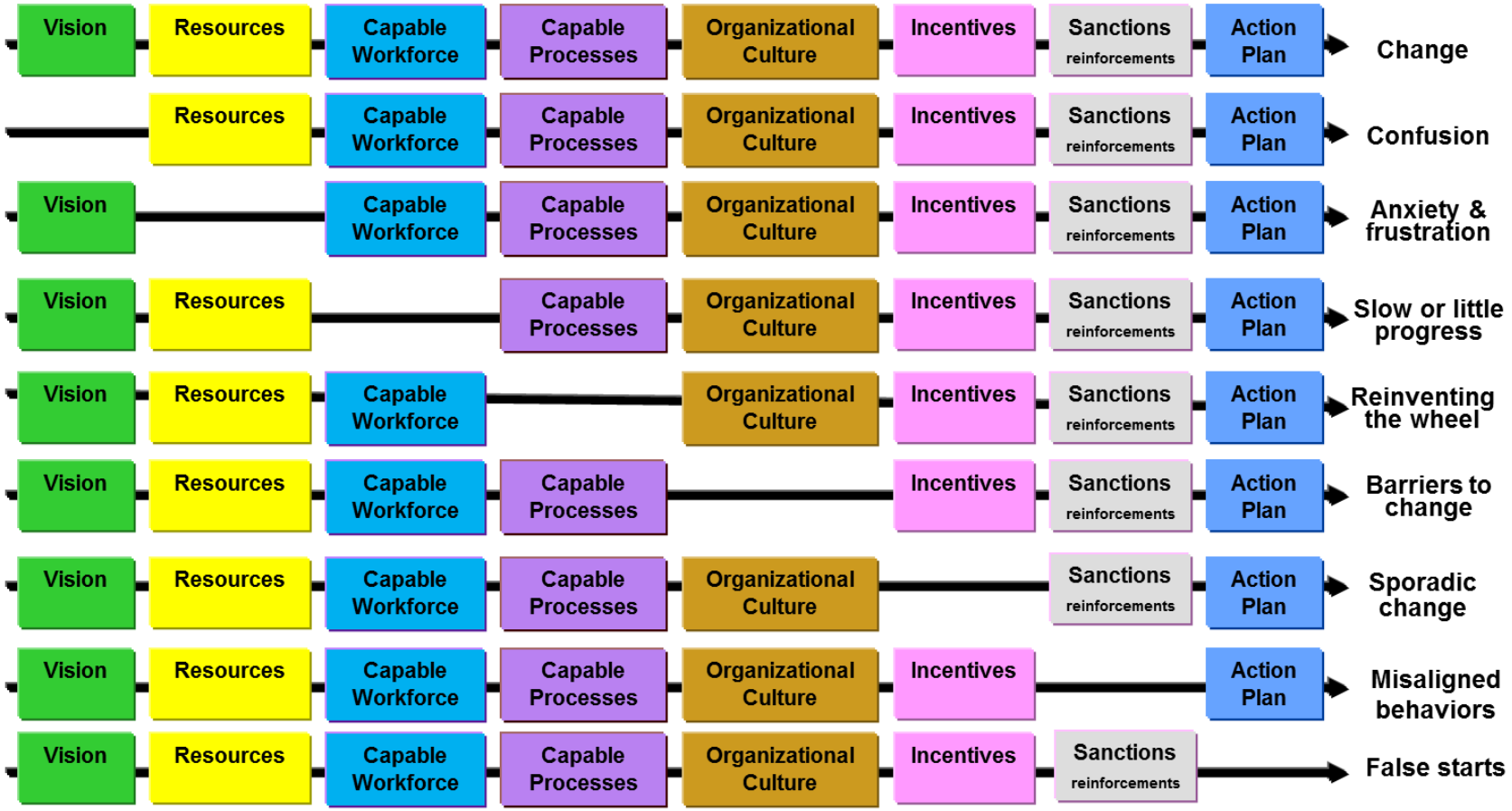
DOD Acquisition Reviews include Supply Chain Risk Management and Software Assurance



Key questions

- Do acquirers know why they need include requirements for secure code?
- How do acquirers articulate the requirements for secure code?
- What standards and best practices exist to communicate expectations?
- What are the critical success factors for developers developing secure code?
- How do acquires know their requirements for secure code have been met?
- How should acquirers communicate with other stakeholders?
- Next Steps?

