

Cyber Security and Information Assurance Services

NASA Independent Verification and Validation (IV&V) Program

<http://www.nasa.gov/centers/ivv/home/index.html>

**Get Confidence in Mission
Security with IV&V
Information Assurance**



IV&V
IA

September 10, 2014

- Threat Landscape
- Regulatory Framework
- Life-cycles
- IV&V Rigor and Independence

Threat Landscape



- Continuously evolving
 - Network connectivity is constantly increasing
- More capable, diverse and distributed
 - Attacks are increasing in sophistication and frequency
- Assets
 - High Value Targets



“...the threat to NASA’s information security is persistent and ever changing. Unless NASA is able to continuously innovate and adapt, their data, systems, and operations will continue to be endangered.”

– Congressional Subcommittee on Investigations and Oversight; Committee on Science, Space, and Technology, Feb 2012

IV&V SSO IA Mission



Ensuring Mission and Safety Critical Software and Systems Operate Reliably, Safely, and **Securely**

- Perform the ***“information system and security control assessment and monitoring”*** techniques that NIST attributes to the IV&V assessor.
 - Risk Management Framework for the design, development, implementation, operation, maintenance, and disposition of federal information systems.
- Perform **Security Analyses** throughout the development life-cycle.
 - IEEE-1012 Standard for System and Software V&V
- Counteract the threat landscape throughout the system life-cycle, to include for ground, satellite, and command & control systems.
- Techniques deployed throughout project life-cycle phases.

Basis



FISMA requires each agency to use a risk-based approach to develop, document, and implement an agency wide security program for the information and information systems that support the operations and assets of the agency, including those provided or managed by another agency, contractor, or other source.

- OMB-130
 - “Security of Federal Automated Information Systems”
- Agency directives

Security Objectives



CONFIDENTIALITY

“Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information...”

A loss of *confidentiality* is the unauthorized disclosure of information.

INTEGRITY

“Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity...”

A loss of *integrity* is the unauthorized modification or destruction of information.

AVAILABILITY

“Ensuring timely and reliable access to and use of information...”

A loss of *availability* is the disruption of access to or use of information or an information system.

Adequate Security



- Security **commensurate with the risk** and the magnitude of harm resulting from the loss, misuse, or unauthorized access to or modification of information.



- This includes **assuring** that systems and applications used by the agency **operate effectively and provide appropriate confidentiality, integrity, and availability**, through the use of cost-effective management, personnel, operational, and technical controls.

Information Security Paradigm Shift



From...

Policy-based Compliance

- Policy dictates discrete, predefined information security requirements and associated safeguards/countermeasures
- Allows minimal flexibility in implementation
- Little emphasis on explicit acceptance of mission risk



Snapshot

...To

Risk-based Protection

- Enterprise missions and business functions drive security requirements and associated safeguards/countermeasures
- Highly flexible in implementation
- Focuses on acknowledgement and acceptance of mission risk



"Build It Right" Strategy

Continuous Monitoring



Assessment

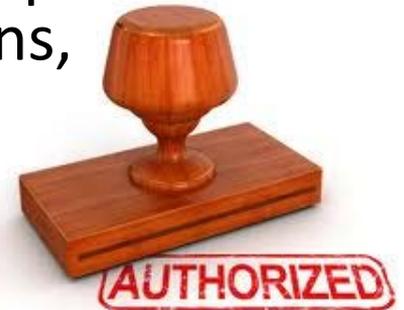


- Process of determining how effectively an entity being assessed (the assessment **object**: e.g., host, system, network, procedure, person) meets **specific security objectives**.
- Comprehensive testing of the **security controls** in an information system to ascertain system **vulnerabilities** and the **risk** associated with system authorization.

