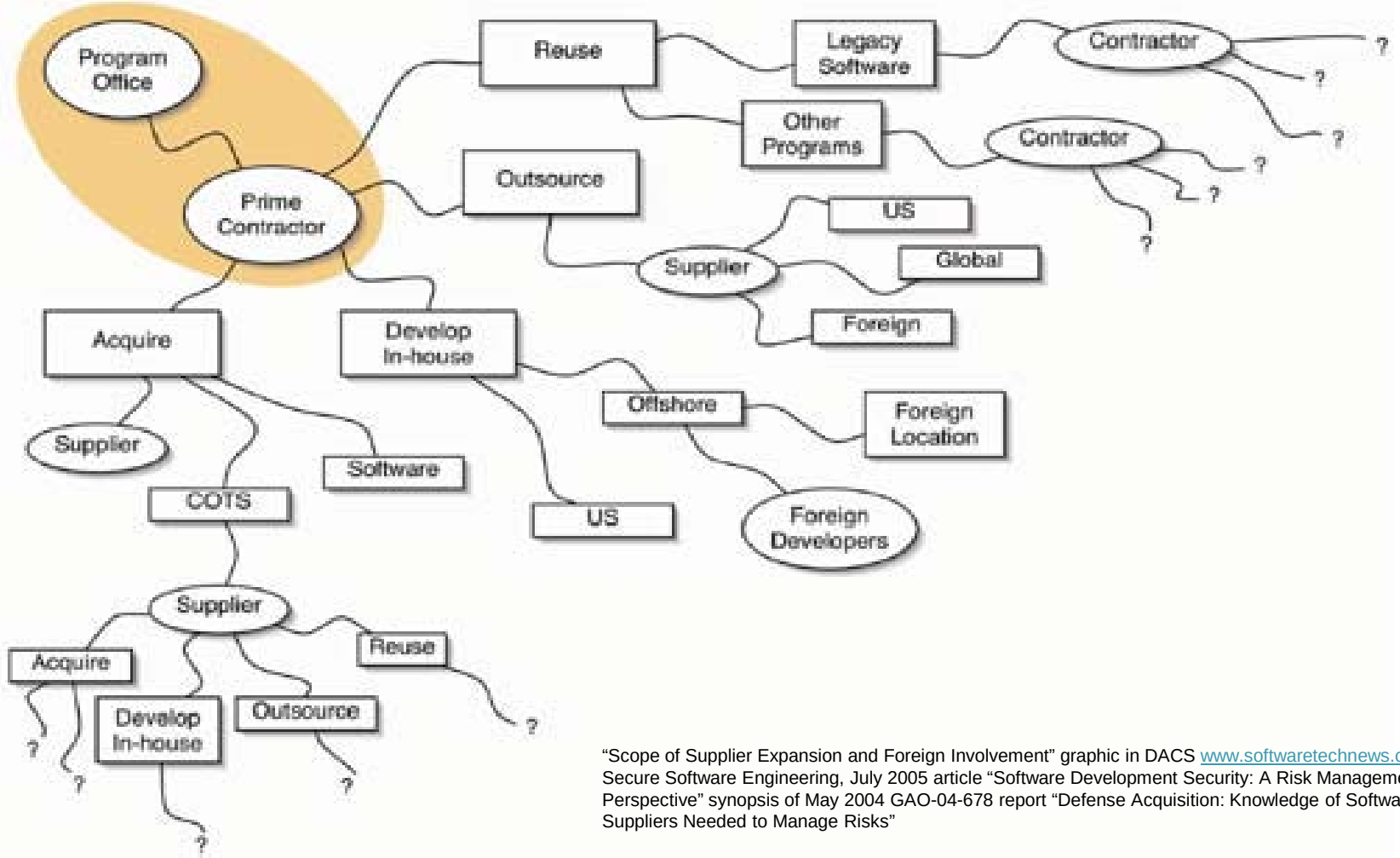
Systems Assurance, The Global Supply Chain, and Efforts To Increase Communication Between Acquisition and Development

Michele Moss
NDIA CMMI Technology Conference
November 17, 2010

Table Of Contents

- Globalization Challenges
- Understanding The Problem
- Working Towards A Solution

Globalization brings challenges



"Scope of Supplier Expansion and Foreign Involvement" graphic in DACS www.softwaretechnews.com Secure Software Engineering, July 2005 article "Software Development Security: A Risk Management Perspective" synopsis of May 2004 GAO-04-678 report "Defense Acquisition: Knowledge of Software Suppliers Needed to Manage Risks"

Technology Is A Focal Point Of Attacks

Who is behind data breaches?	**74%** resulted from external sources (+1%). **20%** were caused by insiders (+2%). **32%** implicated business partners (-7%). **39%** involved multiple parties (+9%).
How do breaches occur?	**7%** were aided by significant errors (<>). **64%** resulted from hacking (+5%). **38%** utilized malware (+7%. **22%** involved privilege misuse (+7%). **9%** occurred via physical attacks (+7%).

** Source – 2009 Verizon Data Breach Investigations Report*

According to an article in the May 2010 National Defense Magazine, well funded nation states and terrorist organizations are engaging in cyber attacks against US government systems. Examples of those include 44,000 Turkish teenagers in a military style community of hackers learning from each other.

There are also 100,000 hackers learning from each other in Saudi Arabia, 40,000 in Iraq, and over 400,000 in China.

32%

3

Increased Priority for Program Protection

- *Threats*: Nation-state, terrorist, criminal, rogue developer who:
  - Gain control of systems through supply chain opportunities
  - Exploit vulnerabilities remotely
- *Vulnerabilities*: All systems, networks, applications
  - Intentionally implanted logic (e.g., back doors, logic bombs, spyware)
  - Unintentional vulnerabilities maliciously exploited (e.g., poor quality or fragile code)
- *Consequences*: Stolen critical data & technology; corruption, denial of critical warfighting functionality

Today's acquisition environment drives the increased emphasis:

Then		Now
Standalone systems	>>>	Networked systems
Some software functions	>>>	Software-intensive
Known supply base	>>>	Prime Integrator, hundreds of suppliers

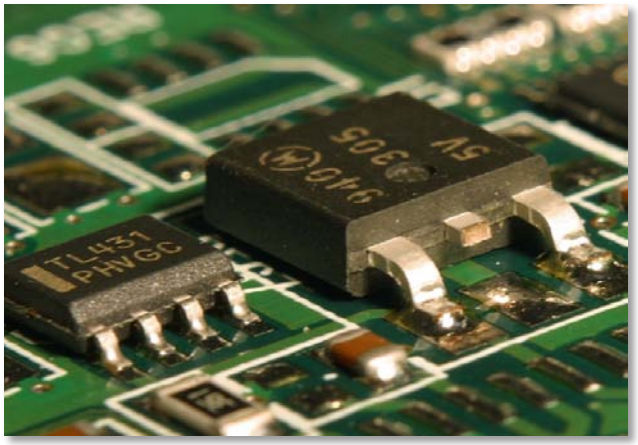
Source: Source: September 28, 2010 SwA Forum, DoD Trusted Defense Systems, Ms. Kristen Baldwin, DDR&E/Systems Engineering

“U.S. charges Florida pair with selling counterfeit computer chips from China to the U.S. Navy and military”

INCIDENT:
On September 14, 2010 Federal prosecutors in Washington unsealed charges accusing a Florida pair of selling more than 59,000 counterfeit computer microchips from China to the U.S. Navy and other clients for military use aboard American warships, fighter planes, missile and antimissile systems. Wren, owner of VisionTech Components and related companies, and McCloskey, an administrator, were charged with conspiracy, trafficking in counterfeit goods and mail fraud.

IMPACT:
The case marked the latest effort by U.S. authorities to stem the flow of fake electronics into the U.S. military supply chain, as warnings mount that fake chips could be defective or "electronic Trojan horses" that would allow hackers to disable them or track their use. Several recent government reports warn that computer chips marked with false brands or mislabeled as military-grade may include imperfections that could cripple or degrade weapons systems in combat or over time.

MITIGATION:
In January the Commerce Department reported that the number of counterfeit incidents discovered by the military and its suppliers more than doubled between 2005 to 2008, to more than 9,356 cases. Meanwhile, lawmakers and congressional investigators have called on the Pentagon and law-enforcement agencies to combat the problem more aggressively.



Courtesy of Don Davidson, OSD TMSN ,Chief of Outreach and Standardization

http://www.washingtonpost.com/wp-dyn/content/article/2010/09/14/AR2010091406468.html

"Recalled BlackBerry Batteries- *Yet another wake-up call on counterfeit parts and product recall mitigation*"

INCIDENT:
On August 10, 2010 the U.S Consumer Product Safety Commission announced that about 470,000 BlackBerry batteries distributed by Asurion were being recalled due to an overheating and safety problem. According to the recall notice, the batteries in question were counterfeit, and "*these batteries were used across virtually all modes of refurbished BlackBerry devices distributed by Asurion prior to November 1, 2009.*"

IMPACT:
The counterfeit batteries can overheat, posing burn and fire hazards. Asurion has received two reports of counterfeit BlackBerry®-branded batteries overheating, causing minor burns to a consumer's finger and minor property damage to a sofa and car seat.

