IVV 09-1: Independent Verification and Validation Technical Framework

Version: P

Effective Date: February 26, 2016

Note: The official version of this document is maintained in IV&V's internal IV&V Management System Website (https://confluence.ivv.nasa.gov:8445/display/IMS). This document is uncontrolled when printed.

Purpose

The purpose of this system level procedure (SLP) is to establish a consistent method for providing IV&V technical services to customers, sufficient to ensure safety and risk mitigation for the successful deployment of software-intensive systems.

Scope

This SLP is applicable to IV&V technical activities provided by the NASA IV&V Program.

Definitions and Acronyms

Official NASA IV&V roles and terms are defined in the Quality Manual. Specialized definitions identified in this SLP are defined below. Additional technical definitions may be found in IEEE Standard 1012-2012, or in NIST-SP 800-53A.

- **Acquirer**
  - The acquirer is the entity or individual who specifies the requirements and accepts the resulting software products. The acquirer is usually NASA or an organization within the Agency but can also refer to the Prime contractor – subcontractor relationship as well.
- **Availability**
  - The information assurance property of availability is defined as ensuring timely and reliable access to and the use of information. [44 U.S.C., Sec. 3542]
- **Confidentiality**
  - The information assurance property of confidentiality is defined as preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information. [44 U.S.C., Sec. 3542]
- **Integrity**
  - The information assurance property of integrity is defined as guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity. [44 U.S.C., Sec. 3542]
- **Mission Project**
  - A Mission Project is a NASA development project (or other development project) that is the recipient of IV&V technical services as defined in a Formal Agreement (FA).
- **Security**
  - Security - **(A)** The protection of computer hardware or software from accidental or malicious access, use, modification, destruction, or disclosure. Security also pertains to personnel, data, communications, and the physical protection of computer installations. **(B)** The protection of information and data so that unauthorized persons or systems cannot read or modify them and authorized persons or systems are not denied access to them.
- **System**
  - A system is a group of interacting, interrelated, and/or interdependent software and/or hardware elements that form a complex whole that accomplishes defined objectives.
- **System Behavior or Behavior**
  - System behavior, or behavior, is the collective response of a system as it reacts to external and internal stimuli. System behavior can be either planned behaviors or unplanned, emergent, behaviors.
- **Validation[1]**
  - Validation is **(A)** The process of evaluating a system or component during or at the end of the development process to determine whether it satisfies specified requirements. **(B)** The process of providing evidence that the system, software, or hardware and its associated products satisfy requirements allocated to it at the end of each life cycle activity, solve the right problem (e.g., correctly model physical laws, implement business rules, use the proper system assumptions), and satisfy intended use and user needs.
- **Verification[1]**
  - Verification is **(A)** The process of evaluating a system or component to determine whether the products of a given development phase satisfy the conditions imposed at the start of that

phase. **(B)** The process of providing objective evidence that the system, software, or hardware and its associated products conform to requirements (e.g., for correctness, completeness, consistency, and accuracy) for all life cycle activities during each life cycle process (acquisition, supply, development, operation, and maintenance); satisfy standards, practices, and conventions during life cycle processes; and successfully complete each life cycle activity and satisfy all the criteria for initiating succeeding life cycle activities (e.g., building the software correctly).

---

[1] As defined in IEEE Std 1012/D15

Acronyms

CDR	Critical Design Review
FA	Formal Agreement
FedRAMP	Federal Risk and Authorization Management Program
FIPS	Federal Information Processing Standards
FISMA	Federal Information Security Modernization Act of 2014
IA	Independent Assessment
IA	Information Assurance
IDD	Interface Design Document
IEEE	Institute of Electrical and Electronics Engineers
IMS	IV&V Management System
IPEP	IV&V Project Execution Plan
IRS	Interface Requirements Specification
IV&V	Independent Verification & Validation
KDP	Key Decision Point
NIST	National Institute of Standards and Technology
NODIS	NASA Online Directives Information System
NPR	NASA Procedural Requirements

PBRA	Portfolio Based Risk Assessment
PDR	Preliminary Design Review
QM	Quality Manual
RBA	Risk Based Assessment
SDD	Software Design Document
SLP	System Level Procedure
SP	Special Publication
SRS	Software Requirements Specification
STD	Standard
TIM	Technical Issue Memorandum
TQ&E	Technical Quality & Excellence
U.S.C.	United States Code
WBS	Work Breakdown Structure

Process Flow Diagram

A process flow diagram does not apply to this SLP; however, the following paragraphs elaborate upon IV&V work performed by the NASA IV&V Program.

