SOFTWARE ASSURANCE FORUM

BUILDING SECURITY IN

Designed In Security Enabling Trustworthy Cyberspace

March 28, 2012

Software Assurance "End State" Objectives…

- **Government, in collaboration with industry/academia, raised expectations for product assurance with requisite levels of integrity and security:**
  - Helped advance more comprehensive software assurance diagnostic capabilities to mitigate risks stemming from exploitable vulnerabilities and weaknesses.
  - Collaboratively advanced use of software security measurement & benchmarking schemes.
  - Promoted use of methodologies and tools that enabled security to be part of normal business.
- **Acquisition managers & users factored risks posed by the software supply chain as part of the trade-space in risk mitigation efforts:**
  - Information on suppliers' process capabilities (business practices) would be used to determine security risks posed by the suppliers' products and services to the acquisition project and to the operations enabled by the software.
  - Information about evaluated products would be available, along with responsive provisions for discovering exploitable vulnerabilities, and products would be securely configured in use.
- **Suppliers delivered quality products with requisite integrity and made assurance claims about the IT/software safety, security and dependability:**
  - Relevant standards would be used from which to base business practices & make claims.
  - Qualified tools used in software lifecycle enabled developers/testers to mitigate security risks.
  - Standards and qualified tools would be used to certify software by independent third parties.
  - IT/software workforce had requisite knowledge/skills for developing secure, quality products.

What if…

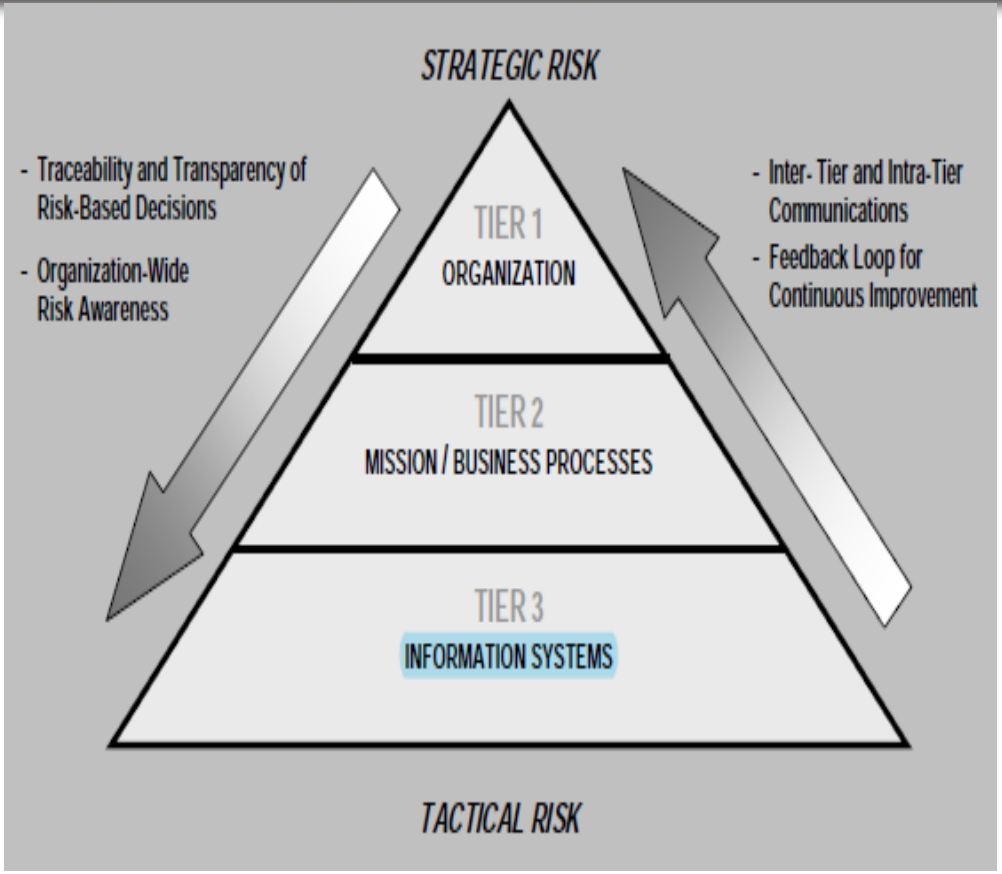
1. The Federal Government supported a culture more demanding of assured products with requisite levels of integrity and security, and in collaboration with industry and academia, would have organizations structured and funded to bring forward more comprehensive software assurance diagnostic capabilities to mitigate risks stemming from exploitable vulnerabilities in products.
2. Components requiring high assurance would be scrutinized, ensuring personnel in several disciplines remain mindful of changing threats and remain focused on discovering exploitable vulnerabilities in software throughout the lifecycle.
3. Acquisition managers would have sufficient information on risks posed by the supply chain with appraisal information on their suppliers' process capabilities to determine risks posed by the suppliers' products and services to the acquisition project and to the operations enabled by the software, and program managers would use that information as part of the trade-space in their acquisition risk mitigation efforts.
4. Suppliers would have assurance standards from which to base their business practices, and would begin to develop software to meet those standards and be able to make assurance claims about the safety, security and dependability of their software in order to increase sales in both the public and private sectors where demand for high assurance products is growing rapidly.

Software Assurance Challenges

Businesses trust that cyber threats are being addressed

When Business do address the SwA problem it is compliance driven

Tactical approaches for swa are being used and as a result do not tie directly to strategic business efforts and SwA does not contribute to business ROI



Summarized from Enhancing Adoption of SwA Practices June 28, 2011 SwA Working Group

Source: NIST 800-37 Guide for Applying the Risk Management Framework to Federal Information Systems A Security Life Cycle Approach

Updates and perspectives on recent NIST guidance

- John Boyens, NIST – NIST 800-53 rev 4 and NIST IR 7622
- Don Davidson, DOD CIO - Emerging SwA Controls for Acquirers
- Michele Moss, Booz Allen Hamilton - Emerging SwA Controls for Suppliers
- Mike Kass, NIST - Software Assurance Tools