MITIGATION:
Consumers who received refurbished BlackBerry devices through Asurion prior to November 1, 2009 were advised to immediately stop using the product and contact Asurion for a replacement product. Asurion is directly contacting known consumers with the affected batteries to notify them of this recall.

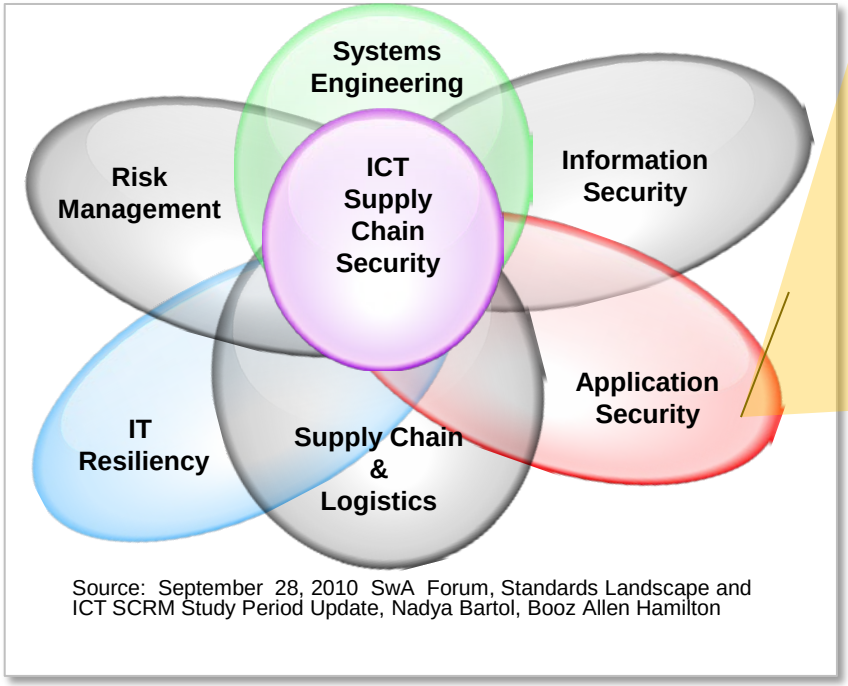
http://www.theferrarigroup.com/blog1/2010/08/11/recalled-blackberry-batteries-yet-another-wake-up-call-on-counterfeit-parts/

Courtesy of Don Davidson, OSD TMSN ,Chief of Outreach and Standardization

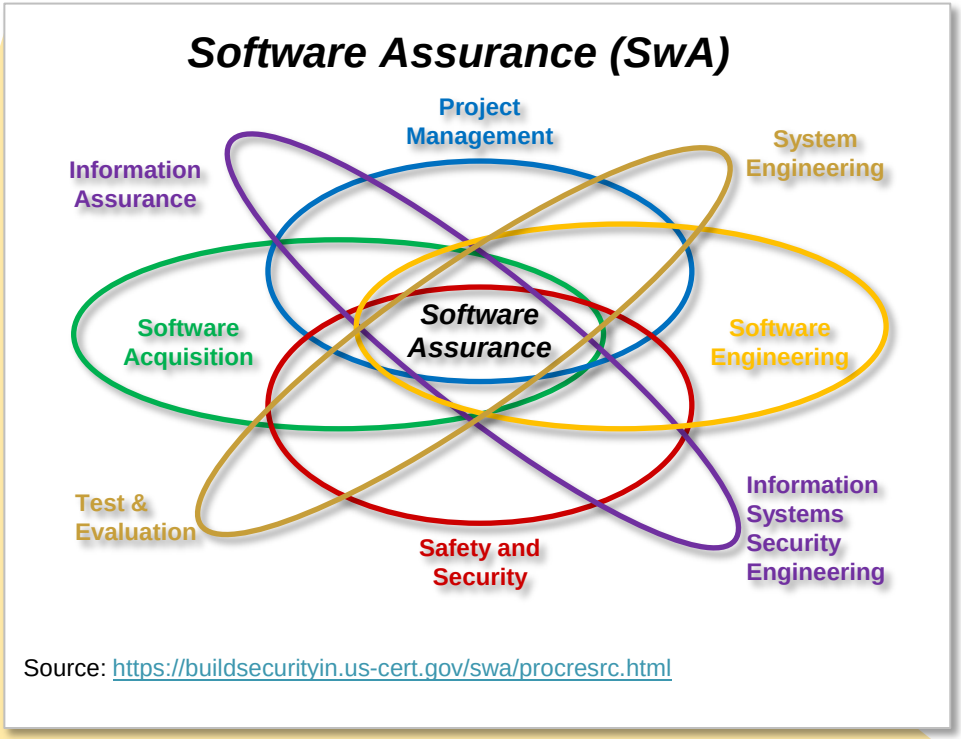
Table Of Contents

- Globalization Challenges
- Understanding The Problem
- Working Towards A Solution

ICT SCRM And SwA Are Complex *Multi-Disciplinary* Challenges

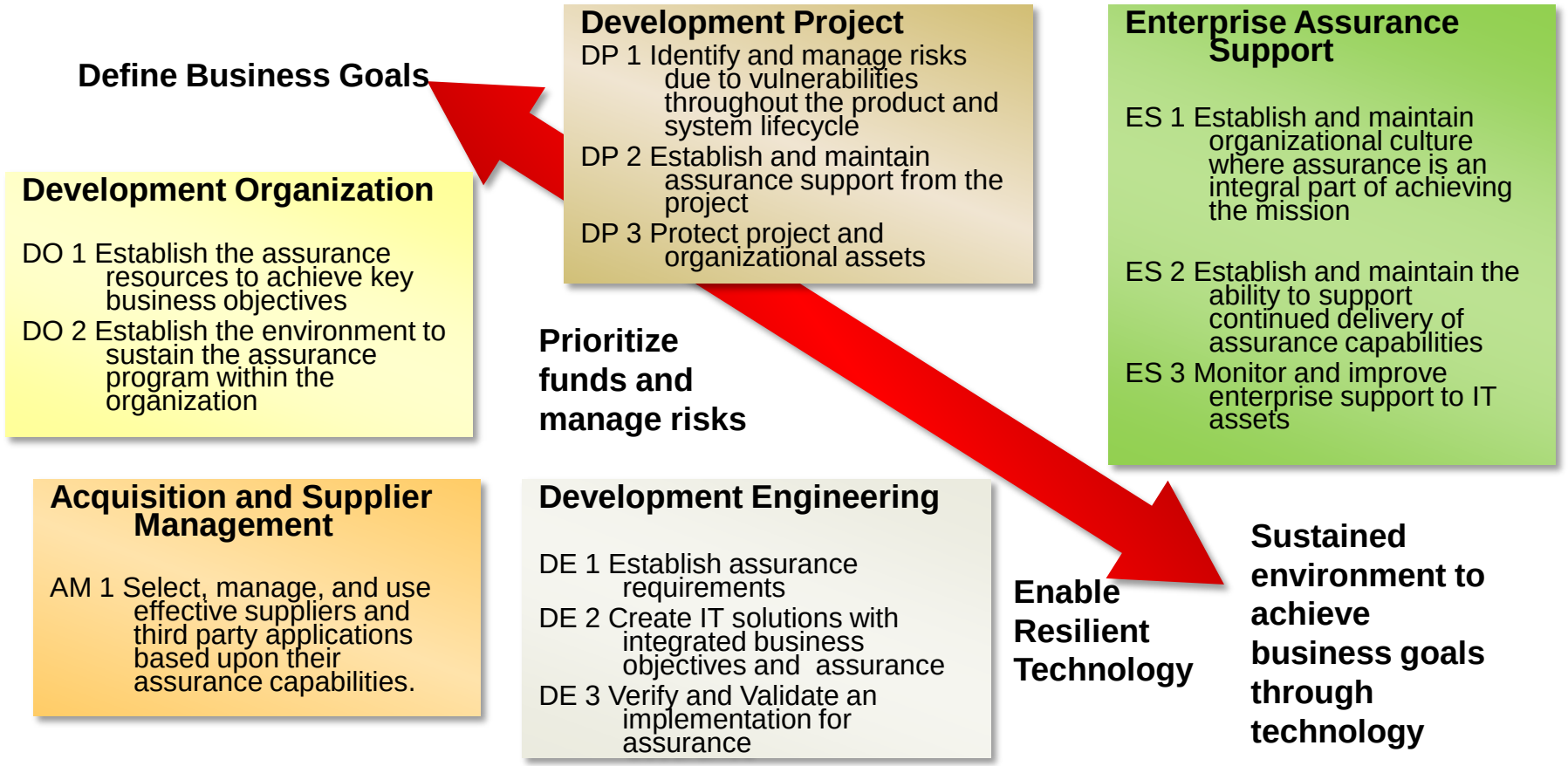


Source: September 28, 2010 SwA Forum, Standards Landscape and ICT SCRM Study Period Update, Nadya Bartol, Booz Allen Hamilton