General Guidance

IV&V, as a part of Software Assurance, plays a role in the overall NASA software risk mitigation strategy applied throughout the lifecycle, to improve the safety, security, and quality of software systems and ensure the integrity, confidentiality and availability of data at rest and in transit of software systems. For additional information regarding software assurance and software safety within NASA, see NASA-STD-8739.8, *Software Assurance Standard*, and NASA-STD-8719.13C, *Software Safety Standard*.

It is recommended that IV&V managers and practitioners read NASA Procedural Requirement (NPR) 7150.2, *NASA Software Engineering Requirements*. The content in NPR 7150.2 will help IV&V personnel establish expectations of what is required of the Mission Project during NASA software development. This includes requirements for software management (including management of safety-critical software), software artifact content, and software engineering across the software lifecycle. Additional details about the requirements for technical reviews (i.e., milestone reviews) can be found in NPR 7123.1B, *NASA Systems Engineering Processes and Requirements*.

It is also recommended that IV&V managers and practitioners read the front matter contained in IEEE Std 1012- 2012 (which will be referred to as "IEEE 1012" for the remainder of this SLP). While the focus of IEEE 1012 is V&V and not specifically IV&V, many of the concepts and points of emphasis are applicable to IV&V and warrant understanding.

Finally, IV&V managers and practitioners are encouraged to review the relevant sections of the Reference Documents as they provide additional context and guidance relevant to the IV&V Technical Framework. With the inclusion of additional Information Assurance requirements in Version P, users of this document are encouraged to review NPR 2810.1A "Security of Information Technology" particularly when access to sensitive or classified data is necessary.

Key Concepts

The following key concepts should always be considered when performing IV&V:

1. *It is important to examine the software in its interactions with the system of which it is a part**[2]***. It is therefore necessary to develop an understanding of the system, system goals, and operational environment. This system understanding represents the IV&V Project's technical reference and should be documented and maintained for usage throughout the IV&V Project lifecycle. Additional views on software and its interactions can be found in Section 1.3 of IEEE 1012 and include environment, operators/users, hardware, and other software.
2. *There are certain perspectives that should be considered during all IV&V analysis.* IEEE 1012 refers to these perspectives as "analysis across all normal and abnormal system operating conditions," and states that "the dynamics of software and the multitude of different logic paths available within software in response to varying system stimuli and conditions demand that the software V&V effort examine the correctness of the code for each possible variation in system conditions." These perspectives may also take the form of the following questions:

    1. Will the system's software do what it is supposed to do?
    2. Will the system's software not do what it is not supposed to do?
    3. Will the system's software respond as expected under adverse conditions?

    The intensity and rigor[3] with which these perspectives are addressed may vary depending on criticality of software or other system/software characteristics.

3. *It is important to recognize that requirements cannot be evaluated in isolation.* Requirements must be evaluated as a set in order to determine that a particular goal, behavior, or attribute of the system/software is being met. The same is true for design elements, code modules, security[4], etc.

4. *When a task completes, consider effects on previous analysis results.* "Results and findings from one V&V task may cause previously completed V&V tasks to be analyzed again with the new data."[4] This is also true for the assessment of the system and software security components in terms of the risks and security threats to the software system.

5. *Throughout all IV&V analysis, the content under evaluation should be related back to acquirer needs, system goals, and information security to ensure that they will be met.* Specific IV&V tasks may require relating the content under evaluation to other information (e.g. higher level requirements,

design elements, etc.). In addition to the task-specific goals and criteria, acquirer needs and system goals should always be considered.

6. *Always focus on the goal of the task and higher level goals of the IV&V Project.* The Technical Framework contained below in Section 4.3 (Table 1) is organized according to IV&V goals (or objectives).[5] IV&V tasks and approaches should be chosen to meet these objectives as they apply to a particular IV&V Project. Some of the objectives in the Technical Framework may not be applicable or feasible for a particular IV&V Project due to mission characteristics, IV&V Project characteristics, etc. In all cases, when planning and executing an IV&V task, ensure the objective of the task and any higher level objectives are met with respect to key concepts provided above.

---

[2] IEEE Std 1012-2012
[3] IEEE Std 1012-2012. "Intensity includes greater scope of analysis across all normal and abnormal system operating conditions. Rigor includes more formal techniques and recording procedures."
[4] For example, security is a key characteristic or attribute of the system/software and its assurance is governed by federal guidelines such as Federal Information Processing Standards (FIPS)-199 and Federal Information Security Modernization Act (FISMA) of 2014. There is a system security categorization determined by criteria in FIPS-199 and the required robustness of controls to protect Federal information and information systems are covered by FISMA 2014. Both are important concepts to understand relative to the planning for IV&V information assurance analyses and the execution of those IV&V tasks. There are additional federal guidelines (e.g. Federal Risk and Authorization Management Program [FedRAMP]) for cloud computing which are applicable to systems that employ the cloud solution within the system.
[5] For the purposes of this SLP, no distinction between "goal" and "objective" is intended.