SOFTWARE ASSURANCE FORUM

BUILDING SECURITY IN

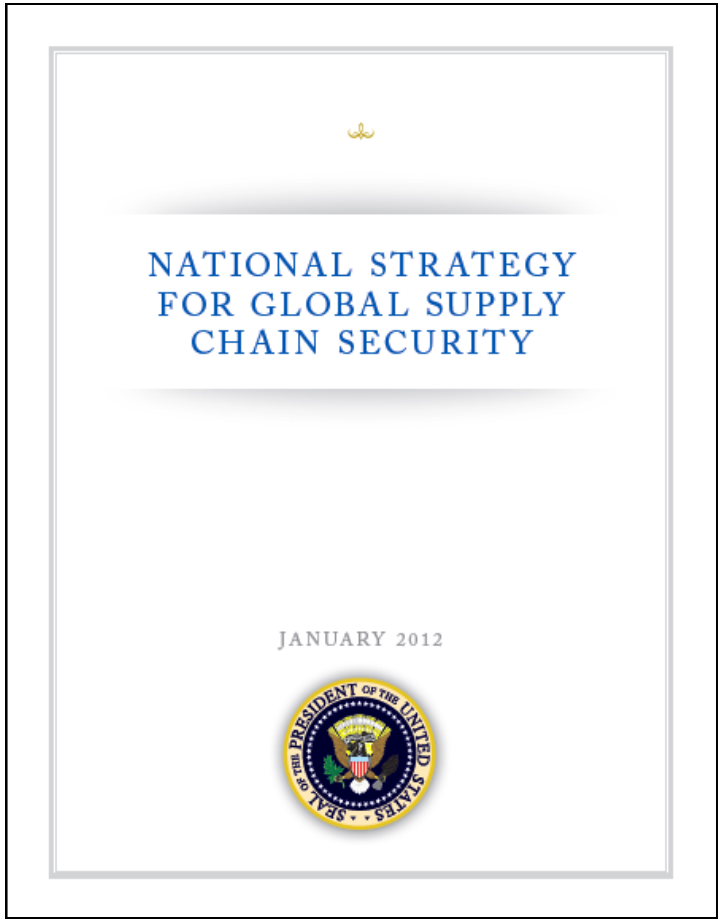
28 March 2012

Designed In Security Enabling Trustworthy Cyberspace – Emerging SwA Controls for Acquirers in Draft NIST 800-53 rev 4

Don Davidson (DOD-CIO TMSN)
Acquisition and Outsourcing Working Group Co-Chair

Homeland Security

Supply Chain: PERSPECTIVES



Supply Chain SECURITY

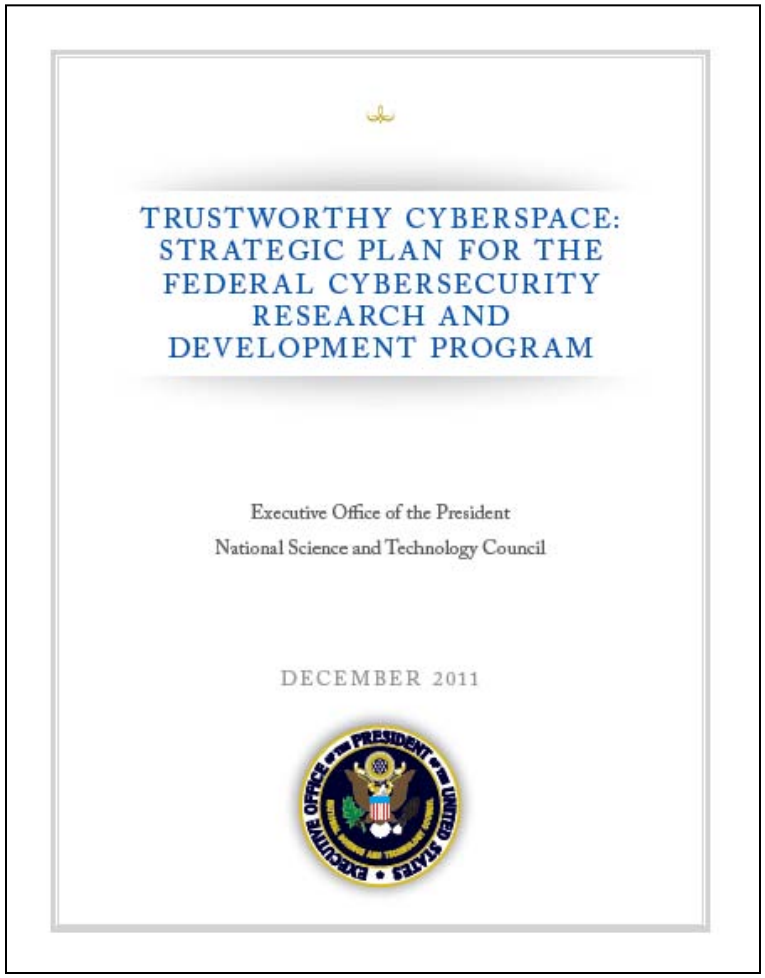
- Nodes of
  storage & throughput
- Lines of
  transport (& communication)

Supply Chain RESILIENCE

- Multi-sources
- Multi-nodes
- Multi-routes

- fix-on-the-fly (while doing , w/ no pause)

… to continue to move product



TRUSTWORTHY CYBERSPACE: STRATEGIC PLAN FOR THE FEDERAL CYBERSECURITY RESEARCH AND DEVELOPMENT PROGRAM

Executive Office of the President
National Science and Technology Council

DECEMBER 2011

This panel is focused on controls for

Product INTEGRITY

How do we improve our trust & confidence in HW, SW & Services we source from a global supply chain?

What if…

SwA Program Goal 1: The Federal Government supported a culture more demanding of assured products with requisite levels of integrity and security, and in collaboration with industry and academia, would have organizations structured and funded to bring forward more comprehensive software assurance diagnostic capabilities to mitigate risks stemming from exploitable vulnerabilities in products.