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

Communication Across Organizational Stakeholders Is Critical to addressing ICT SCRM and SwA Challenges



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

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

A Resilient Technology Best Practices Cross Walk

You have been asked to ensure that the OWASP Top Ten (an assurance coding Standard) are not in the Code

You can look at the OSAMM for guidance on how to do it

SwA Community's Assurance Process Reference Model - Initial Mappings

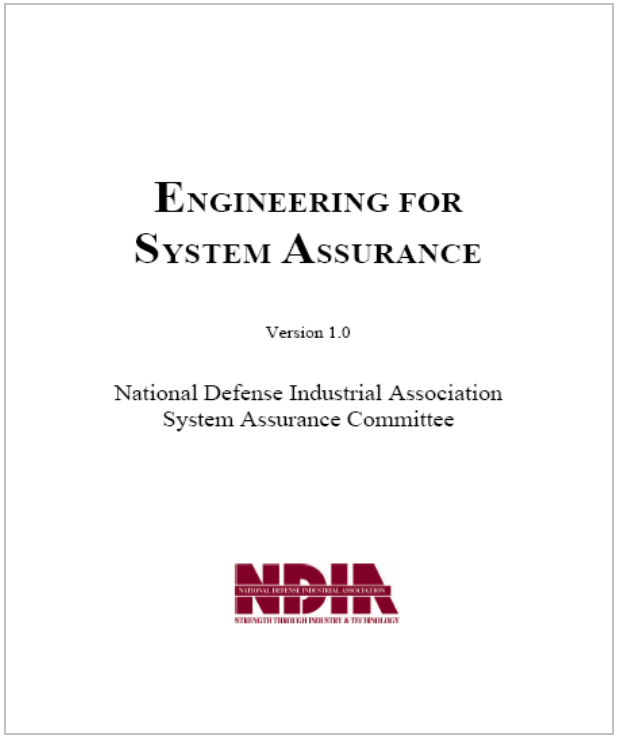
In the following table, all references to "assurance" are intended to include system and software assurance, information assurance, and cybersecurity in support of the business/mission functions supported by systems and software.

Goal	Practice	AF CMMI	BSIMM	CMMI-ACQ	CMMI-DEV	CMMI-SVC	OSAMM	RMM
DE 2 Create IT solutions with integrated business objectives and assurance	Develop alternative solutions and selection criteria for mission and information assurance.	AF TS SP 1.1.1	SFD1.1	ATM SG2	TS SG1		SA1A	RTSE:SG 1 - SG2
			SFD1.2	AVAL SG2			SA1B	KIM:SG2, SG6
	Architect for mission and information assurance.	AF TS SP 2.1.1	SFD2.1	ATM SG2	TS SG2		SA2A	RTSE:SG 3
			SFD2.3	AVAL SG2	TS SG2		SA2B	
	Design for mission and information assurance.	AF TS SP 2.1.2	SFD2.1		TS SG2			
	Implement the mission and information assurance designs of the product components.	AF TS SP 3.1.1	AA3.2		TS SG3		SA1B	
	Identify deviations from mission and information assurance coding standards. Implement appropriate mitigation to meet defined mission and information assurance objectives.	AF TS SP 3.1.2	CR1.4	AVER SG3	TS SG3		CR2A	RTSE:SG 2
			CR2.3				CR2B	RTSE:SG 3
			CR3.1				CR3A	

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

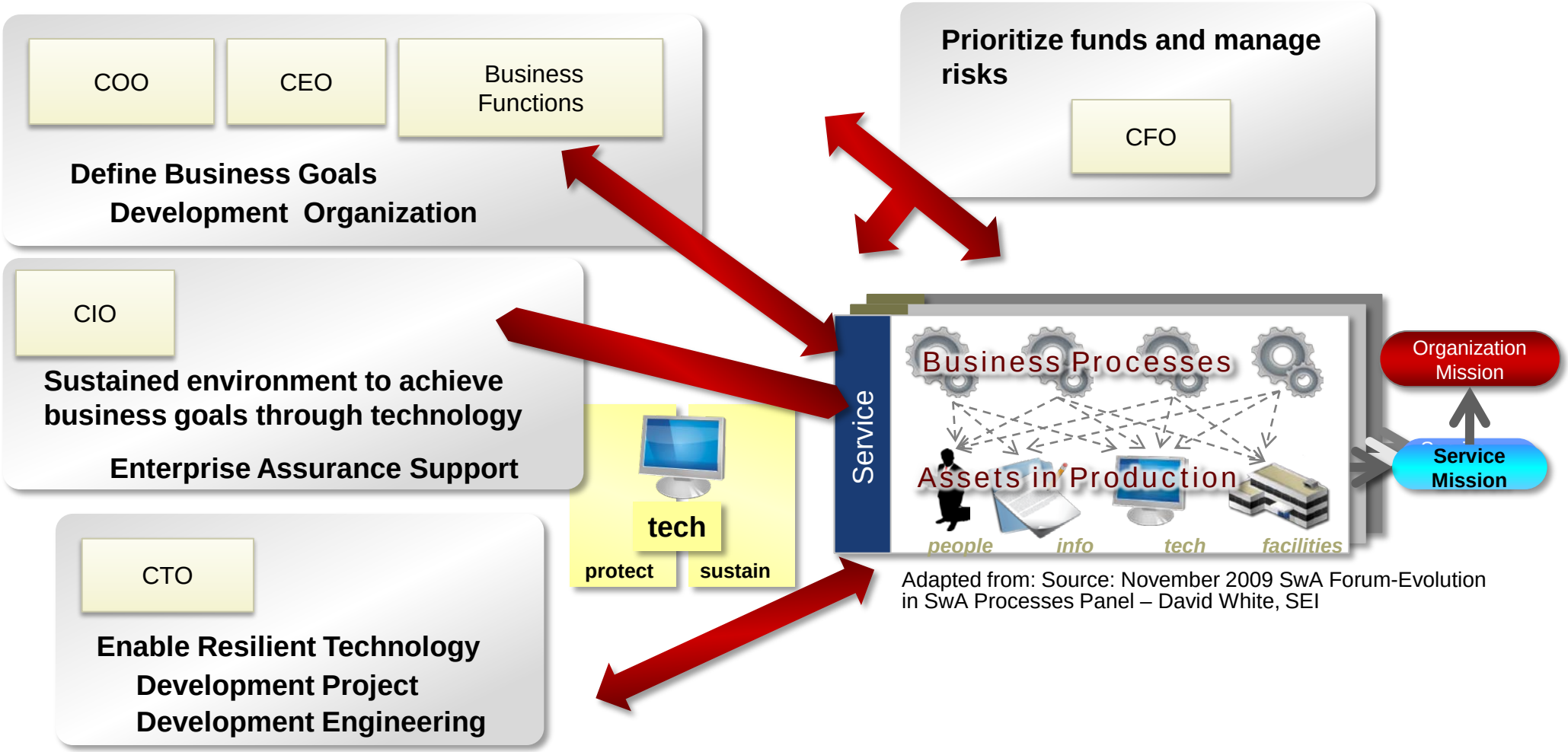
Mapping to the Engineering for System Assurance, v1.0 is in progress

- NDIA/DoD guidebook providing process and technology guidance to increase the level of system assurance.
- Intended primarily to aid program managers (PMs) and systems engineers (SEs) who are seeking guidance on how to incorporate assurance measures into their system life cycles.