NASA Software IV&V Technical Framework

Table 1, below, describes the NASA Software IV&V Technical Framework[6] (or "framework") used by the NASA IV&V Program to support IV&V project analysis activities. The key concepts mentioned above should always be considered when performing IV&V. Activities performed for individual IV&V Projects shall be defined in the associated IV&V Project Execution Plan (IPEP).

Organization of the Framework

The framework, contained in Table 1, is organized according to IV&V goals (or objectives)[7], and is intended to serve as a basis for determining specific objectives for a particular IV&V Project and for selecting IV&V tasks and approaches to meet those objectives (see Key Concept 4.2.6 above). IV&V tasks and approaches are maintained outside of this SLP, with the exception of the tasks under 1.0 Management and Planning.

Due to the goal-based organization of the framework (rather than a phase-based organization), tasks that support multiple goals may be executed concurrently, depending on the characteristics of the IV&V Project and associated Mission Project.

---

[6] This framework is commonly referred to as “the WBS” (work breakdown structure). While the content of the framework may or may not match what would be recognized as a WBS based on common guidance (e.g. the Project Management Body of Knowledge), this type of content meets NASA IV&V needs for defining work, and has come to be known as “the WBS”.
[7] For the purposes of this SLP, no distinction between “goal” and “objective” is intended.

Table 1: NASA Software IV&V Technical Framework

1.0 Management and Planning		
Management of the IV&V effort is performed for all applicable software development lifecycle processes and activities. This involves the following: • A continual review of the IV&V effort • Revision of the IPEP as necessary based upon updated Mission Project schedules and development status • Coordination of the IV&V results with the developer and other appropriate management groups • Promotion of technical exchange between IV&V and the developer (to improve technical knowledge transfer and increase IV&V effectiveness) • Identification of process improvement opportunities in the conduct of IV&V IV&V management assesses proposed changes to the system, software, and security and adjusts IV&V plans accordingly. For such changes, if any new hazards, security threats, or risks are introduced in the software or system development process, it is necessary to identify the impact of the change on established IV&V priorities (i.e. PBRA/RBA output). IV&V task planning is revised by adding or removing IV&V objectives and/or associated tasks or changing the scope or intensity and rigor of existing IV&V tasks. Note: In the event of a discrepancy between the content in this section and IVV 09-4, *Project Management*, IVV 09-4 takes precedence.		
Management and Planning of Independent Verification and Validation	1.1	A) Goal: The goal of this task is to establish, document, communicate, and maintain the infrastructure necessary for effective and efficient direction of the IV&V Project’s management and technical analysis efforts on behalf of the IV&V Project’s customers.

B) Task Description: Generate an IV&V Project Execution Plan (IPEP) for all lifecycle processes using T2103, *IPEP Template*. The IPEP may require updating throughout the lifecycle. Outputs of several other activities are inputs to the IPEP, and the IPEP should be updated when these inputs become available. Identify Mission Project milestones in the IPEP. Schedule IV&V tasks to support Mission Project management reviews and technical reviews. Plan the interface and rules of engagement among the IV&V effort, the Mission Project office, and the software developer. Document the data exchange requirements in the IPEP. Consider IV&V access to appropriate Mission Project artifact management systems, issue and risk tracking systems, etc. Conduct a heritage review to identify relevant products and artifacts from heritage projects that may be applicable to the current project. Document the heritage review results in the IPEP; and revisit when indicators suggest new information should be considered or previous results may be affected.

Identify specific training needs for analysts and other IV&V project members; such training may be oriented to NASA standards and requirements, analysis processes and tools, or mission specific knowledge. Identify the source of the training (including piggy-backing on the mission project or other IV&V projects), timing, and participants. Specific clearances and training is required for handling classified data. Identification of the necessary training, as well as identifying clearance requirements, should be identified as early as possible due to the time required to complete.

Plan the IV&V Project schedule for each IV&V task. Identify the preliminary list of development processes and products to be evaluated by the relevant IV&V processes. Describe IV&V access rights to proprietary and classified information and the process to secure and document those rights. The plan should be coordinated with the developer of the software, which may include not only NASA, but also developers contracted to NASA. Incorporate the project software integrity level scheme (per the approved Risk Based Analysis process [PBRA]) into the planning process.