- SA-4 ACQUISITION PROCESS
- AT-5 CONTACTS WITH SECURITY GROUPS AND ASSOCIATIONS
- CM-10 SOFTWARE USAGE RESTRICTIONS
- CM-11 USER-INSTALLED SOFTWARE
- CM-9 CONFIGURATION MANAGEMENT PLAN

SA-4 Acquisition Process

The organization includes the following requirements, descriptions, and criteria, either explicitly or by reference, in information system acquisition contracts based on applicable federal laws, Executive Orders, directives, policies, regulations, standards, guidelines, and organizational mission/business needs:

a. Security functional requirements;
b. Security strength requirements;
c. Security assurance requirements;
d. Security-related documentation requirements;
e. Description of the information system development environment and environment in which the system is intended to operate; and
f. Acceptance Criteria

Defining security assurance requirements is part of the control ***baseline for all systems***

SA-4 Acquisition Process (continued)

Enhancements for

Moderate systems

(1) developers provide a description of the functional properties of the security controls to be employed

(4) [organization-defined information system components] acquired are explicitly assigned to an information system, and that the owner of the system acknowledges this assignment.

High systems

(2) developers provide design and implementation information for the security controls … at the following level of detail: [Selection (one or more): high-level design in terms of subsystems; low-level design in terms of modules; source-code/hardware schematics

AT-5 Contacts With Security Groups And Associations

The organization establishes and institutionalizes contact with selected groups and associations within the security community:

- To facilitate ongoing security education and training for organizational personnel;
- To maintain currency with recommended security practices, techniques, and technologies; and
- To share current security-related information including threats, vulnerabilities, and incidents.

Moderate and High *systems in today's environment of rapidly changing technologies and threats require ongoing contact with security groups and associations such as SwA, SAFECode, US CERT, Defense Industrial Base, and others*

Configuration Management

CM-9 CONFIGURATION MANAGEMENT PLAN **(Moderate and High)**

"c. Defines the configuration items for the information system and places the configuration items under configuration management."

CM-10 SOFTWARE USAGE RESTRICTIONS **(for all)**

a. Uses software and associated documentation in accordance with contract agreements and copyright laws;
b. Employs tracking systems for software and associated documentation protected by quantity licenses to control copying and distribution; and
c. Controls and documents the use of peer-to-peer file sharing technology to ensure that this capability is not used for the unauthorized distribution, display, performance, or reproduction of copyrighted work.

CM-11 USER-INSTALLED SOFTWARE **(for all)**

The organization enforces explicit rules governing the installation of software by users.

Information system and system items (hardware, software, firmware, and documentation) need to be identified and managed.

What if…

SwA Program Goal 2: Components requiring **high assurance** would be scrutinized, ensuring personnel in several disciplines remain mindful of changing threats and remain focused on discovering exploitable vulnerabilities in software throughout the lifecycle.

- SA-12 SUPPLY CHAIN PROTECTION
- SA-15 DEVELOPMENT PROCESS, STANDARDS, AND TOOLS
- SA-16 DEVELOPER-PROVIDED TRAINING
- SA-17 DEVELOPER SECURITY ARCHITECTURE AND DESIGN
- SC-3 SECURITY FUNCTION ISOLATION
- MA-4 NON-LOCAL MAINTENANCE

Note: SA-12 through SA-19 controls vetted through SCRM WG 2

Buy it well

SA-12 SUPPLY CHAIN PROTECTION

The organization protects against supply chain threats by employing [Assignment: organization-defined security safeguards] as part of a comprehensive, defense-in-breadth information security strategy.

For High systems

SA-15 DEVELOPMENT PROCESS, STANDARDS, AND TOOLS

a. Requires that information system developers follow a documented development process that:
   - Explicitly addresses security requirements;
   - Identifies the standards and tools used in the development process; and
   - Documents the specific tool options and tool configurations used in the development of the information system; and

b. Reviews the development process, standards, tools, and tool options/configurations to ensure that the process, standards, tools, and tool options/configurations selected and employed will lead to satisfying organizational security requirements

For High systems

Build it well (continued)

SA-17 DEVELOPER SECURITY ARCHITECTURE AND DESIGN

The organization requires that information system developers produce a design specification and security architecture for the system that:

a. Is created as an integral part of the system development process;
b. Is consistent with and supportive of the security architecture within the enterprise architecture;
c. Accurately and completely describes the required security functionality, and the allocation of security controls among physical and logical components; and
d. Expresses how individual security functions, mechanisms, and services work together to provide required security capabilities and a unified approach to protection

SC-3 SECURITY FUNCTION ISOLATION

The information system isolates security functions from nonsecurity functions.

For High systems

Use it well

SA-16 DEVELOPER-PROVIDED TRAINING

The organization requires that information system developers provide [Assignment: organization-defined training] on the correct use and operation of the security functions, controls, and/or mechanisms implemented in the system.

MA-4 NON-LOCAL MAINTENANCE

Control Enhancement (3) provides guidance on implementation to include Comparable security capability on information systems, diagnostic tools, and equipment providing maintenance services implies that the implemented security controls on those systems, tools, and equipment are at least as comprehensive as the controls on the information system being serviced.

For High systems

What if…

SwA Program Goal 3: Acquisition managers would have sufficient information on risks posed by the supply chain with appraisal information on their suppliers' process capabilities to determine risks posed by the suppliers' products and services to the acquisition project and to the operations enabled by the software, and program managers would use that information as part of the trade-space in their acquisition risk mitigation efforts.

- CA-2 SECURITY ASSESSMENTS
- MA-2 CONTROLLED MAINTENANCE
- MA-3 MAINTENANCE TOOLS
- SA-9 EXTERNAL INFORMATION SYSTEM SERVICES
- SA-5 INFORMATION SYSTEM DOCUMENTATION
- PL-2 SYSTEM SECURITY PLAN

CA-2 Security Assessments

Supplemental Guidance:

Organizations assess security controls in organizational information systems and the environments in which those systems operate as part of: (i) initial and ongoing security authorizations; (ii) FISMA annual assessments; (iii) continuous monitoring; and (iv) system development life cycle activities. Security assessments: ***(i) ensure that information security is built into organizational information systems; (ii) identify weaknesses and deficiencies early in the development process; (iii) provide essential information needed to make risk-based decisions as part of security authorization processes; and (iv) ensure compliance to vulnerability mitigation procedures.*** Organizations can use other types of assessment activities such as vulnerability scanning, penetration testing, and information system monitoring to ensure that the security posture of information systems during the entire life cycle is maintained. Security assessment reports document assessment results.