Success requires identifying the missing elements of change



Adapted by Buttles from: Delorise Ambrose, 1987

SOFTWARE ASSURANCE FORUM

BUILDING SECURITY IN

Understanding business goals, software assurance requirements and associated is critical

Define Business Goals

Development Organization

DO 1 Establish the assurance resources to achieve key business objectives

DO 2 Establish the environment to sustain the assurance program within the organization

Development Project

DP 1 Identify and manage risks due to vulnerabilities throughout the product and system lifecycle

DP 2 Establish and maintain assurance support from the project

DP 3 Protect project and organizational assets

Enterprise Assurance Support

ES 1 Establish and maintain organizational culture where assurance is an integral part of achieving the mission

ES 2 Establish and maintain the ability to support continued delivery of assurance capabilities

ES 3 Monitor and improve enterprise support to IT assets

Prioritize funds and manage risks

Acquisition and Supplier Management

AM 1 Select, manage, and use effective suppliers and third party applications based upon their assurance capabilities.

Development Engineering

DE 1 Establish assurance requirements

DE 2 Create IT solutions with integrated business objectives and assurance

DE 3 Verify and Validate an implementation for assurance

Enable Resilient Technology

Sustained environment to achieve business goals through technology

The Assurance PRM Is A Holistic Framework that connects CMMI and RMM to facilitate communication

https://buildsecurityin.us-cert.gov/swa/proself_assm.html

Key questions

- Do acquirers know why they need include requirements for secure code?
- How do acquirers articulate the requirements for secure code?
- What standards and best practices exist to communicate expectations?
- What are the critical success factors for developers developing secure code?
- How do acquires know their requirements for secure code have been met?
- How should acquirers communicate with other stakeholders?
- Next Steps?

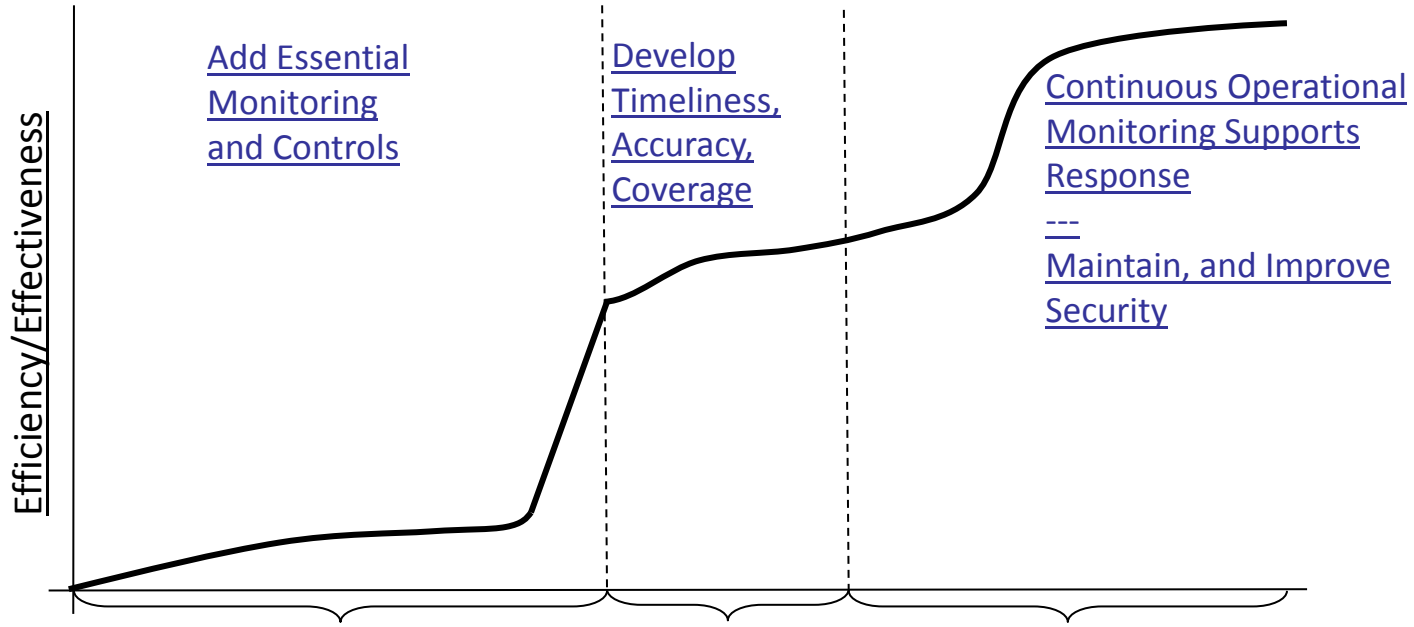
Measure, measure, and measure again

"The only man I know who behaves sensibly is my tailor; he takes my measurements anew each time he sees me. The rest go on with their old measurements and expect me to fit them."