During IV&V Project execution, review and summarize the IV&V effort to define changes to IV&V tasks or to redirect the IV&V effort. Recommend whether to proceed to the next set of IV&V and development life cycle activities, and provide task reports, anomaly reports, and IV&V Activity Summary Reports to the organization(s) identified in the IPEP. Ensure that the IV&V team provides input to the appropriate software assurance personnel and provide feedback to the Mission Project as identified in the IPEP.

Verify that all IV&V tasks comply with task requirements defined in the IPEP. Verify that IV&V task results have a basis of evidence supporting the results. Assess all IV&V results and provide recommendations for input to or inclusion in the IV&V Project Final Report. The management review of IV&V may use any review methodology such as what is provided in IEEE Std 1028 - 2008.

		Evaluate proposed changes to the Mission Project (e.g., anomaly corrections and system, software and security requirements changes) for effects on previously completed IV&V tasks and future IV&V tasks. Verify that the change is consistent with system requirements, federal regulations and compliance, and does not adversely affect other requirements directly or indirectly. An adverse effect is a change that could create new system hazards, create security vulnerabilities, and risks or impact previously resolved hazards and risks. Plan iteration of affected tasks or initiate new tasks to address the software change or iterative development process. Coordinate the IV&V effort with appropriate organizational groups (e.g., management, support functions).
Issue and Risk Tracking	1.2	A) Goal: Identify and communicate factors that are likely to impact IV&V or Mission Project objectives in the areas of performance (quality), safety, security, schedule, and cost. B) Task Description: Track IV&V-generated issues from initiation through closure by the Mission Project and/or IV&V. Issue writing guidelines are maintained by IV&V and act as a guide for writing high-quality issues (S3105, *Guidelines for Writing IV&V TIMs*). All Severity 1 and 2 issues receive an extra level of internal peer review prior to submission to the Mission Project. Identify and track IV&V Project risks and Mission risks. Provide recommendations to mitigate these risks. Risks are managed according to IVV 22, *Risk Management*. Communicate the issues and risks to the appropriate IV&V and Mission Project management utilizing the guidance provided in the referenced IV&V documents.
IV&V Project Closeout	1.3	A) Goal: The goal of this task is to document the performance of all phases of the IV&V Project in an IV&V Project Final Report and to prepare all appropriate documentation for archival and support of future IV&V Heritage Reviews. B) Task Description: Perform an orderly closeout of the IV&V Project, consisting of the following activities: 1. Develop an IV&V Project Final Report as defined in IVV 09-4, *Project Management*. 2. Record any additional IV&V Project-level lessons learned in the NASA IV&V Lessons Learned database. 3. Record any additional IV&V Project-level success stories in the NASA IV&V Success Stories database. 4. Compile all of the IV&V Project work products to support future IV&V Heritage Reviews. 5. Manage the proper disposition of Mission Project artifacts and coordinate with the Records Custodian. 6. Report final effort data for use in IV&V effort estimation or metrics activities.

Management and Technical Review Support	1.4	A) Goal: The goal of this task is to provide the Mission Project an independent evaluation of the lifecycle review artifacts to assist development management decisions on whether the review criteria have been met and how to proceed going forward. B) Task Description: Support Mission Project management reviews and technical reviews (e.g., PDR and CDR) by assessing the review materials, attending the reviews, providing requested status and/or data to the Mission Project, presenting at the reviews, performing an evaluation of the project's fulfillment of the review entrance and exit criteria, and providing task reports and anomaly reports (when appropriate). These reports as a minimum identify any high severity issues, whether technical artifacts have met milestone criteria, and recommended actions going forward. Work performed in support of this task should relate to the critical areas of the system that are within the scope of IV&V, as determined by the Criticality Analysis performed on the particular IV&V Project. The management and technical review support may also use any review methodology such as what is provided in IEEE Std 1028 - 2008.
Criticality Analysis	1.5	A) Goal: The goal is to identify the most critical areas of the system, which serve as a basis for establishing the IV&V focus. This task assists in the planning and scoping of the IV&V analysis and will be performed iteratively during the IV&V Project lifecycle. B) Task Description: The NASA IV&V process for performing this assessment can be found in S3106, *PBRA and RBA Process*. This risk-based approach implies the use of two attributes: Impact and Likelihood.
Identify Process Improvement Opportunities in the Conduct of IV&V	1.6	A) Goal: Perform continuous improvement of IV&V processes. B) Task Description: Gather and analyze lessons learned (following IVV 23, *Less ons Learned*), Success Stories (following IVV 24, *Success Stories*), and IV&V metrics on a periodic basis at no less frequency than every six months or following the completion of a Mission Project milestone. Identify and document any deficiencies in the IV&V process when these deficiencies become evident and implement appropriate corrective action(s) following IVV 14, *Corrective and Preventive Action*, as appropriate. Monitor the effectiveness of the corrective actions being taken. Determine if the corrective actions should be incorporated into the IV&V processes. Document findings in appropriate technical reports. Collect and monitor effort data for use in calibrating effort models. Support internal IV&V Project reviews and knowledge sharing events (e.g. TQ&E Checkpoint Reviews and Technical Discussions).
2.0 Verify and Validate Concept Documentation		

Concept documentation represents the delineation of a specific implementation solution to solve the acquirer's problem. The objective of Concept IV&V is to validate the selected solution and ensure that no false assumptions have been incorporated in the solution. Additional objectives:

2.1 Ensure that software planned for reuse meets the fit, form, and function, and security as a component within the new application.