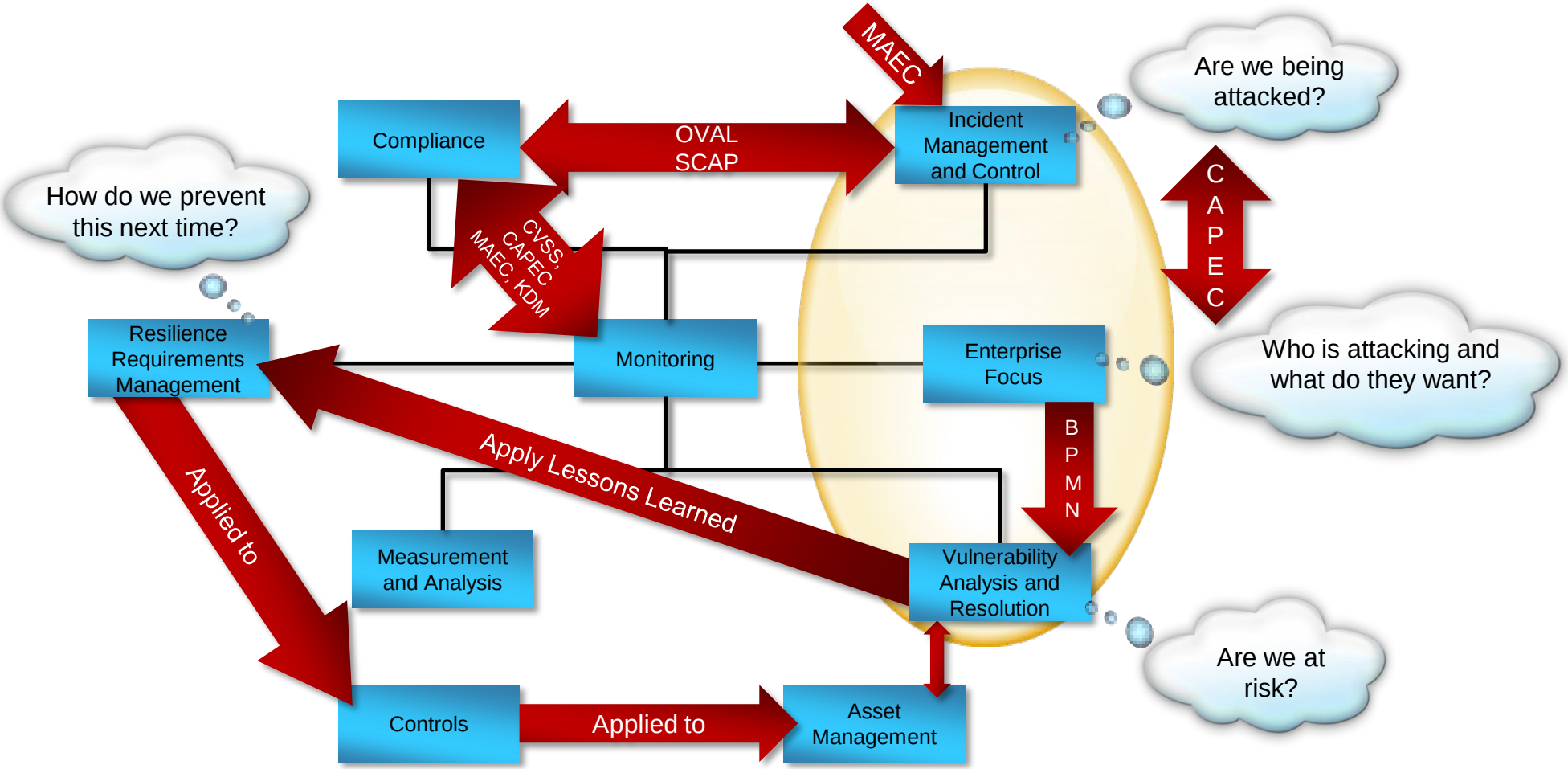
http://www.acq.osd.mil/sse/ssa/docs/SA-Guidebook-v1-Oct2008.pdf

Enterprise Leadership and Resilient Technology



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

SwA, SCRM, And Continuous Improvement Contribute To Operational Resilience



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

ICT Supply Chain Assurance:
An IATAC State-of-the-Art Report

The following link is available to personnel accessing from within a .mil or .gov domain:

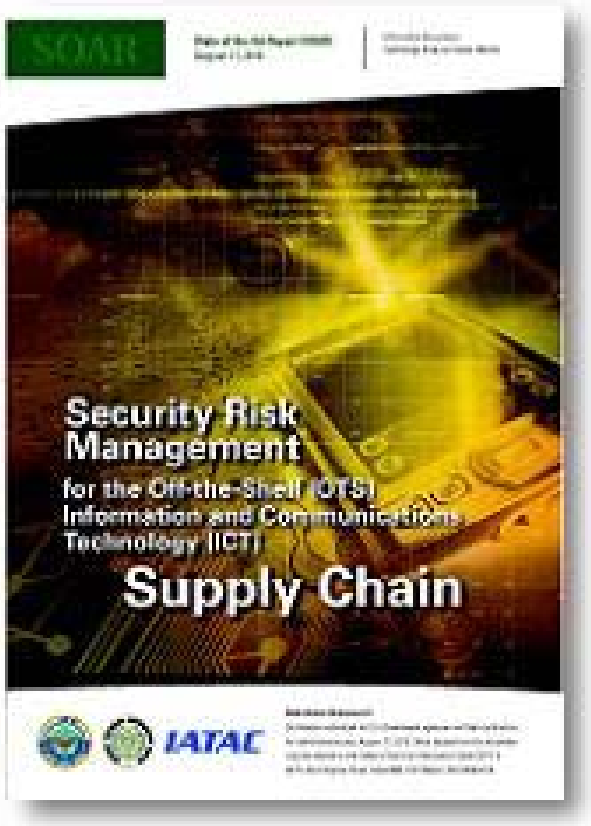
URL: http://iac.dtic.mil/iatac/pdf/supply_chain.pdf

You may also contact IATAC directly to obtain access to this report. The easiest way for you and the IATAC team to get you the report is for you to

Information Assurance Technology Analysis Center (IATAC)

Email: iatac@dtic.mil

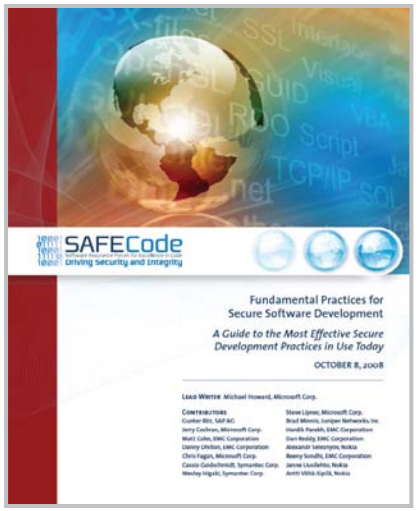
URL: http://iac.dtic.mil/iatac/



SAFECode (www.safecode.org)

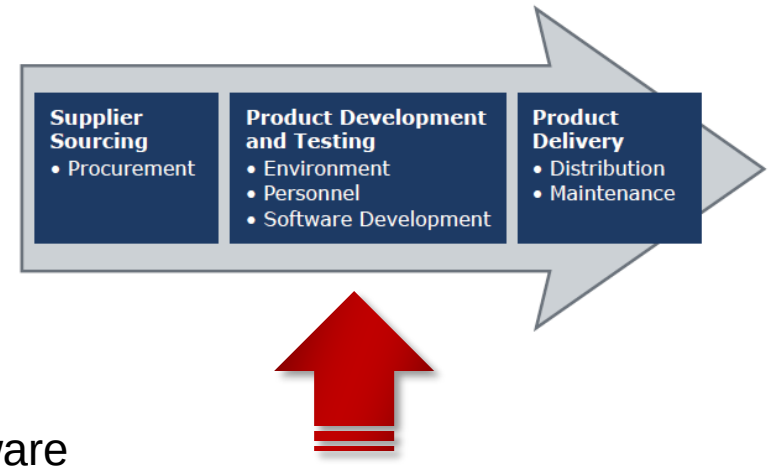
- SAFECode is a global, industry-led effort to identify and promote best practices for developing and delivering more secure and reliable software, hardware and services

- 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



Describing the Software Supply Chain

- Sophisticated IT solutions are composed of a collection of components
- Each component or its parts can be:
  - Developed by its supplier or on that supplier's behalf by their subcontractors; or
  - Licensed to the supplier by another vendor or obtained from Open Source repositories; or
  - Acquired outright by the supplier