- George Bernard Shaw

Source: www.CartoonStock.com

Robust measurement does not happen overnight and requires foundational capabilities in place to be effective



LINCOLN LABORATORY
MASSACHUSETTS INSTITUTE OF TECHNOLOGY

Courtesy of Matt Coose, DHS

Security control measures

- Percent of new systems that have completed certification and accreditation (C&A) prior to their implementation (NIST SP 800-53 Control: CA-6: Security Accreditation)
- Percent of employees who are authorized access to information systems only after they sign an acknowledgement that they have read and understood rules of behavior (NIST SP 800-53 Controls – PL-4: Rules of Behavior and AC-2: Account Management)
- Percent of the agency's information system budget devoted to information security (NIST SP 800-53 Controls – SA-2; Allocation of Resources)

Security Control Measures address compliance with the end state of the system, but not the underlying processes, structures, and code

Measurement for secure code requires understanding code level attributes …

Vulnerability

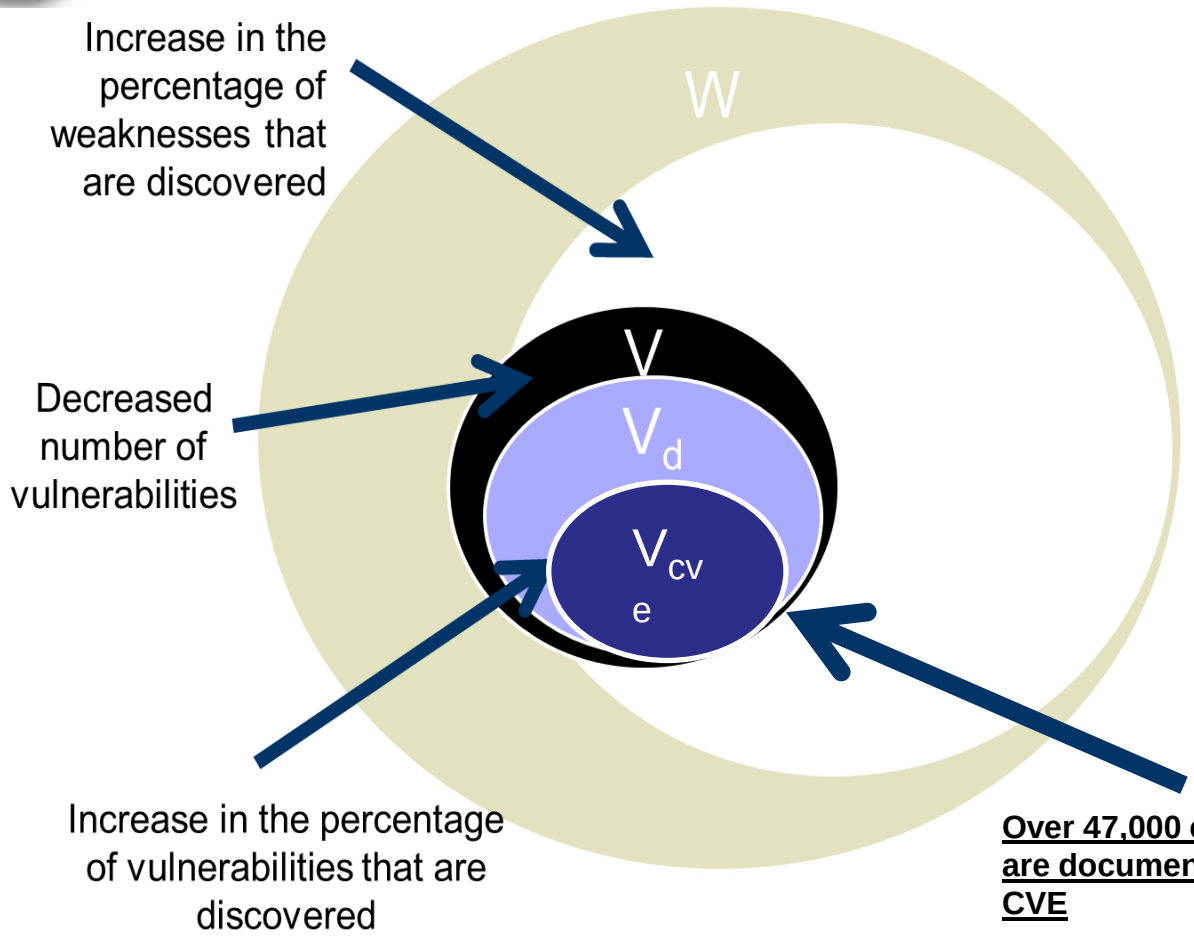
- A *(software) vulnerability* is a collection of one or more weaknesses that contain the right conditions to permit unauthorized parties to force the software to perform unintended behavior (a.k.a. “is exploitable”)
- CVE® is a publicly available and free to use list or dictionary of standardized identifiers for common computer vulnerabilities and exposures.

Weakness

- A *(software) weakness* is a property of software/systems that, under the right conditions, may permit unintended / unauthorized behavior.
- The Common Weakness Enumeration (CWE™) is a list of software weaknesses.