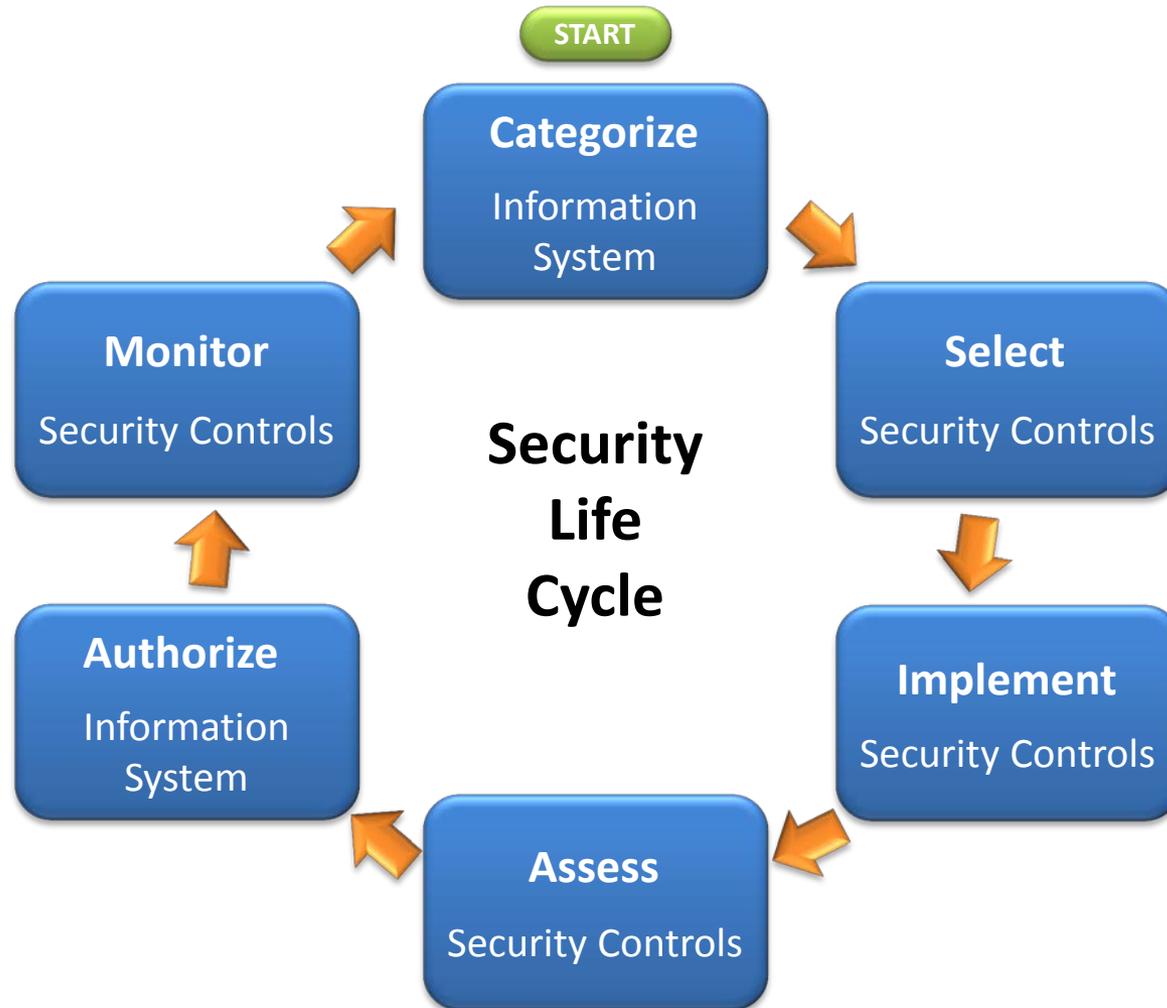
Authorization



- The official management decision given by a senior organizational official
 - Authorizes operation of an information system
 - Explicitly **accepts the risk** to organizational operations and assets, individuals, or other organizations, based on the implementation of an **agreed-upon set of security controls.**
- Ensures
 - Adequate countermeasures and mitigating factors are **in place**
 - Adequate countermeasures and mitigating factors are **operating** as intended
 - Risk level is **understood** and **thoroughly documented.**