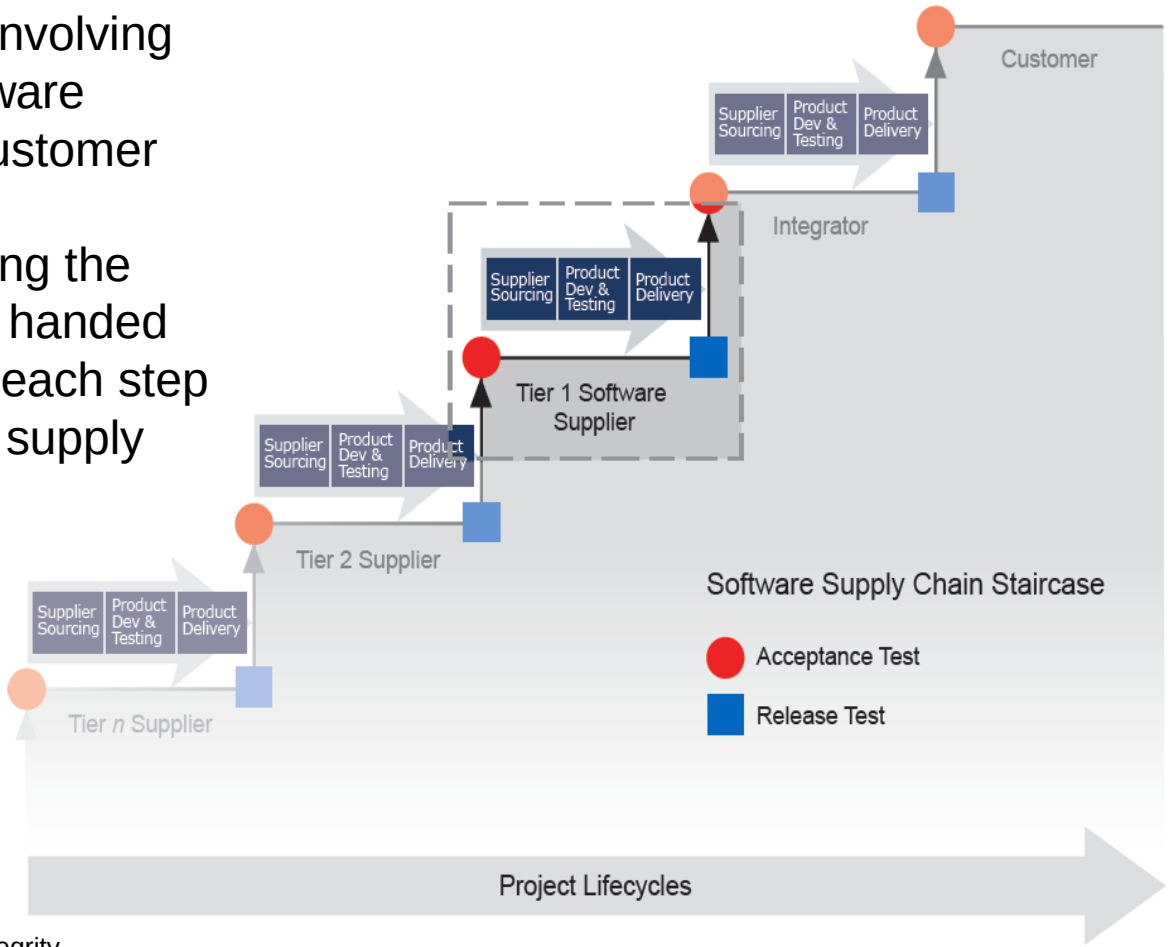
- Regardless of the development scenario, each software supplier in the supply chain must manage three sets of controls:
  - 1. Supplier Sourcing — Select the suppliers, establish the specification for the supplier's deliverables, and receive software/hardware deliverables from the suppliers;
  - 2. Product Development and Testing — Build, assemble, integrate and test components and finalize for delivery; and,
  - 3. Product Delivery — Deliver and maintain their product components to their customer.

Source – SAFECode: Framework for Software Supply Chain Integrity

Software Supply Chain Staircase

- Figuratively, an IT solution supply chain can resemble a collection of staircases involving the successive transmission of software components from a supplier to its customer

- In this figure, components move along the “staircase” supply chain as they are handed off from one supplier to the next. At each step a supplier controls three links in the supply chain:
  1. Goods received from suppliers;
  2. Their product production; and
  3. What is delivered to their customers



Source – SAFECode: Framework for Software Supply Chain Integrity

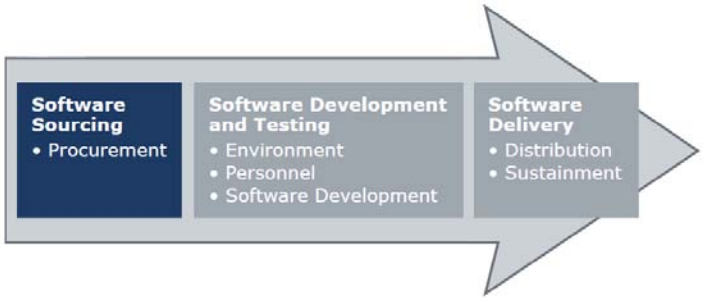
Fundamental Software Supply Chain Integrity Controls

- Software supply chain integrity controls address the access, storage and handling of development assets throughout the supply chain – supplier sourcing, product development and testing, and product delivery.
- Some fundamental software supply chain integrity controls, derived from established security and integrity principles, include:

Control Title	Description
Chain of Custody	The confidence that each change and handoff made during the source code's lifetime is authorized, transparent and verifiable
Least Privilege Access	Personnel can access critical data with only the privileges needed to do their jobs.
Separation of Duties	Personnel cannot unilaterally change data, nor unilaterally control the development process
Tamper Resistance and Evidence	Attempts to tamper are obstructed, and when they occur they are evident and reversible.
Persistent Protection	Critical data is protected in ways that remain effective even if removed from the development location.
Compliance Management	The success of the protections can be continually and independently confirmed
Code Testing and Verification	Methods for code inspection are applied and suspicious code is detected.

Source – SAFECode: Framework for Software Supply Chain Integrity

Software Sourcing Controls: Contractual

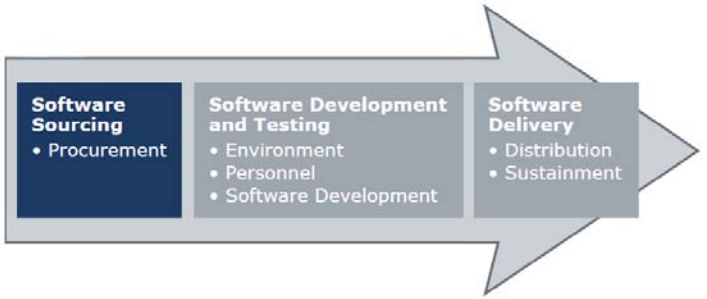


- A vendor's engagement with a supplier is governed by a written agreement, for example a license or a contract
- The written agreement must explicitly state the vendors an supplier's expectations, as well as the consequences of any non-compliance with the terms of the agreement

– Software sourcing controls:
  – Defined Expectations — Clear language regarding the requirements to be met by the code and the development environment should be set forth
  – Ownership and Responsibilities — IC and responsibilities for protecting the code and development environment must be articulated
  – Vulnerability Response — How well is the supplier equipped to collect input on vulnerabilities from reputable sources and appropriate remedies
  – Security Training — How well is the partner able to effectively train its developers on security development practices
  – Open Source Software — The use of OSS presents alternative challenges in the context of supply chain integrity

Source - SAFECode: Software Integrity Controls: An Assurance-Based Approach to Minimizing Risks in the Software Supply Chain

Software Sourcing Controls: Technical

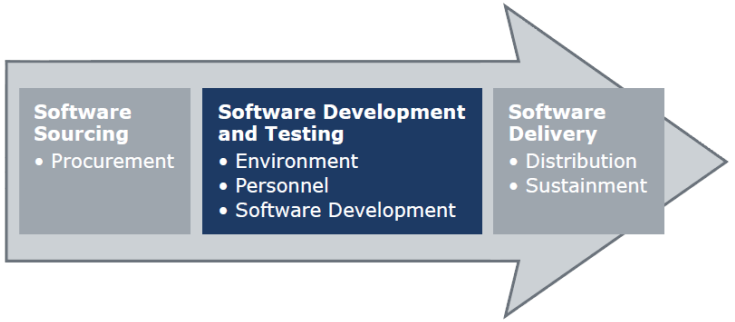


- Secure Transfer — Delivered code should be transferred securely, using authenticated endpoints and encrypted sessions
- Sharing of System and Network Resources — The digital identities a vendor issues to suppliers to enable access to the vendor's network and resources should be established with strong controls enforced to limit access to only those resources needed to perform the supplier's role
- Malware Scanning — Supplier content to be transmitted to the vendor should be scanned for malware using the most recent malware signature files and more than on commercial scanning engine
- Secure Storage — Source code should be stored securely with need-to-know access controls applied
- Code Exchange — Processes using digitally signed packages and verifiable checksums or hashes should be in place to ensure that received code is complete and authentic

Source - SAFECode: Software Integrity Controls: An Assurance-Based Approach to Minimizing Risks in the Software Supply Chain

Software Development and Testing Controls: Technical

- People Security — Ensure that adequate background checks are performed, that roles and responsibilities and access rights are clearly defined, and that segregation of duties and controlled automated processes are applied.