Source: http://makingsecuritymeasurable.mitre.org/ and DHS Software Assurance Program

From incident response teams we know that some vulnerabilities are exploited



Adapted from Richard Struse, DHS Software Assurance Program

SOFTWARE ASSURANCE FORUM

BUILDING SECURITY IN

Industry vetted practices to AVOID common software weaknesses that can be exploited are available today

Today

CWE & SANS Institute TOP 25 MOST DANGEROUS SOFTWARE ERRORS

OWASP The Open Web Application Security Project http://www.owasp.org

Tomorrow

Common Weakness Scoring System (CWSS™)

Common Weakness Risk Analysis Framework (CWRAF™)

Adapted from Richard Struse, DHS Software Assurance Program

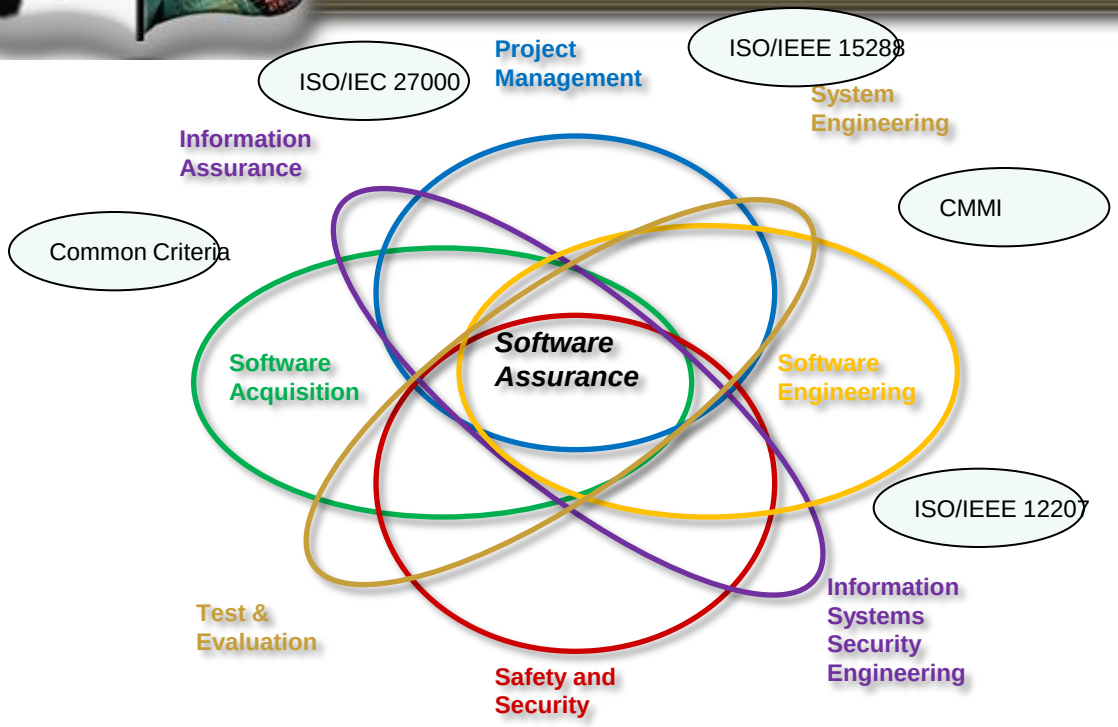
Key questions

- Do acquirers know why they need include requirements for secure code?
- How do acquirers articulate the requirements for secure code?
- What standards and best practices exist to communicate expectations?
- What are the critical success factors for developers developing secure code?
- How do acquires know their requirements for secure code have been met?
- How should acquirers communicate with other stakeholders?
- Next Steps?