2.2 Ensure that the system architecture contains the necessary computing related items (subsystems, components, etc.) to carry out the mission of the system and satisfy user needs and operational scenarios or use cases.

2.3 Ensure that the concepts for the operations, mission objectives (including mission retirement), and the system are sufficiently defined as a basis for the engineering and planning of computing related functions.

2.4 Ensure that feasibility studies provide the results necessary to confidently support the key decisions that drove the need for the study.

2.5 Ensure that known software based hazard causes, contributors, and controls are identified and documented.

2.6 Ensure that security threats and risks are known, up to date, appropriately documented, and are correct for this mission and that relevant regulatory requirements are identified.

2.7 Ensure that appropriate plans are in place to update the security threats and risks over the course of the development lifecycle to allow for introduction of new or changing threats, and are consistent with project data categorization (e.g. FIPS).

2.8 Ensure the security risks introduced by the system itself, as well as those associated with the environment with which the system interfaces, are appropriately accounted for in the known threats.

2.9 Ensure the system concept from a security perspective and assure that potential security risks with respect to confidentiality (disclosure of sensitive information/data), integrity (modification of information/data), availability (withholding of information or services), and accountability (attributing actions to an individual/ process) have been identified. Include an assessment of the sensitivity of the information/data to be processed and assessment of its consistency with FIPS categorization.

3.0 Verify and Validate Requirements

Requirements IV&V addresses a system's software requirements including analysis of the functional and performance requirements, interfaces external to the software, and requirements for qualification, safety and security, dependability, human factors engineering, data definitions, user documentation for the software, installation and acceptance, user operation and execution, and user maintenance. The objective of Requirements IV&V is to ensure the system's software requirements are high quality (correct, consistent, complete, accurate, unambiguous, and verifiable), and will adequately meet the needs of the system and expectations of its customers and users, considering its operational environment under nominal and off-nominal conditions, and that no unintended features are introduced (see Key Concepts 4.2.1 and 4.2.2, above). Additional objectives:

3.1 Ensure that the system requirements are of high quality and are consistent with acquirer needs as they relate to the system's software.

3.2 Ensure that all (in-scope) parent requirements are represented in the appropriate child requirements and that the child requirements do not introduce capability that is not required.

3.3 Ensure that the software requirements are of high quality and adequately meet the needs of the system with respect to expectations of its customer and users, operational environment, and both functional and non-functional perspectives.

3.4 Ensure that the requirements for software interfaces with hardware, user, operator, and other systems are adequate to meet the needs of the system with respect to expectations of its customer and users, operational environment, dependability and fault tolerance, and both functional and non-functional perspectives.

3.5 Ensure that software requirements meet the dependability and fault tolerance required by the system and provide the capability of controlling identified hazards and do not create hazardous conditions.

3.6 Ensure that the requirements address the security threats and risks identified within the system concept specifications and/or the system security concept of operations (e.g. System Security Plan).

3.7 Ensure that requirements define appropriate security controls to the system, subsystem, according to NPR 2810 and driven by the Project's security needs and requirements.

NASA Missions go through a logical decomposition in defining their requirements. Each IV&V Project needs to identify how its Mission's requirements are decomposed and which levels of decomposition warrant IV&V analysis in order to meet the objectives of the IV&V Project.

4.0 Verify and Validate Test Documentation

Test Content IV&V addresses test plans, procedures, cases, and designs. The objective is to ensure that the collection of test related content will serve as a sufficient means to verify and validate that the implementation meets the requirements and operational need under nominal and off-nominal conditions (see Key Concepts 4.2.1 and 4.2.2 above).

Test content should be evaluated for requirements coverage and test completeness, considering the extent of the software exercised, the appropriateness of the verification method (e.g. test, analysis, demonstration, inspection), whether the set of inputs used during testing are a fair representative sample from the set of all possible inputs to the software, and whether test inputs include boundary condition inputs, rarely encountered inputs, invalid inputs, inputs related to identified hazards, safety and security of the software and system. Additional objectives:

4.1 Ensure that the planned tests are sufficient to:

4.1.1 Ensure that the software correctly implements system, software, and security requirements in an operational environment under nominal and off-nominal conditions.