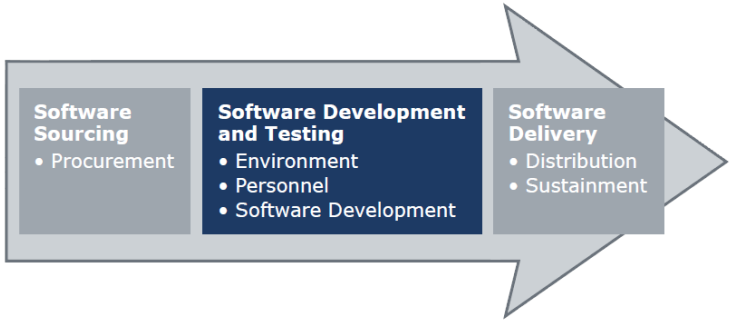


- Physical security — Building security and physical access control should be applied to development locations and code repositories and periodically re-assessed using a risk-based process
- Network Security — Network security standards should be established and applied using a risk-based process for code-related assets
- Code Repository Security — All code-related assets should be housed in source code repositories to enable additional attention to security and access control
- Build Environment Security — Build environments should be as automated as much possible to minimize the opportunity for human intervention in the regular build process

Source - SAFECode: Software Integrity Controls: An Assurance-Based Approach to Minimizing Risks in the Software Supply Chain

Software Development and Testing Controls: Security Testing

- Peer Review \ Manual Inspection —
  - Are not often popular given issues of scalability, but automated tools can enable some scalability by collecting and processing more artifacts in preparation for peers performing a focused review
  - Also, when teams are assigned to work together on code files, an important dynamic is present whereby reviewers can more readily identify code that does not belong within a code set

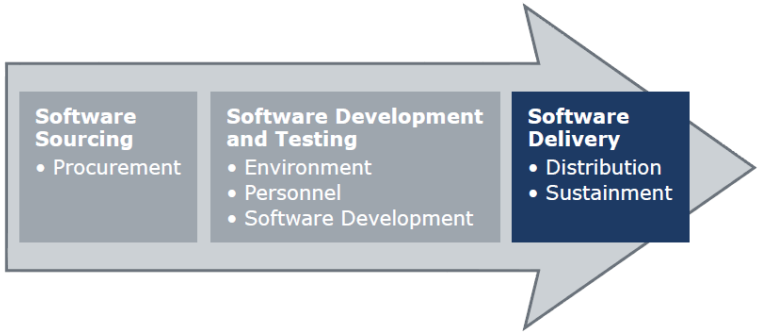


- Testing for Secure Code —
  - The size of the code base for many software projects today requires automated code review and testing tools
  - Building these tests to run in a repeatable automated manner increases the assurance that they will be performed and analyzed often
  - These tools include: static code analysis tools, vulnerability scanners, binary code analysis tools, malware detection tools, security compliance validation tools, and code coverage tools

Source - SAFECode: Software Integrity Controls: An Assurance-Based Approach to Minimizing Risks in the Software Supply Chain

Software Delivery Controls: Publishing and Dissemination

- Covers new product delivery and the delivery of maintenance patches
- Not always last stage of the supply chain
- As software components leave the supplier, software integrity and authenticity become a shared responsibility between the supplier and customer.

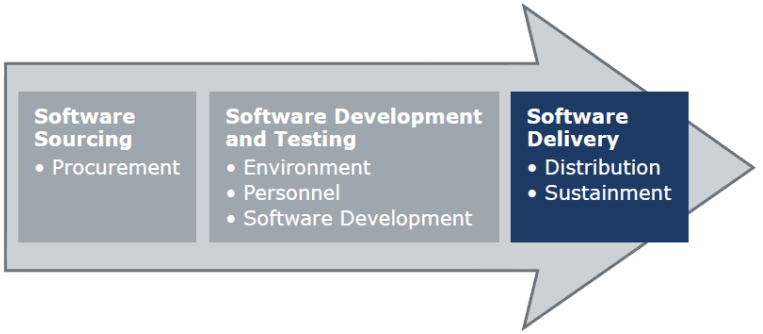


- Malware Scanning — Products should be scanned for malware using the most recent malware signature files and more than one commercial scanning engine
- Code Signing — The software vendor's product should be strongly digitally marked with the software vendor's identity in a way that can't be altered, yet may be verified by the customers
- Delivery — A vendor's process for delivering products both online and through distributions using physical and electronic media should be secured; information on code signing and checksums should be available to customers.
- Transfer — Vendors should transfer products in such a way that the receiver can confirm that the product is coming from the software vendor

Source - SAFECode: Software Integrity Controls: An Assurance-Based Approach to Minimizing Risks in the Software Supply Chain

Software Delivery Controls: Authenticity

- Over one in five software packages is counterfeit or pirated[1]
- Authenticity is a core element of software assurance
- The risk of counterfeit software can be greatly reduced through purchase from only authorized resellers, careful examination of product packaging and media, and technology to notify user when they may be the victim of counterfeit software



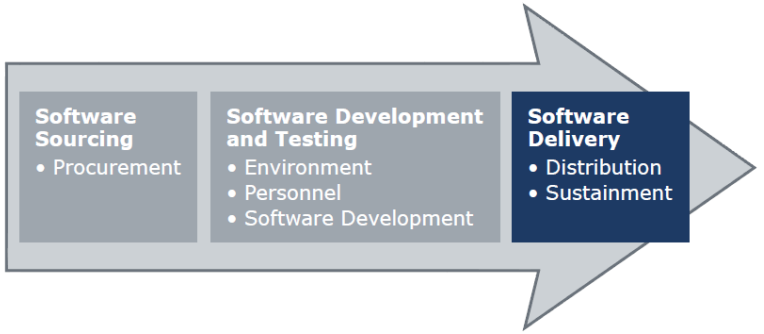
- Cryptographic Hashed or Digitally Signed Components — digitally signed components or checksum hashes are an essential authenticity control to prove that components are genuine
- Notification Technology — Vendors can leverage technology to detect certain aspects of the product's integrity and notify the user if the software is deemed to be counterfeit.
- Authentic Verification During Program Execution — the practice of verification when the application is installed on a computer; each time the application runs, the integrity of the files is verified

1 Business Software Alliance, Piracy Study, May 12, 2009

Source - SAFECode: Software Integrity Controls: An Assurance-Based Approach to Minimizing Risks in the Software Supply Chain

Software Delivery Controls: Deployment and Sustainment

- The software life cycle extends beyond delivery of the initial software vendor's product and into the product's sustainment or maintenance phase.
- As a result, patches and hot fixes should be subject to the same software integrity controls as the original code



- Only authorized service personnel with ongoing access to genuine parts and proper disposal procedures should be involved in the sustainment process
- Secure Configurations — Whenever possible, software vendors should ship products with a secure configuration being set as the default configuration
- Custom Code Extensions — Integrators must follow secure development practices as they extend code functionality through the provided secure interfaces

1 Business Software Alliance, Piracy Study, May 12, 2009

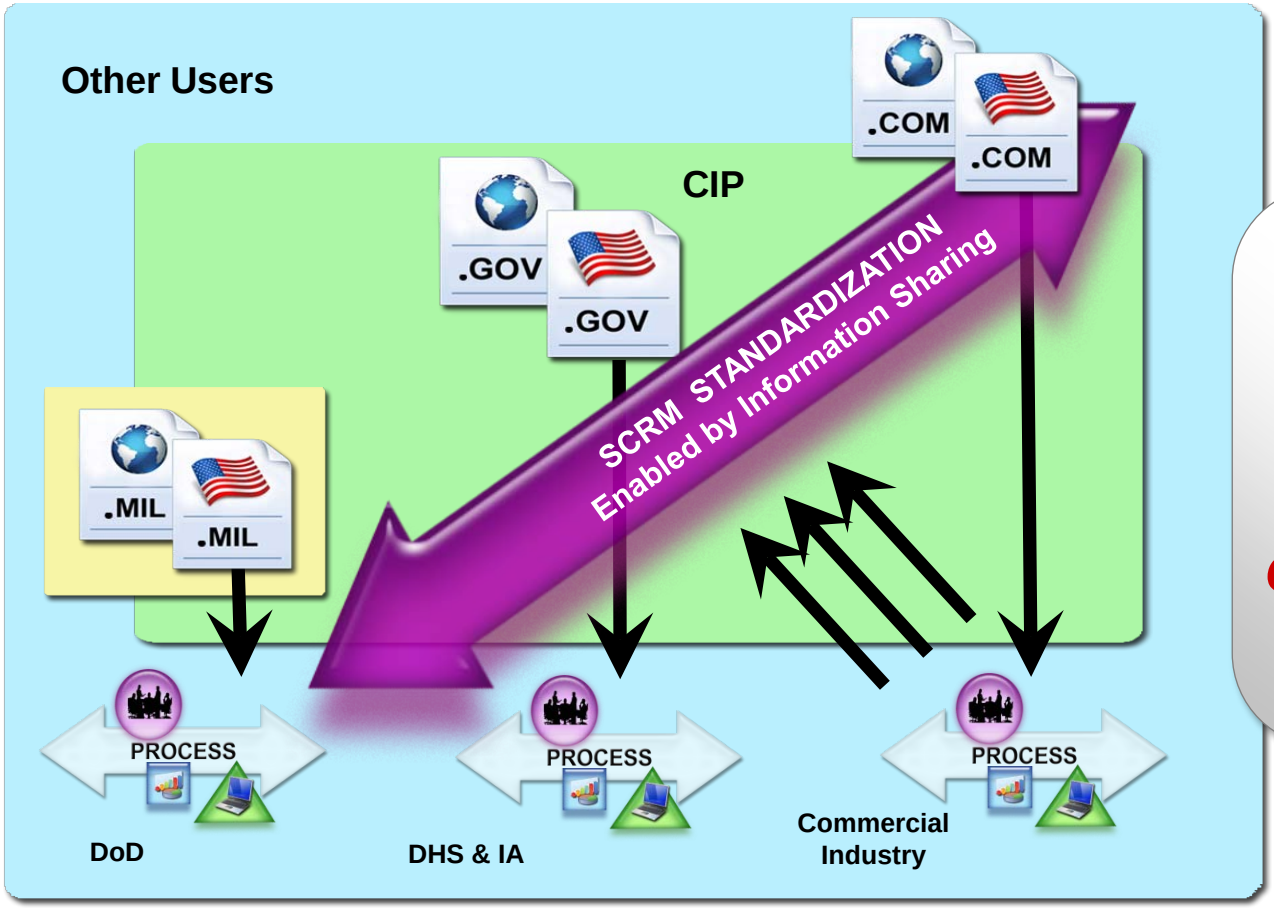
Source - SAFECode: Software Integrity Controls: An Assurance-Based Approach to Minimizing Risks in the Software Supply Chain