SOFTWARE ASSURANCE FORUM

BUILDING SECURITY IN

SwA requires multi-disciplinary collaboration



Source: https://buildsecurityin.us-cert.gov/swa/procresrc.html

Communication Challenges

- Vocabulary
- Reserved Words
- Priorities
- Perspective

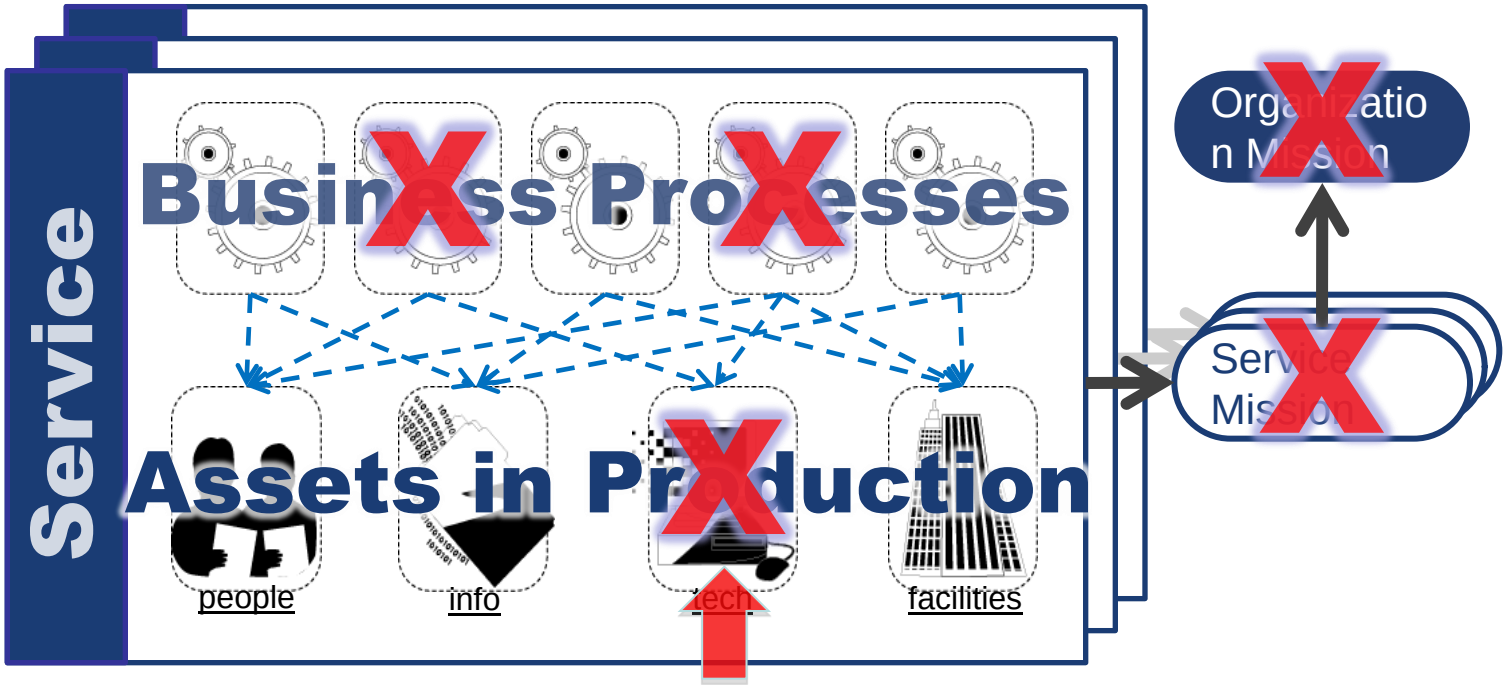
- **Experience**
- **Objectives**
- **Drivers**
- **Risks**

Without a common language we cannot communicate across disciplines

SOFTWARE ASSURANCE FORUM

BUILDING SECURITY IN

Business functions rely on accurate and reliable information from technology that functions as intended (and only as intended)



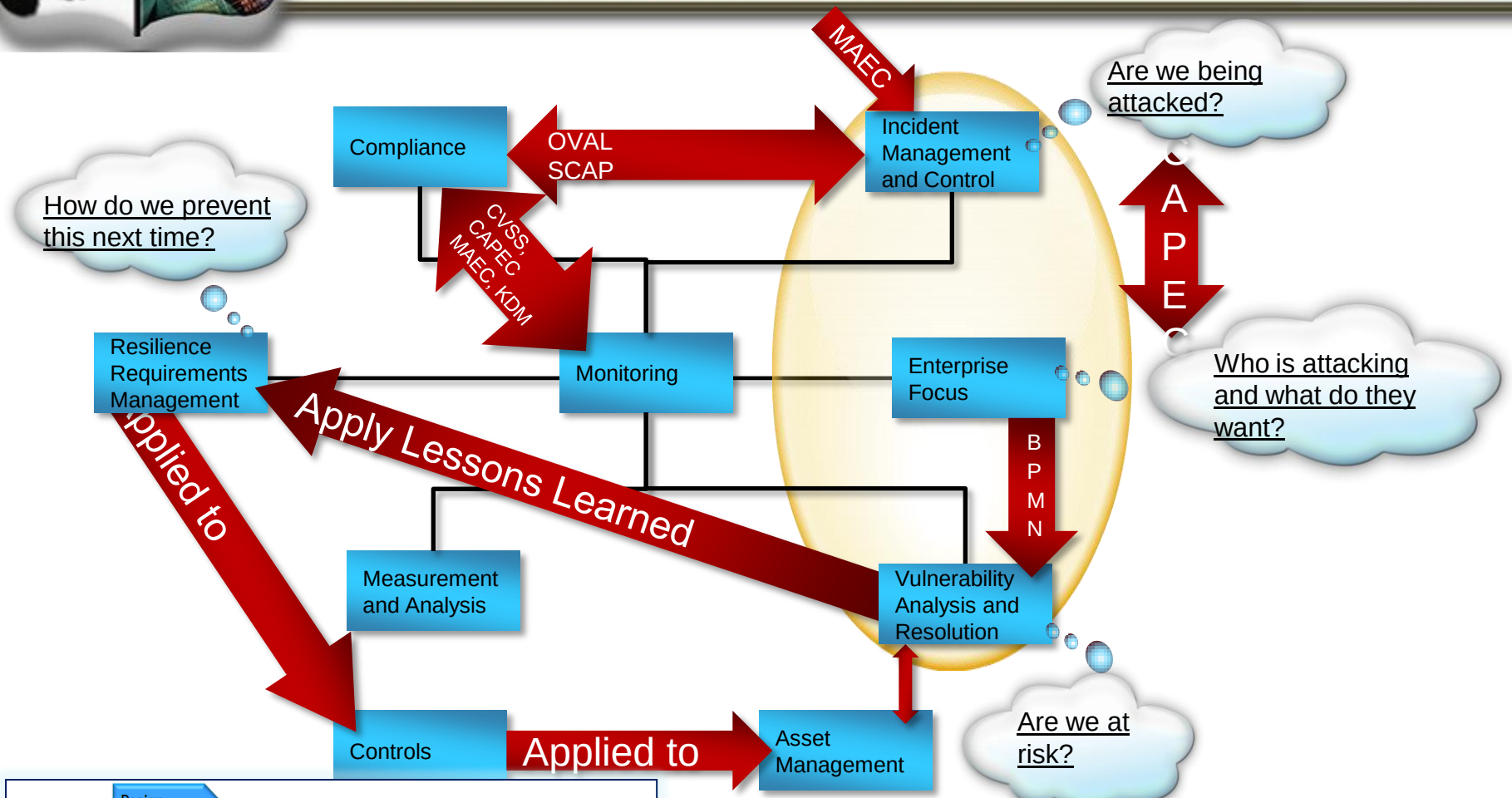
CERT | Software Engineering Institute | Carnegie Mellon.