4.1.2 Ensure that the complete, integrated system complies with its specified system requirements allocated to software and to validate whether the system meets its original objectives.

4.1.3 Ensure that the software meets all of the (in-scope) software requirements and is ready to be integrated with system hardware.

4.1.4 Ensure that the software correctly and securely implements the software requirements and design as each software component (e.g., units or modules) is incrementally integrated with each other.

4.1.5 Ensure that the software components (e.g., units, source code modules) correctly implement software component requirements.

4.2 Ensure that valid relationships are defined between the Test Plans, Designs, Cases, and Procedures for test types and documents subject to IV&V test analysis.

4.3 Ensure that the planned regression testing to be performed when changes are made to any previously examined software products is sufficient to identify any unintended side effects or impacts of the change on other aspects of the system (including not increasing the security risk).

4.4 Ensure that any simulations are sufficiently complete, correct, and accurate to perform the intended testing.

4.5 Ensure that the Test Cases under analysis:

4.5.1 Specify the correct test inputs, predicted results, and sets of execution conditions necessary to satisfy their intended test objectives (covering both nominal and off-nominal conditions)

4.5.2 Verify specific security controls (physical, procedural and automated controls) cannot be breached leading to compromise of information confidentiality, integrity, or availability.

4.6 Ensure that the Test Procedures under analysis specify the correct sequence of actions necessary for the execution of the tests to satisfy their intended test objectives.

4.7 Ensure that the Test Designs under analysis correctly specify the details of the test approach for the covered software feature or combination of software features and identify the associated tests.

4.8 Ensure that the test environment is sufficiently complete, correct, and accurate to perform the intended testing.

4.9 Ensure that the integrated system testing covers any areas that may potentially increase the security risk,

NASA Missions may use different terminology in defining their test content. Each IV&V Project needs to understand how its Mission's test content is being developed and plan accordingly. Also, because test cases, procedures, and designs may be developed iteratively and at multiple levels, IV&V task iteration may be necessary. For example, test cases may be written at the unit level (4.1.5), integration level (4.1.4), and qualification level (4.1.3), meaning that objective 4.5 may need to be met for each of these levels of testing.

Note: Test results evaluation is included below in 6.0, *Verify and Validate Implementation*.

5.0 Verify and Validate Design

In software design, software requirements are transformed into an architecture and a detailed design for each software component. The design also includes databases and system interfaces (e.g., hardware, operator/user, software components, and subsystems). Design IV&V addresses software architectural design and software detailed design. The objective of Design IV&V is to ensure that the design is a correct, accurate, and complete transformation of the software requirements that will meet the operational need under nominal and off-nominal conditions, that no unintended features are introduced, and that design choices do not result in unacceptable operational risk (see Key Concepts 4.2.1 and 4.2.2 above). Additional objectives:

5.1 Ensure that all (in-scope) requirements (e.g. SRS and IRS) are represented in the appropriate elements of the design (e.g. SDD and IDD) and that the design does not introduce capability that is not required.

5.2 Ensure that the design provides the required capability (meeting software architecture, software security, and software requirements), is able to reliably meet user needs, and is sufficiently stable to proceed with implementation.

5.3 Ensure that the proposed software architecture satisfies the needs of the system, and that it is a feasible solution (i.e. will successfully satisfy the needs of the system, while still being practical).

5.4 Ensure that the internal and external software interface designs are provided for all (in-scope) interfaces with hardware, user, operator, software, and other systems and that they provide sufficient detail to enable the development of software components that implement the interfaces.

5.5 Ensure that complex algorithms have been correctly derived, provide the needed behavior under off nominal conditions and assumed conditions, and that the derivation approach is known and understood to support future maintenance.

5.6 Ensure that the design provides the dependability and fault tolerance required by the system and that the design is capable of controlling identified hazards and does not create hazardous conditions.

5.7 Ensure that the architecture and detailed design adequately address the identified security requirements both for the system and security risks, including the integration with external components and information and data utilized, stored, and transmitted through the system.

5.8 Ensure that identified security threats and vulnerabilities are prevented, controlled, or mitigated via proposed design components. Any unmitigated threats and vulnerabilities are documented and addressed as part of the system and software operations.