Table Of Contents

- Globalization Challenges
- Understanding The Problem
- Working Towards A Solution

SCRM Stakeholders

US (CNCI) has vital interest in the global supply chain.



SCRM "commercially acceptable global standard(s)" must be derived from Commercial Industry Best Practices.

SCRM Standardization Requires Public-Private Collaborative Effort

Courtesy of Don Davidson, OSD TMSN ,Chief of Outreach and Standardization

Major Efforts being executed by DDRE/SE

- Implementing 5200.39 and 5000.02 Program Protection Policy
  - Review/Coordination of PPPs for ACAT I programs
  - Program protection assessment methodology
  - Guidance and best practice countermeasures, education and training, industry outreach, to assist programs with CPI identification and protection
- Supply Chain Risk Management
  - Procedures, capability to utilize threat information in acquisition
  - Commercial standards for secure components (ISO/IEC, The Open Group)
- Horizontal Protection Procedures
  - Acquisition Security Database (ASDB) oversight and implementation
- Advancing the practice: Systems Security Engineering
  - SERC Research Topic – “Security Engineering”
  - INCOSE Working Group on Systems Security Engineering
  - DoD/NSA Criticality Analysis Working Group
- DoD Anti-Tamper Executive Agent
  - Anti-Tamper IPT, AT policy, guidance advocate
  - Legislative Proposal – Defense Exportability Fund Pilot Program
- Countering Counterfeits Tiger Team
  - Lifecycle strategy to reduce counterfeits, especially microelectronics

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

The Open Group
Trusted Technology Provider Framework (TTPF)

Purpose

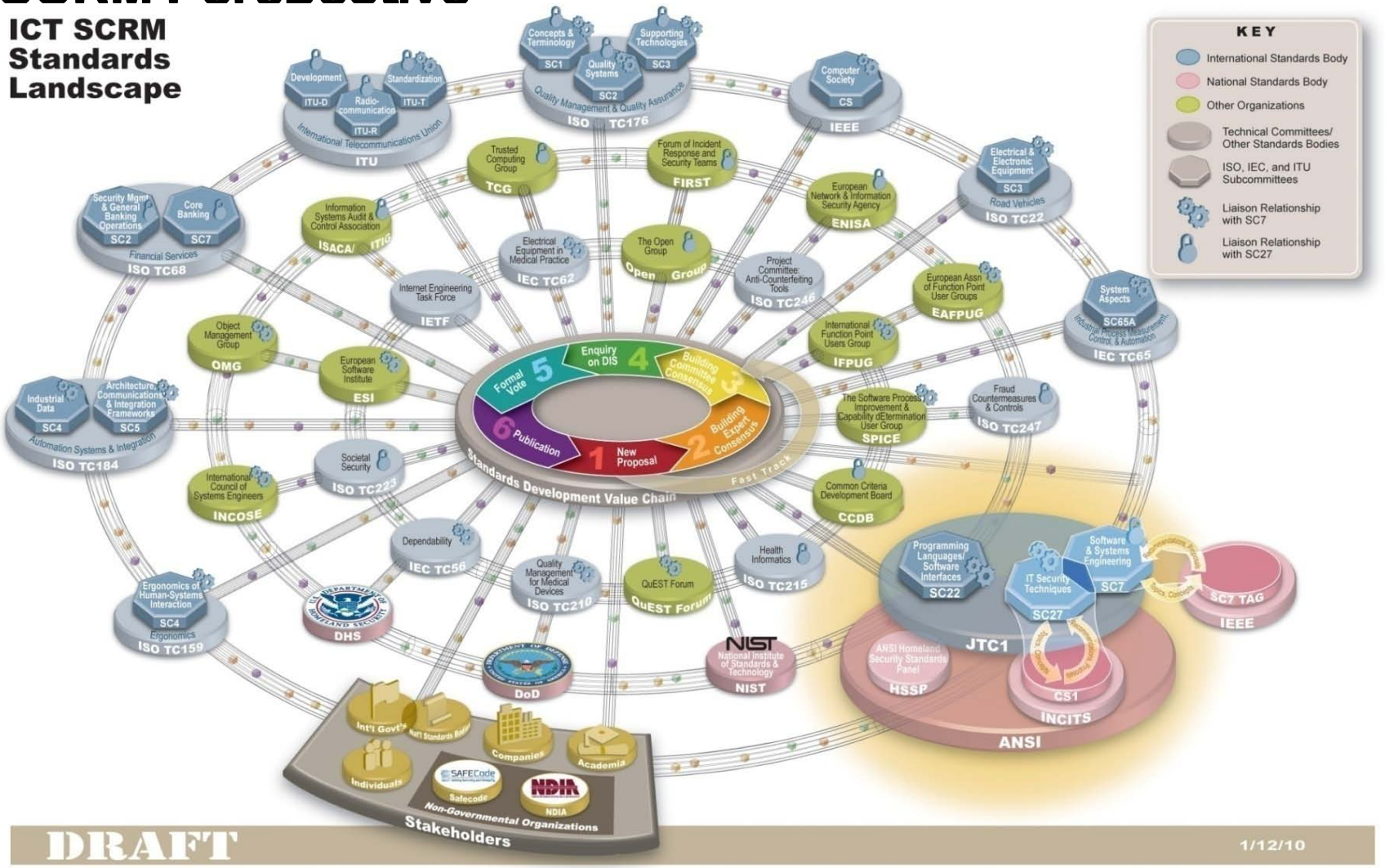
Identify and gain consensus on common processes, techniques, methods, product and system testing procedures, and language to describe and guide product development and supply chain management practices that can mitigate vulnerabilities which could lead to exploitation and malicious threats to product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