Risk Management Framework



Security Categorization



Security Objective	POTENTIAL IMPACT		
	LOW	MODERATE	HIGH
Confidentiality	The unauthorized disclosure of information could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized disclosure of information could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized disclosure of information could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals.
Integrity	The unauthorized modification or destruction of information could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized modification or destruction of information could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized modification or destruction of information could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals.
Availability	The disruption of access to or use of information or an information system could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals.	The disruption of access to or use of information or an information system could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals.	The disruption of access to or use of information or an information system could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals.

Security Controls



For *low-impact* information systems

organizations must, as a minimum, employ appropriately tailored security controls from the **low baseline** of security controls defined in NIST SP 800-53 and must ensure that the minimum assurance requirements associated with the low baseline are satisfied.

For *moderate-impact* information systems

organizations must, as a minimum, employ appropriately tailored security controls from the **moderate baseline** of security controls defined in NIST SP 800-53 and must ensure that the minimum assurance requirements associated with the moderate baseline are satisfied.

For *high-impact* information systems

organizations must, as a minimum, employ appropriately tailored security controls from the **high baseline** of security controls defined in NIST SP 800-53 and must ensure that the minimum assurance requirements associated with the high baseline are satisfied.

Organizations must employ all security controls in the respective security control baselines unless specific exceptions are allowed based on the tailoring guidance provided in NIST SP 800-53.

Security Control Selection

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

TABLE D-2: SECURITY CONTROL BASELINES⁹²

CNTL NO.	CONTROL NAME	PRIORITY	INITIAL CONTROL BASELINES		
			LOW	MOD	HIGH
Access Control					
AC-1	Access Control Policy and Procedures	P1	AC-1	AC-1	AC-1
AC-2	Account Management	P1	AC-2	AC-2 (1) (2) (3) (4)	AC-2 (1) (2) (3) (4) (5) (11) (12) (13)
AC-3	Access Enforcement	P1	AC-3	AC-3	AC-3
AC-4	Information Flow Enforcement	P1	Not Selected	AC-4	AC-4
AC-5	Separation of Duties	P1	Not Selected	AC-5	AC-5
AC-6	Least Privilege	P1	Not Selected	AC-6 (1) (2) (5) (9) (10)	AC-6 (1) (2) (3) (5) (9) (10)
AC-7	Unsuccessful Logon Attempts	P2	AC-7	AC-7	AC-7
AC-8	System Use Notification	P1	AC-8	AC-8	AC-8

Development / Acquisition

Initiation

Implementation

O&M

Step 1
CATEGORIZE
Information System

Step 2
SELECT
Security Controls

Step 3
IMPLEMENT
Security Controls

Step 4
ASSESS
Security Controls

Step 5
AUTHORIZE
Information System

Step 6
MONITOR
Security Controls

1. Categorize information system (IS) and document in security plan
2. Describe IS and system boundary in security plan
3. Register IS

1. Identify common security controls
2. Select IS security controls and document in security plan
3. Develop strategy for continuous monitoring of security control effectiveness
4. Review and approve security plan

1. Implement security controls specified in security plan
2. Document security control implementation, planned inputs, expected behavior, expected outputs

1. Develop, review, and approve a plan to assess security controls
2. Assess security controls using security assessment plan
3. Prepare security assessment report
4. Conduct remediation based on report findings; reassess

1. Prepare POA&M
2. Assemble security authorization package and submit to AO
3. Determine risk
4. Determine if risk is acceptable

RMF Tasks

- Information System Owner
- Information Owner
- Risk Executive
- CIO
- AO
- ISSO

- CIO
- Information Security Architect
- Information System Owner
- AO
- Risk Executive
- ISSO
- ISSE