6.0 Verify and Validate Implementation

In software implementation, the design is transformed into code, database structures, and related machine executable representations. The objective of Implementation IV&V is to verify and validate that these transformations are correct, accurate, and complete, yielding source code that correctly implements requirements, meets the operational need under nominal and off-nominal conditions, and introduces no unintended features (see Key Concepts 4.2.1 and 4.2.2 above). Implementation IV&V also seeks to ensure that the source code and documentation (both embedded and stand-alone) are complete and provide an adequate reference for source code maintainability and upgrade. Additional objectives:

6.1 Ensure that all (in-scope) elements of the design (e.g. SDD and IDD) are represented in the appropriate source code components and that the source code does not introduce capability that is not required.

> 6.1.1 Ensure that the implementation adheres to the system and software design in that it addresses the identified security risks and that the implementation does not introduce new security risks through specific code constructs, features, or coding flaws (e.g. Common Weakness Enumerations).

6.2 Ensure that the source code components can reliably perform required capabilities under nominal and off-nominal conditions, perform no undesired behaviors, and that the documentation (both embedded and stand-alone) can facilitate code maintenance.

6.3 Ensure that the source code that interfaces with hardware, user, operator, software, and other systems reliably provides the right services and data and receives data for internal use.

6.4 Ensure that test results are as expected (per the corresponding plans, cases, procedures, design) and the impacts of any discrepancies are understood.

6.5 Ensure that the source code components provide the dependability and fault tolerance required by the system and that the source code is capable of controlling identified hazards and does not create hazardous conditions.

6.6 Ensure that all (in-scope) requirements (e.g. SRS and IRS) are represented in the appropriate source code components and that the source code does not introduce capability that is not required.

6.7 Ensure that the system and software-required threat controls and safeguards are correctly implemented per proposed (or baselined) design components and validate that they provide the desired levels of protection against threats to the system. Any unmitigated threats and vulnerabilities are documented and addressed as part of the system and software operations.

6.8 Ensure the appropriate level of data protection is defined and maintained across all instances and transactions throughout the system and that the security controls are defined to provide comprehensive (end-to-end) protection for the life of the data.

7.0 Verify and Validate Operations and Maintenance Content

The objective of Operations and Maintenance IV&V is to ensure operating plans and procedures are correct and usable, ensure that new constraints, changes in the operating environment, proposed software system changes, and their impact on the software are understood and appropriately addressed, and to ensure that anomalies that are discovered during operation are understood and appropriately addressed. Additional objectives:

7.1 Ensure that the disaster recovery plan is adequate to restore critical operation of the system in the case of an extended system outage.

7.2 Ensure deployment readiness and operational readiness of the software.

7.3 Ensure that the operating procedures are consistent with the user documentation and conform to the system requirements.

7.4 Ensure that the effect of software operation anomalies are understood and appropriately addressed.

7.5 Ensure that training documentation provides adequate guidance to system operators and users to enable correct use of the system and that this documentation is consistent with the system design and implementation.

7.6 Ensure that the software requirements and implementation address 1) specific migration requirements, 2) migration tools, 3) conversion of software products and data, 4) software archiving, 5) support for the prior environment, and 6) user notification.

7.7 For software retirement, ensure that the installation package addresses: 1) software support, 2) impact on existing systems and databases, 3) software archiving, 4) transition to a new software product, and 5) user notification.

7.8 Ensure that user documentation is consistent with the implementation and capable of communicating the use of user-accessible system functions.

7.9 Ensure that the installed software does not introduce new or increased vulnerabilities or security risks to the overall system and that procedures are in place to identify and apply security patches and to periodically test the system configuration for vulnerabilities.

7.10 Ensure that no new security risks are introduced due to changes in the operational environment.

7.11 Ensure that updated security analyses are performed to respond to changes in external interfaces, threats, or technology in general and that any residual risk is identified.

Mapping to NASA-STD-8739.8

The following table provides a mapping between IV&V-related requirements from NASA-STD-8739.8, *Soft ware Assurance Standard*, and the contents of this SLP. The items in Table 2 are included here because they explicitly mention responsibilities related to IV&V. Other content from NASA-STD-8739.8 may be of interest to IV&V for other reasons (see Section 4.1 of this SLP)

Table 2: NASA-STD-8739.8 Mapping

8739.8 Req. #	8739.8 Req. Text	IVV 09-1 Content
7.5.1	All software projects that are identified as safety-critical or software Class A by using NPR 7150.2, Software Engineering Software Assurance Classification Assessment shall be candidates for IV&V with safety criticality as the highest criterion.	Not applicable. This is an IV&V Program function that is outside the scope of this SLP.
7.5.2	IV&V work shall be performed by the contractors selected and managed by the NASA IV&V Facility.	Not applicable. This is an IV&V Program function that is outside the scope of this SLP.
7.5.3	When the IV&V function is required, the provider shall provide all required information to NASA IV&V Facility personnel. (This requirement includes specifying on the contracts and subcontracts, IV&V's access to system and software products and personnel.)	Per 8739.8, IV&V is not responsible for this. However, it is addressed from IV&V's perspective in Table 1, Section 1.1B, first paragraph.
7.5.4	The NASA IV&V Facility shall initially conduct a planning and scoping exercise to determine the specific software components to be analyzed and the tasks to be performed. The IV&V approach will be documented in an IV&V plan.	Table 1, Section 1.5. Note: IV&V Plan and IPEP are synonymous.
7.5.5	The IV&V team shall provide input to the appropriate software assurance personnel, as well as provide feedback to the project manager as agreed in the IV&V Plan.	Table 1, Section 1.1B, third paragraph. Note: IV&V Plan and IPEP are synonymous.