Standards Development Organizations Landscape: an SCRM Perspective



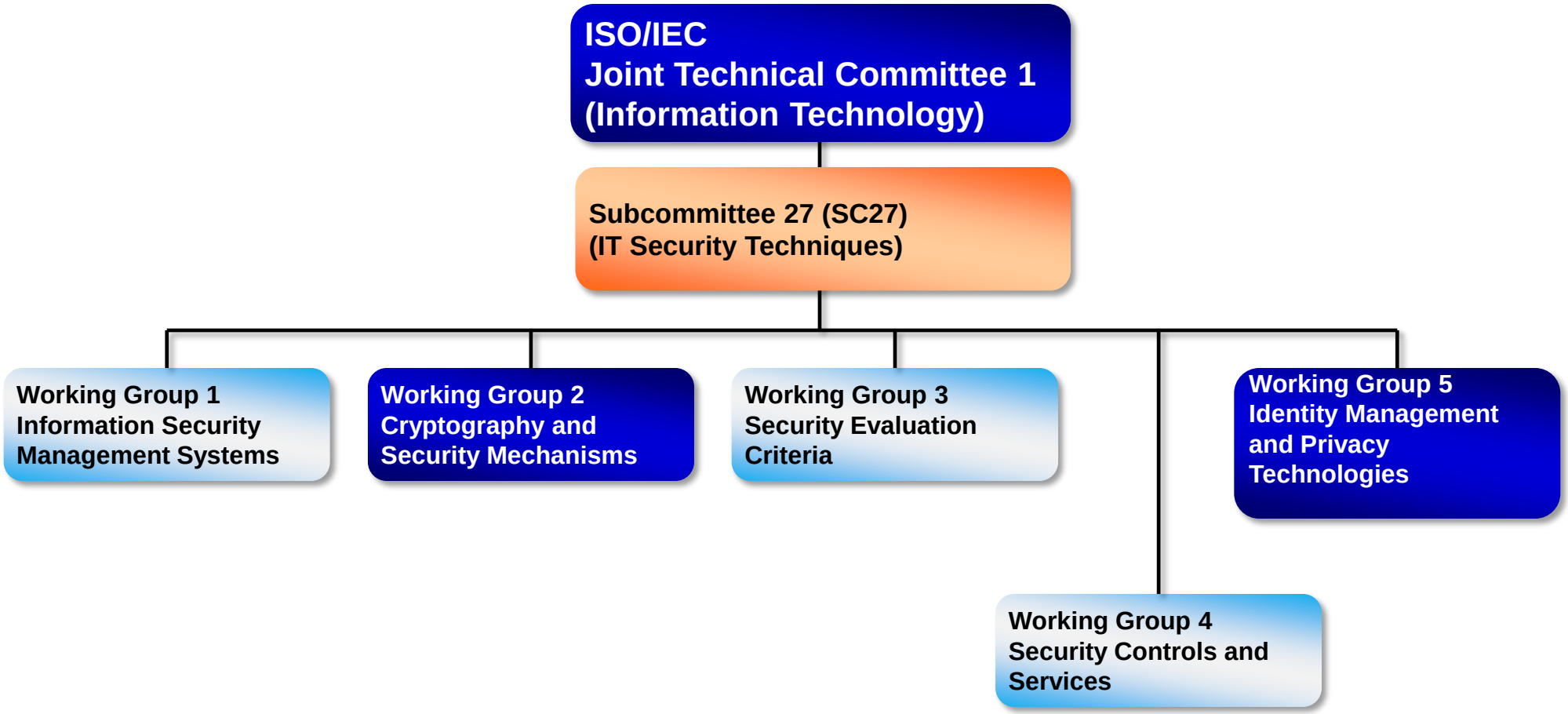
Courtesy of Don Davidson, OSD TMSN ,Chief of Outreach and Standardization

CS1 ICT SCRM Ad Hoc Group

- Established in February 2009
- Joint with SC7 TAG
- Substantial industry and government participation
- Contributed to several new and under revision standards
- Developed consensus-based USNB proposal for ICT Supply Chain Assurance Standard

Courtesy of Nadya Bartol, Booz Allen Hamilton

ISO/IEC JTC1 SC27 focuses on IT Security Techniques



Courtesy of Nadya Bartol, Booz Allen Hamilton

What is the Problem and Gaps We Are Trying to Address?

Problem

- Information and Communication Technology (ICT) products are assembled, built, and transported by multiple vendors around the world before they are acquired ***without the knowledge of the acquirer***
- Abundant opportunities exist for malicious actors to tamper with and sabotage products, ultimately compromising system integrity and operations ***evidenced by multiple recently publicized incidents*** (counterfeit hardware sold to government agencies)
- Organizations acquiring hardware, software, and services are not able to understand and manage the security risks associated with the use of these products and services

Need

- Provide a common language for addressing the problem
- Provide a resource that would help acquirers ***articulate requirements*** to product and service providers and ***monitor implementation*** in a recognizable manner that is vetted internationally
  - Increase confidence in acquired products and services from security risk point of view
  - Create a common language to articulate expectations regarding security risks associated with product and service acquisition
- Provide a resource that would help product and service providers ***demonstrate responsible practices, regardless of where they are located***

Courtesy of Nadya Bartol, Booz Allen Hamilton

ISO/IEC 27036: Information technology – Security techniques – Information Security for Supplier Relationships (proposed title)

- 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

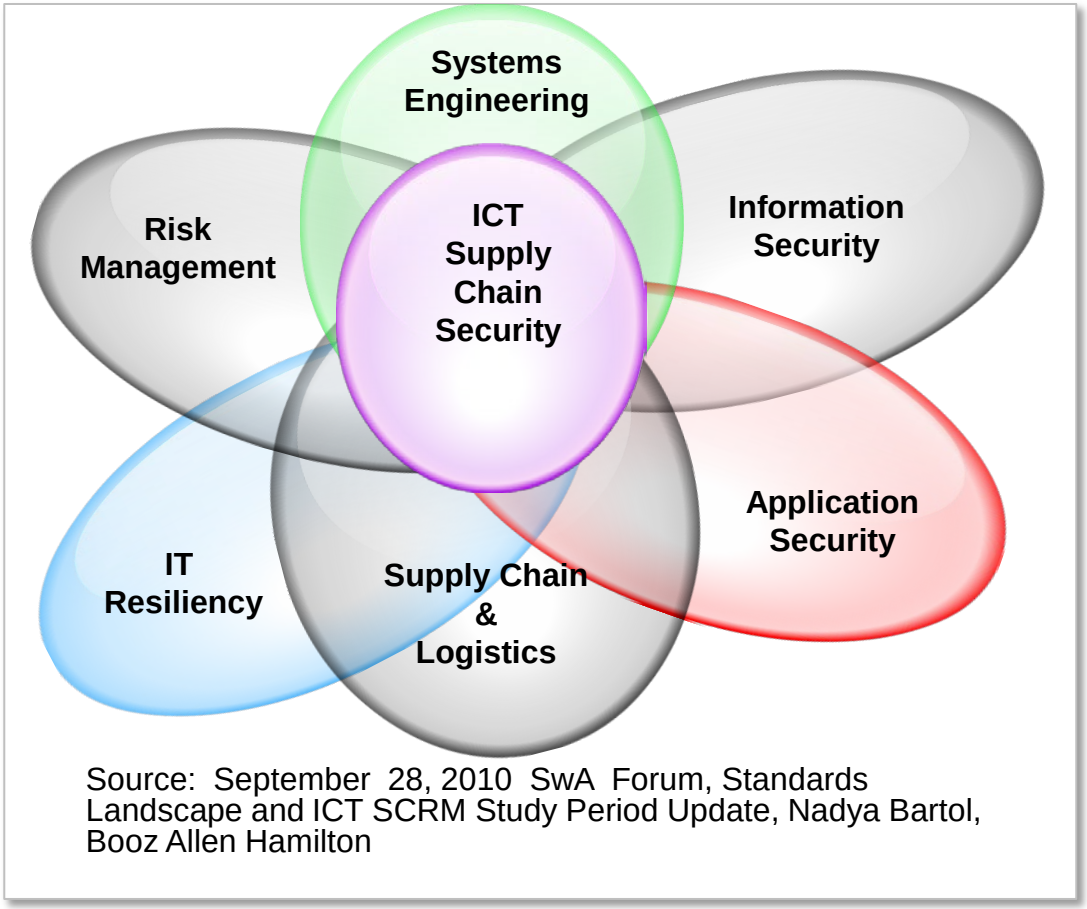
- Relevant Documents to be considered
  - Management Systems: ISO/IEC 27000 family; ISO 28000, Supply Chain Resiliency; ISO/IEC 20000, IT Service Management
  - Risk Management: ISO 31000, ISO/IEC 27005, and ISO/IEC 16085
  - Lifecycle Processes and Practices, software acquisition, and software assurance ISO/IEC/IEEE 15288 (systems), ISO/IEC/IEEE 12207 (software), IEEE 1062 (software acquisition), ISO/IEC15026 (software assurance)
  - ISO TMB NWIP on Outsourcing

Courtesy of Nadya Bartol, Booz Allen Hamilton

What's next?

- Participate in SC7 TAG intersections through your SC7 TAG
- Participate through your IEEE representative to the SC7 TAG
- Participate through the SwA Working Groups and Forum
- Stay Tuned …

ICT Supply Chain Risk Management (SCRM)



Source: September 28, 2010 SwA Forum, Standards Landscape and ICT SCRM Study Period Update, Nadya Bartol, Booz Allen Hamilton

Back-up

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

The DHS SwA Processes and Practices Working Group has synthesized the contributions of leading government and industry experts into a set of high-level goals and supporting practices (an evolution of the SwA community's Assurance Process Reference Model)

The goals and practices are mapped to specific industry resources providing additional detail and real world implementation and supporting practices

- Assurance Focus for CMMI
- Building Security In Maturity Model
- Open Software Assurance Maturity Model
- CERT® Resilience Management Model
- CMMI for Acquisition
- CMMI for Development
- CMMI for Services
- SwA Community's Assurance Process Reference Model –Initial Mappings
- SwA Community's Assurance Process Reference Model - Self Assessment
- SwA Community's Assurance Process Reference Model – Mapping to Assurance Models

Other valuable resources that are in the process of being mapped include

- NIST IR 7622: DRAFT Piloting Supply Chain Risk Management Practices for Federal Information Systems
- NDIA System Assurance Guidebook
- Microsoft Security Development Lifecycle
- SAFECode