*Security assessments for **all systems** should include security activities throughout the lifecycle*

Maintenance

MA-2 CONTROLLED MAINTENANCE Supplemental Guidance:

. ….Organizations consider supply chain issues associated with replacement components for information systems.

MA-3 MAINTENANCE TOOLS (**Moderate and High)**

The organization approves, controls, and monitors information system maintenance tools.

SA-9 EXTERNAL INFORMATION SYSTEM SERVICES Supplemental Guidance:

“Organizations document the basis for trust relationships so the relationships can be monitored over time. External information”

Security considerations must continue throughout operations and maintenance/sustainment activities

SA-5 Information System Documentation

The organization:

c. Documents attempts to obtain information system documentation when such documentation is either unavailable or nonexistent and takes [Assignment: organization-defined actions] in response;

d. Protects documentation as required, in accordance with the risk management strategy; and

e. Distributes documentation to [Assignment: organization-defined personnel].

*Organizational personnel should have documentation to help them understand the implementation and operation of security controls associated with **ALL** organizational information systems*

PL-2 System Security Plan

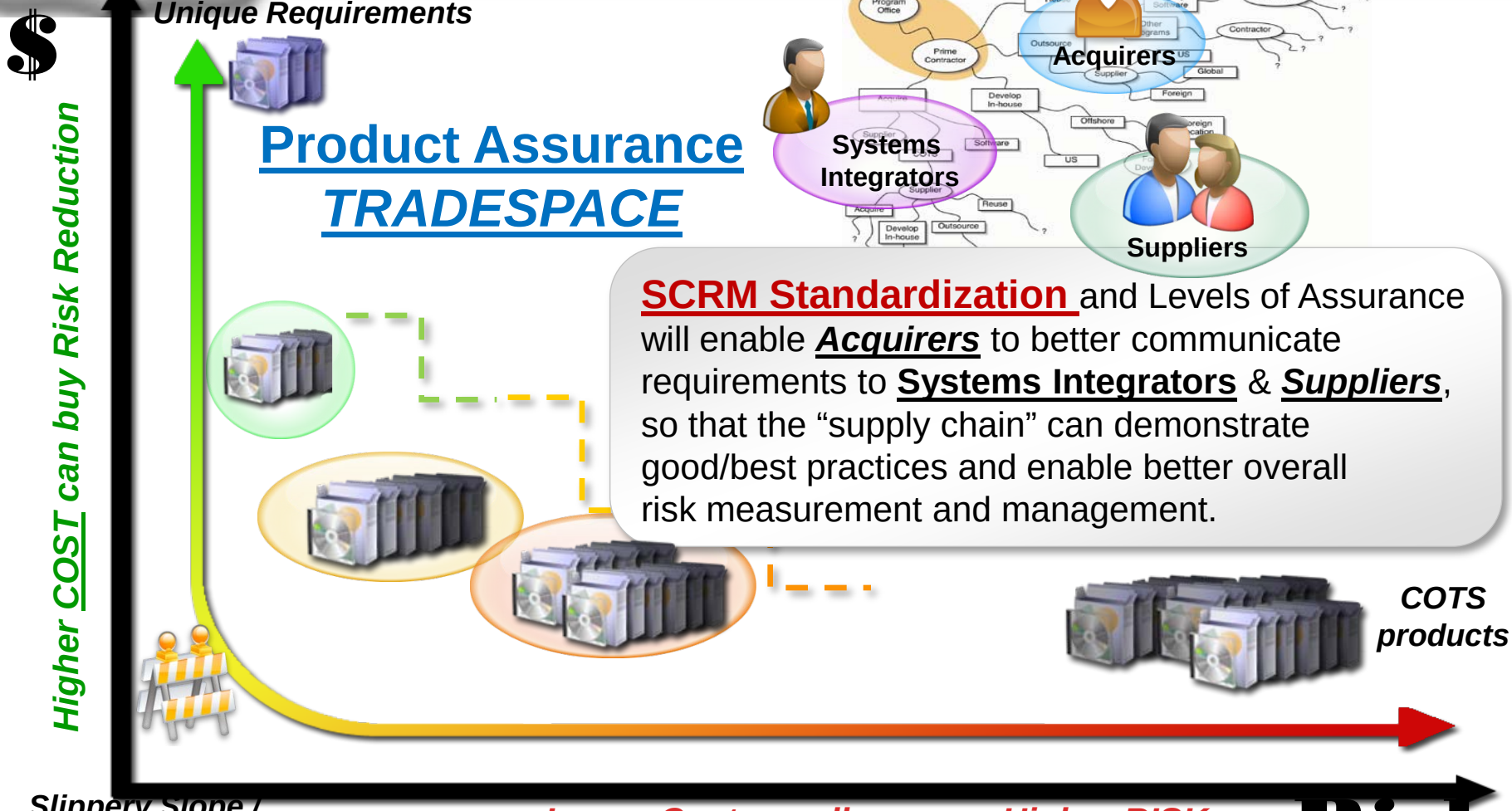
Enhancement: (3) SYSTEM SECURITY PLAN | PLAN / COORDINATE WITH OTHER ORGANIZATIONAL ENTITIES

The organization plans and coordinates security-related activities affecting the information system before conducting such activities in order to reduce the impact on other organizational entities.

Moderate and High *systems require coordination with other organizations for security-related activities (i.e. security assessments, audits, information system hardware and software maintenance, and contingency plan testing)*

SOFTWARE ASSURANCE FORUM

BUILDING SECURITY IN



SOFTWARE ASSURANCE FORUM

BUILDING SECURITY IN

28 March 2012

Designed In Security Enabling Trustworthy Cyberspace – Emerging SwA Controls for Suppliers in Draft NIST 800-53 rev 4

Michele Moss (Booz Allen Hamilton)
Processes and Practices Working Group Co-Chair

Homeland Security

What if…

SwA Program Goal 4: Suppliers would have assurance standards from which to base their business practices, and would begin to develop software to meet those standards and be able to make assurance claims about the safety, security and dependability of their software in order to increase sales in both the public and private sectors where demand for high assurance products is growing rapidly.