- Information System Owner
- Information Owner
- ISSO
- ISSE

- Security Control Assessor
- AO
- CIO
- IS Owner
- Info Owner
- ISSO
- ISSE

- Information System Owner
- AO
- Info Owner
- ISSO
- Security Control Assessor
- Risk Executive

RMF Roles

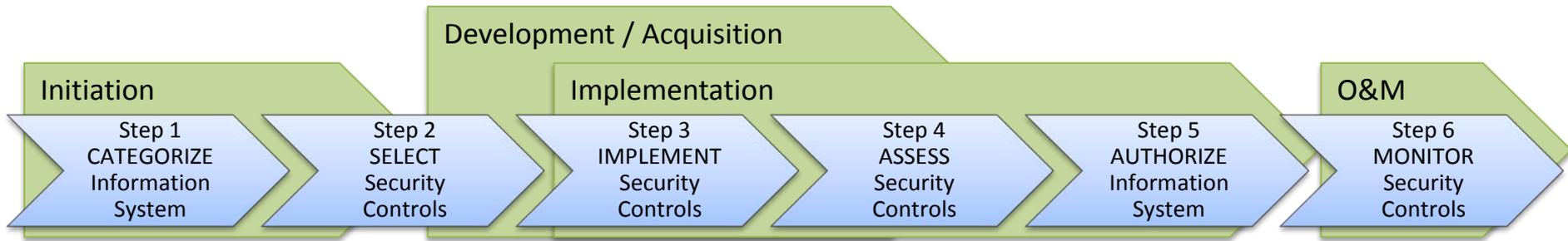
IV&V Security Analysis



- IEEE 1012-2012, Standard for System and Software Verification and Validation
 - Security Analysis throughout
 - “to verify that the system-required threat controls and safeguards are correctly implemented and to validate that they provide the desired levels of protection of system vulnerabilities.”
- IVV 09-1
 - 2.0 Verify and Validate Concept Documentation
 - 2.6 Ensure that security threats and risks are known and documented and that relevant regulatory requirements are identified.

Specific V&V activities that may be appropriate for “critical” security requirements necessary to control threats and exposure to vulnerabilities may include the following activities:

- a) **Traceability** of critical requirements through the life cycle to verify implementation.
- b) Evaluation of potential threat sources and vulnerabilities to validate that critical security requirements are **complete** and are appropriate for the system operational need.
- c) Evaluation of **architectures and designs** to determine whether security functions meet required capabilities, whether additional threat controls are needed, and whether design changes are needed to remove vulnerabilities.
- d) Application of **verification methods** (analyses, inspections, demonstrations, or tests) that are intended to determine whether plausible threats can exploit vulnerabilities. These verification methods may include the following:
 - 1) Statistical analyses to determine whether the probability of breaching a security control is within acceptable levels. This may include **simulations** or mathematical models (e.g., for encryption methods).
 - 2) **Inspections** to verify that security controls are implemented as specified. This may also include inspections that regulatory or policy standards have been followed.
 - 3) **Demonstrations** in an operational setting to show that security controls are reasonable and effective.
 - 4) Tests to verify that specific security controls (physical, procedural, and automated controls) cannot be breached. For IT systems, this may also include **vulnerability scanning and penetration testing**.