Mapping to NPR 7150.2B

The following table provides a mapping between IV&V-related requirements from NPR 7150.2B, *NASA Software Engineering Requirements*, and the content of this SLP. The items in Table 3 are included here because they explicitly mention responsibilities related to IV&V. Other content from NPR 7150.2B may be of interest to IV&V for other reasons (see Section 4.1 of this SLP).

Table 3: NPR 7150.2B Mapping

7150.2B Req. #	7150.2B Req. Text	IVV 09-1 Content

SWE-141	3.6.2 For projects reaching Key Decision Point (KDP) A after the effective date of this directive's revision, the program manager shall ensure that software IV&V is performed on the following categories of projects: a. Category 1 projects as defined in NPR 7120.5. b. Category 2 projects as defined in NPR 7120.5 that have Class A or Class B payload risk classification per NPR 8705.4. c. Projects specifically selected by the NASA CSMA to have software IV&V.	All
SWE-131	3.6.3 If software IV&V is performed on a project, the project manager shall ensure that an IV&V Project Execution Plan (IPEP) is developed.	Section 4.3. Table 1, Section 1.1B, first paragraph.

Metrics

Any metrics associated with this SLP are established and tracked within the NASA IV&V Metrics Program.

Records

There are no records associated with this SLP.

References

REFERENCES	
Document ID/Link	**Title**
FIPS Publication 199	FIPS Publication 199, Standards for Security Categorization of Federal Information and Information Systems
IEEE Std 1012 - 2012	IEEE Standard for System, Software and Hardware Verification and Validation
IEEE Std 1012/D15	Draft IEEE Standard for System, Software and Hardware Verification and Validation
IEEE Std 1028 - 2008	IEEE Standard for Software Reviews and Audits

IVV QM	NASA IV&V Quality Manual
IVV 09-4	Project Management
IVV 14	Corrective and Preventive Action
IVV 22	Risk Management
IVV 23	Lessons Learned
IVV 24	Success Stories
NASA-STD-8719.13C	Software Safety Standard
NASA-STD-8739.8	Software Assurance Standard
NIST-SP-800-53A	National Institute of Standards and Technology Special Publication 800-53A, Rev 4
NPR 2810.1A	Security of Information Technology
NPR 7123.1B	NASA Systems Engineering Processes and Requirements
NPR 7150.2B	NASA Software Engineering Requirements
NPR 7120.5E	NPR 7120.5 Space Flight Program and Project Management Requirements
S3105	Guidelines for Writing IV&V TIMs
S3106	PBRA and RBA Process
T2103	IV&V Project Execution Plan (IPEP) Template

If any procedure, method, or step in this document conflicts with any document in the NASA Online Directives Information System (NODIS), this document shall be superseded by the NODIS document.

Any external reference shall be monitored by the Document Owner for current versioning.

Version History

VERSION HISTORY				
Version	**Description of Change**	**Rationale for Change**	**Author**	**Effective Date**

Basic	Initial Release		Bill Jackson IT/215	08/15/1997
A – L	Revision information older than 7-year retention period relocated to Revision History Overflow Document		Various	03/06/1998 – 02/02/2009
M	Updated to align with industry standards (after an assessment team recommendation)		Jeff Northey	08/31/2010
N	Annual Document review feedback: minor changes to increase clarity		Jeff Northey	01/27/2011
O	Add training paragraph to section 4.3; add Success Stories; clarify WBS 1.3f, *effort data*. Replace description of IV&V Project Final Report with reference to IVV 09-4		Pat Theeke	06/06/2012
P	Revision to add wording throughout to integrate Information Assurance analyses throughout the IV&V lifecycle. Also incorporates some terminology changes from the latest version of IEEE 1012. Added TOC.	Reflect the security objectives from IEEE 1012 as well as the IA related objectives that were developed as part of the CD Initiative. IEEE 1012 is the IEEE standard from which 09-1 draws its heritage.	Van Casdorph/ Wes Deadrick	02/26/2016