- SA-3 SYSTEM DEVELOPMENT LIFE CYCLE
- AT-3 SECURITY TRAINING
- IR-4 INCIDENT HANDLING
- PS-7 THIRD-PARTY PERSONNEL SECURITY
- SA-10 DEVELOPER CONFIGURATION MANAGEMENT
- SA-11 DEVELOPER SECURITY TESTING
- CM-2 BASELINE CONFIGURATION
- CM-4 SECURITY IMPACT ANALYSIS
- CM-7 LEAST FUNCTIONALITY
- AC-5 SEPARATION OF DUTIES
- AC-6 LEAST PRIVILEGE
- SA-8 SECURITY ENGINEERING PRINCIPLES

SA-3 System Development Life Cycle

For all systems, the organization:

a. Manages the information system using a documented system development life cycle methodology that incorporates information security considerations;

b. Defines and documents information security roles and responsibilities throughout the system development life cycle;

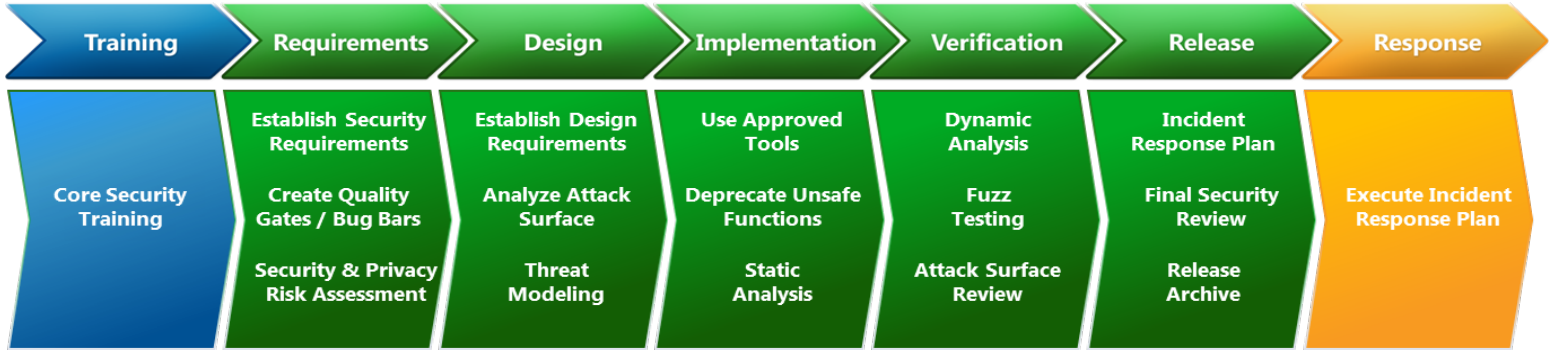
c. Identifies individuals having information security roles and responsibilities; and

d. Integrates the organizational information security risk management process into the system development life cycle activities.

Security awareness and training programs can help ensure that individuals having key security roles and responsibilities have the appropriate experience, skills, and expertise to conduct assigned system development life cycle activities

AT-3 Security Training

Supplemental Guidance: In addition, organizations provides enterprise architects, information system developers, software developers, acquisition/procurement officials, information system managers, system/network administrators, personnel performing independent verification and validation activities, security control assessors, and other personnel having access to system-level software, adequate security-related technical training specifically tailored for their assigned duties.



www.microsoft.com/sdl

IR-4 Incident Handling

For all systems, the organization:

a. Implements an incident handling capability for security incidents that includes preparation,

detection and analysis, containment, eradication, and recovery;

b. Coordinates incident handling activities with contingency planning activities; and

c. Incorporates lessons learned from ongoing incident handling activities into incident response procedures, training, and testing/exercises, and implements the resulting changes accordingly.

Organizations must consider incident response as part of the definition, design, and development of mission/business processes and information systems

PS-7 Third-party Personnel Security

For all system, the organization:

a. Establishes personnel security requirements including security roles and responsibilities for third-party providers;

b. Requires third-party providers to comply with personnel security policies and procedures of the organization;

c. Documents personnel security requirements; and

d. Monitors provider compliance.

Third-party providers include, for example, service bureaus, contractors, and other organizations providing information system development, information technology services, outsourced applications, and network and security management

Configuration Management

CM-2 BASELINE CONFIGURATION **(Moderate and High)**

The organization develops, documents, and maintains under configuration control, a current baseline configuration of the information

SA-10 DEVELOPER CONFIGURATION MANAGEMENT **(All systems)**

Supplemental Guidance for moderate and high systems: Organizations consider the quality and completeness of the configuration management activities conducted by developers as evidence of applying effective security safeguards. Information system developer is a general term that includes developers or manufacturers of information technology products (including hardware, software, firmware), systems integrators, vendors, and product resellers.

CM-4 SECURITY IMPACT ANALYSIS Supplemental Guidance: **(Moderate and High)**

…. to understand security control requirements and reviewing system design documentation to understand control implementation and how specific changes might affect the controls.

CM-7 Least Functionality

Control Enhancements for **moderate systems**

(1) LEAST FUNCTIONALITY | PERIODIC REVIEW

a. Disables [Assignment: organization-defined functions, ports, protocols, and services within the information system deemed to be unnecessary or nonsecure].

(4) LEAST FUNCTIONALITY | UNAUTHORIZED SOFTWARE

– The organization:

a. Identifies [Assignment: organization-defined software not authorized to execute on the information system];

b. Employs an allow-all, deny-by-exception policy to prohibit the execution of unauthorized software on the information system; and

c. Reviews and updates the list of unauthorized software [Assignment: organization-defined frequency].

SA-11 Developer Security Testing

For moderate and high systems, *t*he organization requires that information system developers:

a. Create and implement a security test and evaluation plan that provides for testing/evaluation:
   - At the depth of [Selection (one or more): security-related functional properties; security related externally visible interfaces; high-level design; low-level design; implementation representation (source code/hardware schematics)];
   - - At the rigor of [Selection: showing; demonstrating; rigorously demonstrating];

b. Include testing/evaluation at [Selection (one or more): unit; integration; system; regression]; and

c. Produce evidence of the execution of security testing/evaluation plan and the results of the testing/evaluation.