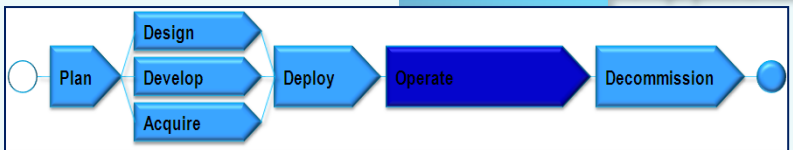
Adapted from: November 2009 SwA Forum-Evolution in SwA Processes Panel – David White, SEI

SOFTWARE ASSURANCE FORUM

BUILDING SECURITY IN

Operational impacts from threats to business functions can be understood by communicating software level vulnerabilities





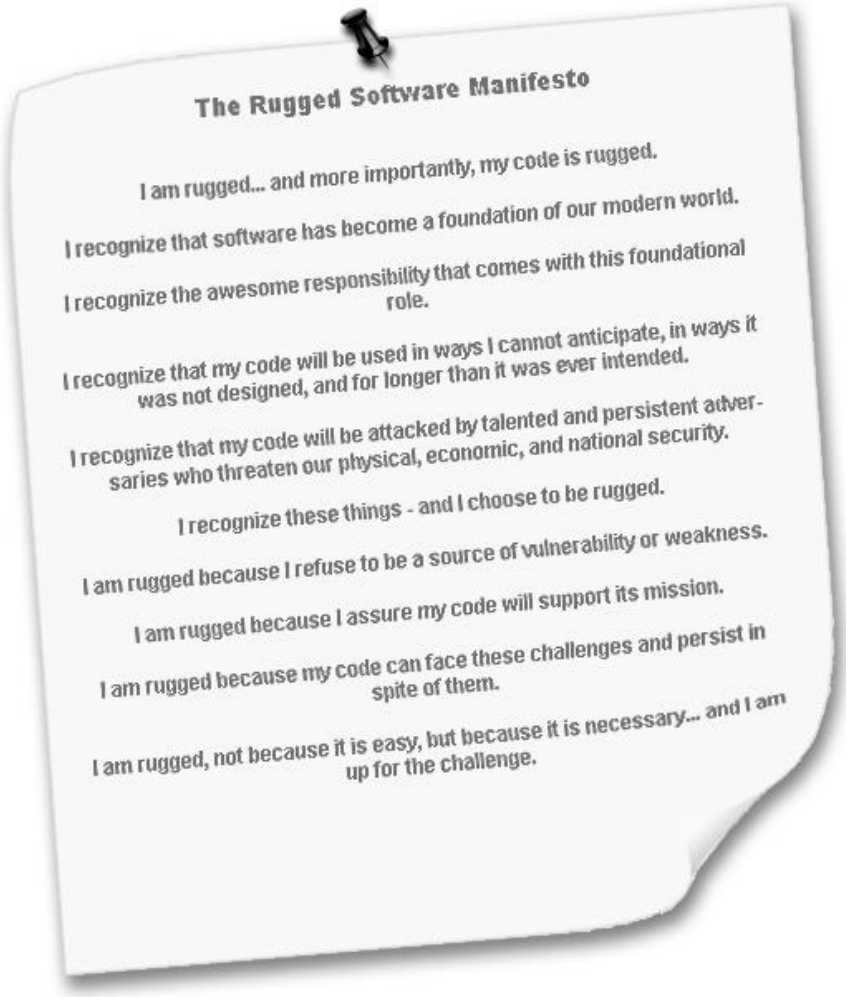
Adapted from September 2010 SwA Forum, CERT RMM for Assurance , Lisa Young, SEI