IV&V 09-1 Technical Framework

1.0 Management and Planning

2.0 Verify and Validate Concept Documentation

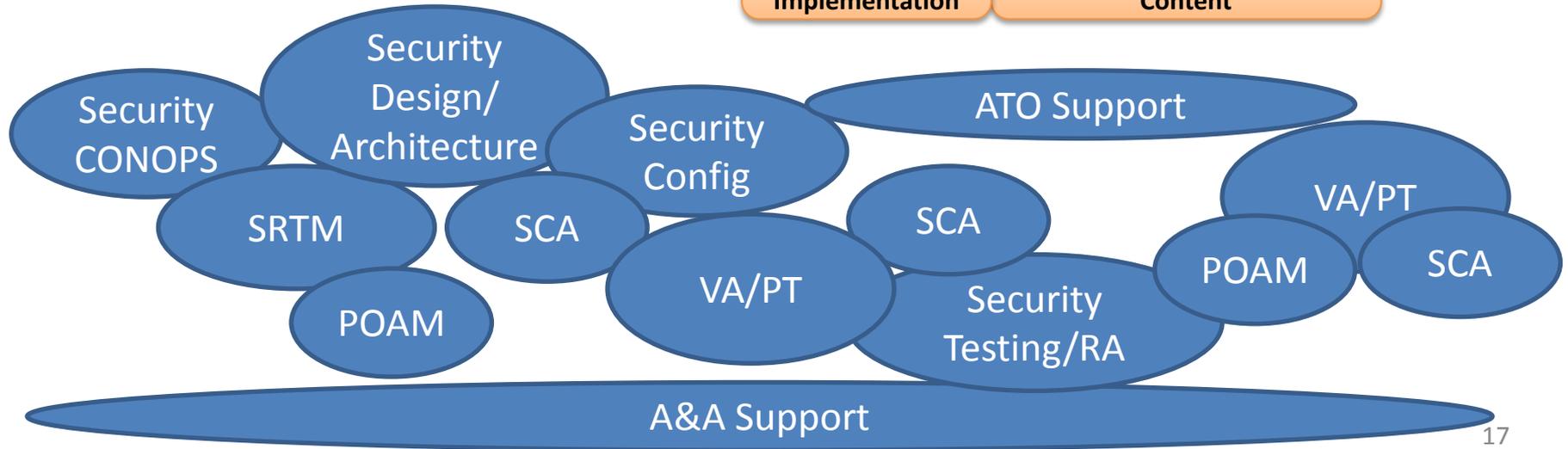
3.0 Verify and Validate Requirements

4.0 Verify and Validate Test Documentation

5.0 Verify and Validate Design

6.0 Verify and Validate Implementation

7.0 Verify and Validate Operations and Maintenance Content



Methods



Step 1
CATEGORIZE
Information System

**Validate System Security Categorization and
Regulatory Security Requirements by Inspection**

FIPS 199
SP 800-60



Step 2
SELECT
Security Controls

**Verify Security Control Selection and Threats/Risks
Identification by Inspection**

FIPS 200
SP 800-53



Step 3
IMPLEMENT
Security Controls

**Verify Security Control Implementation by
Inspection**

SP 800-70



Step 4
ASSESS
Security Controls

Verify Security Remediation Actions by Inspection

SP 800-53A
SP 800-115



Step 5
AUTHORIZE
Information System

**Verify Security Risk Action Plan before Operations
by Inspection**

SP 800-37



Step 6
MONITOR
Security Controls

Vulnerability Assessments / Penetration Testing

SP 800-37
SP 800-53A
SP 800-137

IA Services Implementation



What



When



Where



Who



How



Why



- *Safety and Mission Assurance*
- *Software Engineering*
- *CIO*
- *Missions*

Inspiration



NIST Wants Developers of Critical Systems to Consider Security From the Start

The US National Institute of Standards and Technology (NIST) wants developers of critical systems to **build security into their products “from the ground up.”** The voluntary guidelines are intended to be a roadmap for IT management responsible for securing systems that underlie the country’s critical infrastructure. The 121-page draft document describes 11 core technological processes in systems and software development. The draft is open to public comment through July 11, 2014. One of the document’s co-authors describes it as “a disciplined and structured process to show how ... security actually does get baked into the process.”

– SANS NewsBites Vol. 16 Num. 039

“I applaud the attempt to shift attention from the component-level to the system-level and move the consideration of... threats to the earliest stage (design requirements) in the lifecycle. ...**organizations remain ill-equipped** to implement what is suggested [in SP 800-160].”

– SANS NewsBites Editor