Developmental security testing occurs at all post-design phases of the system development life cycle.

Access Control

AC-5 SEPARATION OF DUTIES **(moderate and high)**

- "c. Defines information system access authorizations to support separation of duties."

Addresses the potential for abuse of authorized privileges and helps to reduce the risk of malevolent activity without collusion

AC-6 LEAST PRIVILEGE **(moderate and high)**

The organization employs the concept of least privilege, allowing only authorized accesses for users (and processes acting on behalf of users) which are necessary to accomplish assigned tasks in accordance with organizational missions and business functions.

Processes operate at privilege levels no higher than necessary to accomplish required organizational missions and/or functions

SA-8 Security Engineering Principles

For moderate and high systems, the organization applies information system security engineering principles in the specification, design, development, implementation, and modification of the information system.

Security engineering principles include, for example:

- Security engineering principles include, for example: (i) developing layered protections; (ii) establishing sound security policy, architecture, and controls as the foundation for design; (iii) incorporating security requirements into the system development life cycle; (iv) delineating physical and logical security boundaries; (v) ensuring system developers are trained on how to build secure software; (vi) tailoring security controls to meet organizational and operational needs; **(vii) performing threat modeling to identify use cases, threat agents, attack vectors, and attack patterns as well as compensating controls and design patterns needed to mitigate risk; and (viii) reducing risk to acceptable levels, thus enabling informed risk management decisions.**

What if …

“NEW” SwA Program Goal: Operations should inform development and acquisition of diagnostic results indicating exploitable vulnerabilities in products currently used or planned to be used in mission/business critical systems.

- CA-7 CONTINUOUS MONITORING
- IR-8 INCIDENT RESPONSE PLAN
- AC-17 REMOTE ACCESS
- RA-5 VULNERABILITY SCANNING

CA-7 Continuous Monitoring

For all systems, the organization develops a continuous monitoring strategy and implements a continuous monitoring program that includes:

a. Establishment of [Assignment: organization-defined metrics] to be monitored;

b. Establishment of [Assignment: organization-defined frequencies] for monitoring and assessments;

c. Ongoing security control assessments in accordance with the organizational continuous monitoring strategy;

d. Ongoing security status monitoring of organization-defined metrics in accordance with the organizational continuous monitoring strategy;

e. Correlation and analysis of security-related information generated by assessments and monitoring;

f. Response actions to address results of the analysis of security-related information; and

g. Reporting the security status of organization and the information system to [Assignment: organization-defined personnel] [Assignment: organization-defined frequency].

Continuous monitoring programs facilitate ongoing awareness of threats

IR-8 Incident Response Plan

Supplemental Guidance: It is important that organizations develop and implement a coordinated approach to incident response. Organizational missions, business functions, strategies, goals, and objectives for incident response help determine the structure of incident response capabilities. **As part of a comprehensive incident response capability, organizations consider the coordination and sharing of information with external organizations, including, for example, external service providers and organizations involved in the supply chain for organizational information systems**.

AC-17 Remote Access

Enhancement for **moderate and high** systems:

(1) REMOTE ACCESS | AUTOMATED MONITORING / CONTROL

- The organization employs automated mechanisms to facilitate the monitoring and control of remote access methods.

Automated monitoring and control of remote access sessions allows organizations to ***detect cyber attacks and also ensure ongoing compliance with remote access policies by auditing activities of remote users*** *on a variety of information system components (e.g., servers, workstations, notebook computers, smart phones).*

RA-5 Vulnerability Scanning

Supplemental Guidance: Security categorization of information systems guides the frequency and comprehensiveness of vulnerability scans. Organization determine the required vulnerability scanning for all information system components, ensuring that **potential sources of vulnerabilities such as networked printers, scanners, and copiers are not overlooked**. **Vulnerability analyses for custom software applications may require additional approaches such as static analysis, dynamic analysis, binary analysis, or hybrid of the three approaches.** Organizations can employ these analysis approaches in a variety of tools (e.g., web-based application scanners, static analysis tools, binary analyzers) and in source code reviews. Vulnerability scanning includes, for example: (i) scanning for patch levels; (ii) scanning for functions, ports, protocols, and services that should not be accessible to users or devices; and (iii) scanning for improperly configured or incorrectly operating information flow control mechanisms.

SOFTWARE ASSURANCE FORUM

BUILDING SECURITY IN

28 March 2012

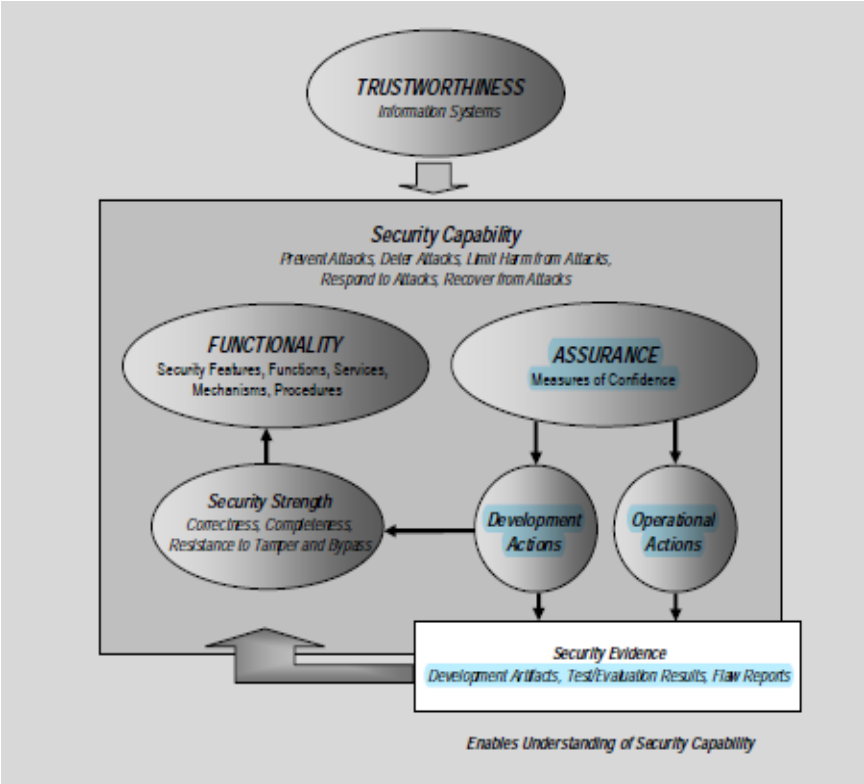
Designed In Security Enabling Trustworthy Cyberspace – Software Assurance Technology and Tools and NIST SP 800-53 Revision 4 Security Controls