SOFTWARE ASSURANCE FORUM

BUILDING SECURITY IN

Today's environment requires an innovative way to look at the value and use of the software we develop and/or integrate

http://www.ruggedsoftware.org/



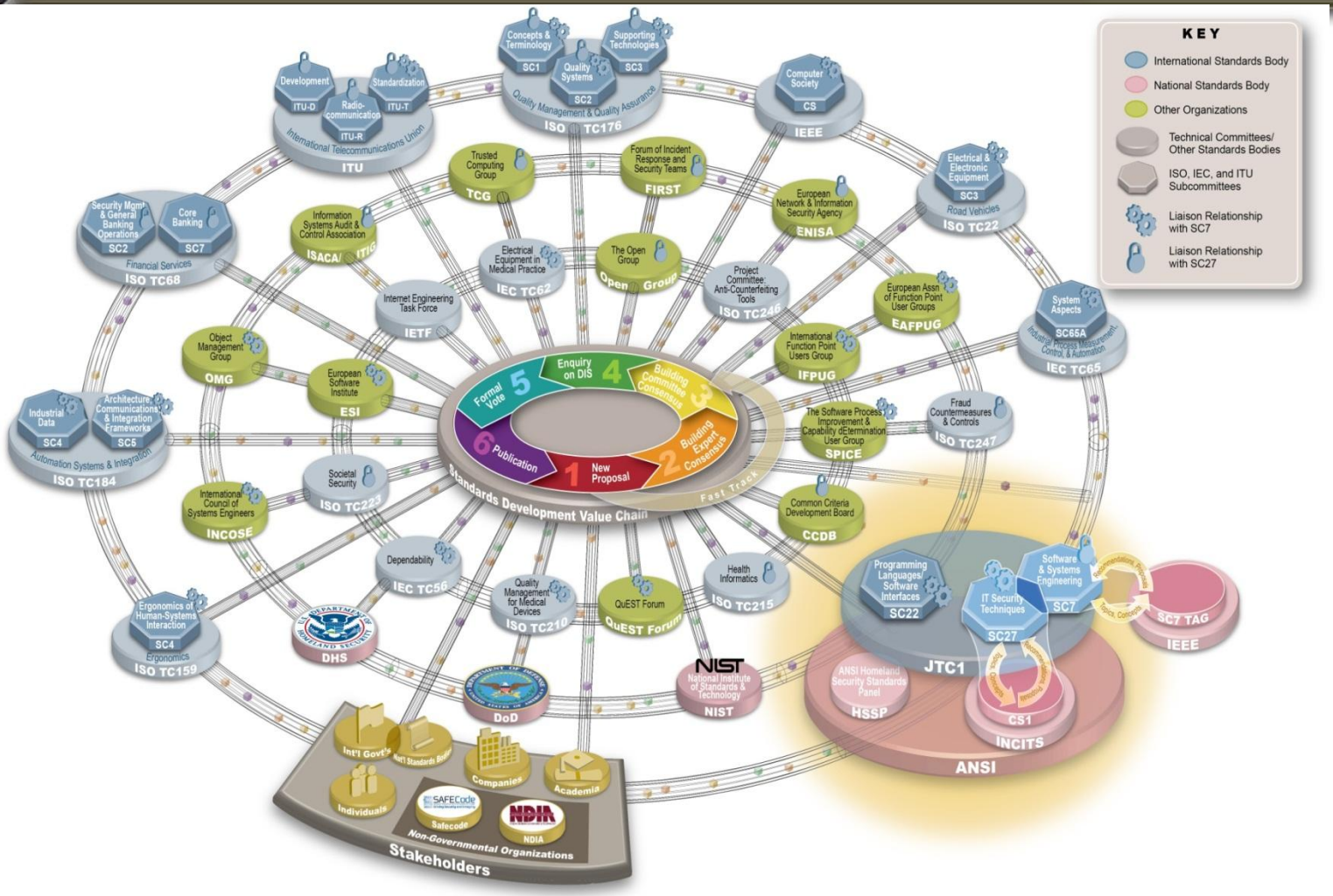
Key questions

- Do acquirers know why they need include requirements for secure code?
- How do acquirers articulate the requirements for secure code?
- What standards and best practices exist to communicate expectations?
- What are the critical success factors for developers developing secure code?
- How do acquires know their requirements for secure code have been met?
- How should acquirers communicate with other stakeholders?
- Next Steps?