Michael Kass (NIST)
Technology and Tools Working Group Co-Chair

Homeland Security

Trustworthiness and Assurance as Defined in SP 800-53r4

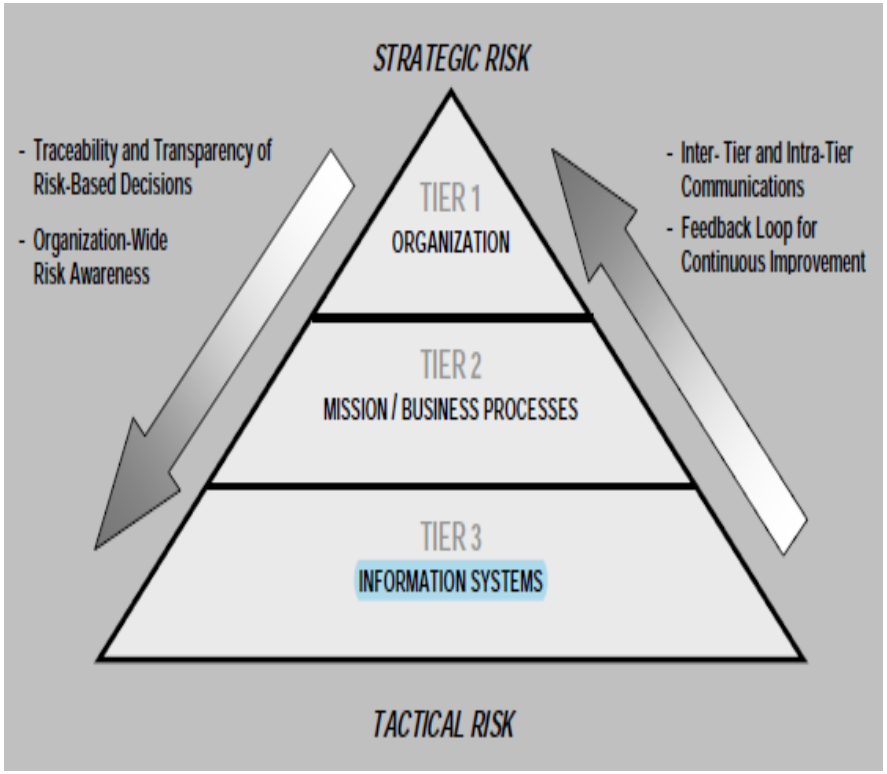
- **Trustworthiness** – the degree to which systems can be expected to preserve the confidentiality, integrity and availability of the information being processed, stored or transmitted across the full range of threats
- **Assurance** – the *measure of confidence* that the security functionality is implemented correctly, operates as intended and produces the desired outcome against the system security requirements
- **Development & Operational Actions** –
  - Development - CM and secure engineering principles
  - Operational - Integrity checks, continuous monitoring, penetration testing
- **Security Evidence** – development artifacts, test/evaluation results, weakness and vulnerability reports



Homeland Security

NIST SP 800-53r4: 3 Levels of Risk

- **SP 800-53 R4 Addresses Risk at 3 Levels**
  - **Organization -** a prioritization of organizational missions/business functions consistent with the strategic goals and objectives of the organization and measures of performance.
  - **Mission/Business Process** - defining the mission/business processes needed to support the organizational missions/business functions.
  - **Information Systems** – selecting, implementing, assessing and monitoring security controls
- **Our focus –** security controls addressing assurance through the use of automated tools, enumerations at *the information systems tier* in the strategic risk stack



Homeland Security

Technology/Tools in Support of SP 800-53r4

- NIST SP 800-53r4 incorporates guidance in the use of automated tools enumerations and technologies in its security controls, including:
  - Security Content Automation Protocol (SCAP), Common Vulnerabilities and Exposures (CVE), Common Vulnerability Scoring System (CVSS), Common Weakness Enumeration (CWE), Open Vulnerability Assessment Language (OVAL)
- In addition to controls above, we identified other controls where existing and emerging standards in security assurance would apply, including:
  - Common Attack Pattern Enumeration and Classification (CAPEC)
  - Malware Attribution Enumeration and Classification (MAEC)
  - Incident Object Description Exchange Format (IODEF)
  - Software Assurance Findings Expression Schema (SAFES)
  - Cyber Observable eXpression (CybOX)
  - ISO/OMG KDM Standard-based tools

SOFTWARE ASSURANCE FORUM

BUILDING SECURITY IN

Assurance Tools and Technology Map to SP 800-53r4 Controls

- **IR – Incident Response**
  - IR-6: Incident Reporting *(IODEF, CybOX)*
- **RA – Risk Assessment**
  - RA-5: Vulnerability Scanning *(CWE, CVE, CCE, OVAL, CVSS, CPE, CAPEC)*
- **SA – System and Services Acquisition**
  - SA-11: Developer Security Testing *(CAPEC, CWE)*
  - SA-12: Supply Chain Protection (MAEC, CAPEC, CWE)
  - SA-15: Development Process, Standards and Tools (CWE, CAPEC, CVE, NVD)
- **SC – System and Communications Protection**
  - SC-2,3,4.. . Other architecture requirements (ISO/*OMG standards-based static binary analysis tools)*
  - SC-38: Malware Analysis(MAEC, CybOX)
- **SI – System and Information Integrity**
  - SI-2: Flaw Remediation *(CWE, CVE)*
  - SI-3: Malicious Code Protection *(MAEC)*

ID	FAMILY	ID	FAMILY
AC	Access Control	MP	Media Protection
AT	Awareness and Training	PE	Physical and Environmental Protection
AU	Audit and Accountability	PL	Planning
CA	Security Assessment and Authorization	PS	Personnel Security
CM	Configuration Management	RA	Risk Assessment
CP	Contingency Planning	SA	System and Services Acquisition
IA	Identification and Authentication	SC	System and Communications Protection
IR	Incident Response	SI	System and Information Integrity
MA	Maintenance	PM	Program Management

Homeland Security

IR – Incident Response

Current federal policy requires that all federal agencies (unless specifically exempted from such requirements) report security incidents to the United States Computer Emergency Readiness Team (US-CERT) within specified time frames designated in the US-CERT Concept of Operations for Federal Cyber Security Incident Handling.