SOFTWARE ASSURANCE FORUM

BUILDING SECURITY IN

Cyber security and software assurance standard development organization landscape



SC22 – Programming Languages, ISO/IEC TR 24772, Programming Language Vulnerabilities

- Targets building software that is inherently less vulnerable through improving the programming languages, or, at least, improve the usage of them in coding
- A catalog of 60+ issues that arise in coding when using any language and how those issues may lead to security and safety vulnerabilities
- Cross-referenced to CWE
- Each discussion includes
  - Description of the mechanism of failure
  - Recommendations for programmers: How to avoid or mitigate the problem.
  - Recommendations for standardizers: How to improve programming language specifications.

Courtesy of Jim Moore, MITRE

ISO/IEC 27036: Information technology – Security techniques – Information Security for Supplier Relationships

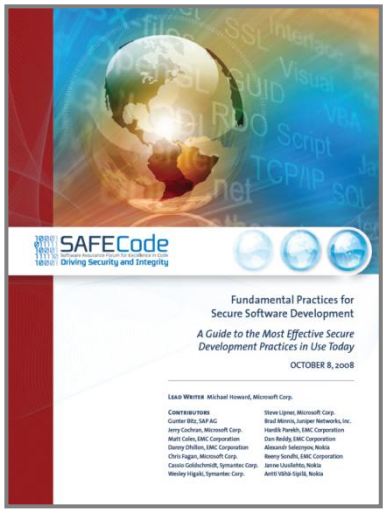
- Scope: This international standard covers information security in relationships between acquirers and suppliers to provide appropriate information security management for all parties. In particular, it also includes management of information security risks related to these relationships.
- The standard will be subdivided into the following parts:
  - Part 1 – Overview and Concepts
  - Part 2 – Common Requirements
  - Part 3 – Guidelines for ICT Supply Chain
  - Part 4 – Guidelines for Outsourcing

NIST IR 7622, Piloting Supply Chain Risk Management for Federal Information Systems

- Initially based on DoD ICT SCRM Key Practices document and developed in close collaboration with the industry
- Introduces the notion of supply chain players
  - Acquirer - For this document, the acquirer is always a government agency (including those agencies taking on the role of integrator).
  - Integrator – A third-party organization that specializes in combining products/elements of several suppliers to produce elements (information systems).
  - Supplier – Third-party organization providing individual elements. *Synonymous with vendor and manufacturer; also applies to maintenance/disposal service providers*
- Lays out pre-requisites of being able to address ICT SCRM challenge
- States specific practices that are consistent with DoD guidance and ISO frameworks

SAFECode (www.safecode.org)

- SAFECode is a global, industry-led effort to identify and promote best practices for developing and delivering more secure and reliable software, hardware and services
- White papers
  - Software Assurance: An Overview of Current Industry Best Practices
  - Fundamental Practices for Secure Software Development
  - Security Engineering Training: A Framework for Corporate Training Programs on the Principles of Secure Software Development
  - Framework for Software Supply Chain Integrity
  - Software Integrity Controls: An Assurance-Based Approach to Minimizing Risks in the Software Supply Chain



SOFTWARE ASSURANCE FORUM

BUILDING SECURITY IN

The Open Group Trusted Technology Provider Framework

Purpose

Identify and gain consensus on common processes, techniques, methods, product and system testing procedures, and language to describe and guide product development and supply chain management practices that can mitigate vulnerabilities which could lead to exploitation and malicious threats to product integrity.

Objectives

- Identify product assurance practices that should be expected from all commercial technology vendors based on the baseline best practices of leading trusted commercial technology suppliers
- Help establish expectations for global government and commercial customers when seeking to identify a trusted technology supplier
- Leverage existing globally recognized information assurance practices and standards
- Share with commercial technology consumers secure manufacturing and trustworthy technology supplier best practices
- Harmonize language used to describe best practices

Source: Source: September 28, 2010 SwA Forum, DoD Trusted Defense Systems, Ms. Kristen Baldwin, DDR&E/Systems Engineering

What's next?

- Continued collaboration to:
  - Reach and enable developers
  - Reach and enable executives
  - Develop and promote resources for us by developers and executives
- Participation in international standardization efforts
  - SC7 TAG intersections through your SC7 TAG
  - CS1/SC27
  - IEEE representative to the SC7 TAG
  - SC22
- Participation through the SwA Working Groups and Forum
- Stay Tuned …

SOFTWARE ASSURANCE FORUM

BUILDING SECURITY IN

Contact information

Mr. Donald Davidson,
Chief, Outreach, Science & Standards
Trusted Mission Systems & Networks
TMSN / DoD CIO
Don.Davidson@osd.mil

Michele Moss
Lead Associate
Booz Allen Hamilton
moss_michele@bah.com