- **IR-6: Incident Reporting** - The organization requires personnel to report suspected security incidents to the organizational incident response capability within an organization-defined time period; and reports security incident information to organization-defined authorities.
- Supplemental control guidance includes:
  - The organization employs automated mechanisms to assist in the reporting of security incidents. (IODEF, CybOX)

RA – Risk Analysis

- **RA-5: Vulnerability Analysis** - organization scans for vulnerabilities in the information system and hosted applications; employs vulnerability scanning tools and techniques that promote interoperability among tools and the automation of the vulnerability management process by using standards for:
  - Enumerating platforms, software flaws and improper configurations *(CPE, CWE, CVE, CCE)*
  - Formatting and making transparent checklists and test procedures *(OVAL)*
  - Measuring vulnerability impact *(CVSS)*
  - Remediating legitimate vulnerabilities in accordance with organizational assessment of risk *(CWE mitigations)*
- Control enhancements include:
  - Vulnerability analyses for custom software applications may require additional approaches such as static analysis, dynamic analysis, binary analysis, or hybrid of the three approaches. *(*CWE*, CWE-compatible tools,* CAPEC*, CAPEC-compatible tools)*

SA – Systems and Services Acquisition

- **SA-11: Developer Security Testing** - a developer's test and evaluation plans provide the specific activities that developers plan to carry out including the types of analyses, testing, and reviews of software and firmware components, the degree of rigor to be applied in the analyses, tests, and reviews, and the types of artifacts produced during those processes.
- Control enhancements require information system developers to:
  - Use of one or more source code analysis tools to examine the system for common flaws *(CWE-compatible tools)*
  - Perform threat and vulnerability analysis and subsequent testing of the as-built information system (CAPEC, *CAPEC-compatible* tools)
  - Remediate security flaws or identify and document such flaws *(CWE)*
  - Perform manual code reviews of the IT product or information system *(CWE as guidance)*
  - Perform penetration testing of the information system (CAPEC, *CAPEC-compatible* tools)
  - Perform an attack surface review
  - Perform regression testing

SA – Systems and Services Acquisition

- **SA-12: Supply Chain Protection** – an organization protects against supply chain threats by employing security safeguards as part of a comprehensive defense-in-breadth information security strategy.
- Control enhancements include:
  - The organization (or an independent third party entity) conduct assessments of systems, system components, IT products or services prior to acceptance, selection or update … to uncover unintentional and intentional vulnerabilities including:
    - Malware *(MAEC)*
    - Malicious processes (CAPEC)
    - Counterfeits
  - Assessments can include:
    - Static or dynamic analysis tools *(CWE-compatible tools, CAPEC-compatible tools)*
    - Black box/White box testing (*CAPEC-compatible tools)*
    - Penetration testing (*CAPEC-compatible tools)*
    - Simulations
    - Fuzz testing

SA – Systems and Services Acquisition

- **SA-15: Development Process, Standards and Tools** – an organization reviews the development process, standards, tools, and tool options and configurations to ensure that the process, standards, tools, and tool options/configurations selected and employed will lead to satisfying organizational security requirements.
- Control enhancements include:
  - **The organization requires that information system developers perform an automated vulnerability analysis** to discover vulnerabilities in the information system (CWE-compatible tools), determine their exploitation potential (CWE and CAPEC), determine potential risk mitigations *(CWE mitigations)* and deliver the output from tools and results of the analysis (SAFES).
  - **The organization requires that information system developers use of threat modeling and vulnerability analysis from similar information systems** to inform the current development process *(CAPEC, CVE, NVD)*

SC – System and Communication Protection

- System and Communication Protection security controls identify many specific architectural security requirements for information systems, including:
  - **SC-2** Application partitioning
  - **SC-3** Security function isolation
  - **SC-4** Information in shared resources
  - **Other SC requirements…**

  for which *(ISO/OMG KDM standard-based static binary analysis tools)* extraction of artifacts provide evidence for compliance verification at code, detail design or architecture levels.
- **SC-38: Malware Analysis –** The organization employs tools and techniques to analyze the behavior of malware and incorporates the results of malware analysis into the organization incident response and flaw remediation process. *(MAEC, CybOX)*

SI – Systems and Information Integrity

- **SI-2: Flaw Remediation** – the organization identifies system flaws, installs security-relevant software and firmware updates, tests software and firmware updates related to flaw remediation for effectiveness and potential side effects on organizational information systems before installation; and incorporates flaw remediation into the organizational configuration management process.
- Supplemental guidance includes:
  - Organizations take advantage of available resources such as the Common Weakness Enumeration (CWE) or Common Vulnerabilities and Exposures (CVE) databases in remediating flaws discovered in organizational information systems. <CAPEC should be in here as well in relation to testing the effectiveness of remediations>

SI – Systems and Information Integrity

- **SI-3: Malicious Code Protection** – the organization employs malicious code protection mechanisms at information system entry and exit points and at workstations, servers, or mobile computing devices on the network to detect and eradicate malicious code:
- Supplemental guidance includes:
  - In addition to commercial off-the-shelf software, malicious code may also be present in custom-built software. This could include, for example, logic bombs, back doors, and other types of cyber attacks that could affect organizational missions/business functions. Traditional malicious code protection mechanisms cannot always detect such code. In these situations, organizations rely instead on other safeguards including, for example, *secure coding practices (CWE)*, configuration management and control, trusted procurement processes, and monitoring practices to help ensure that software does not perform functions other than those functions intended. <CybOX should be in here for defining observables for malicious code behavior and CAPEC should be in here for defining relevant patterns of observables>

Discussion

- What can we as SwA Working Group Co-Chairs do to aid in the implementation of these controls?