ASSURANCE SPECIFICATION DOCUMENTATION STANDARD AND DATA ITEM DESCRIPTIONS (DID)

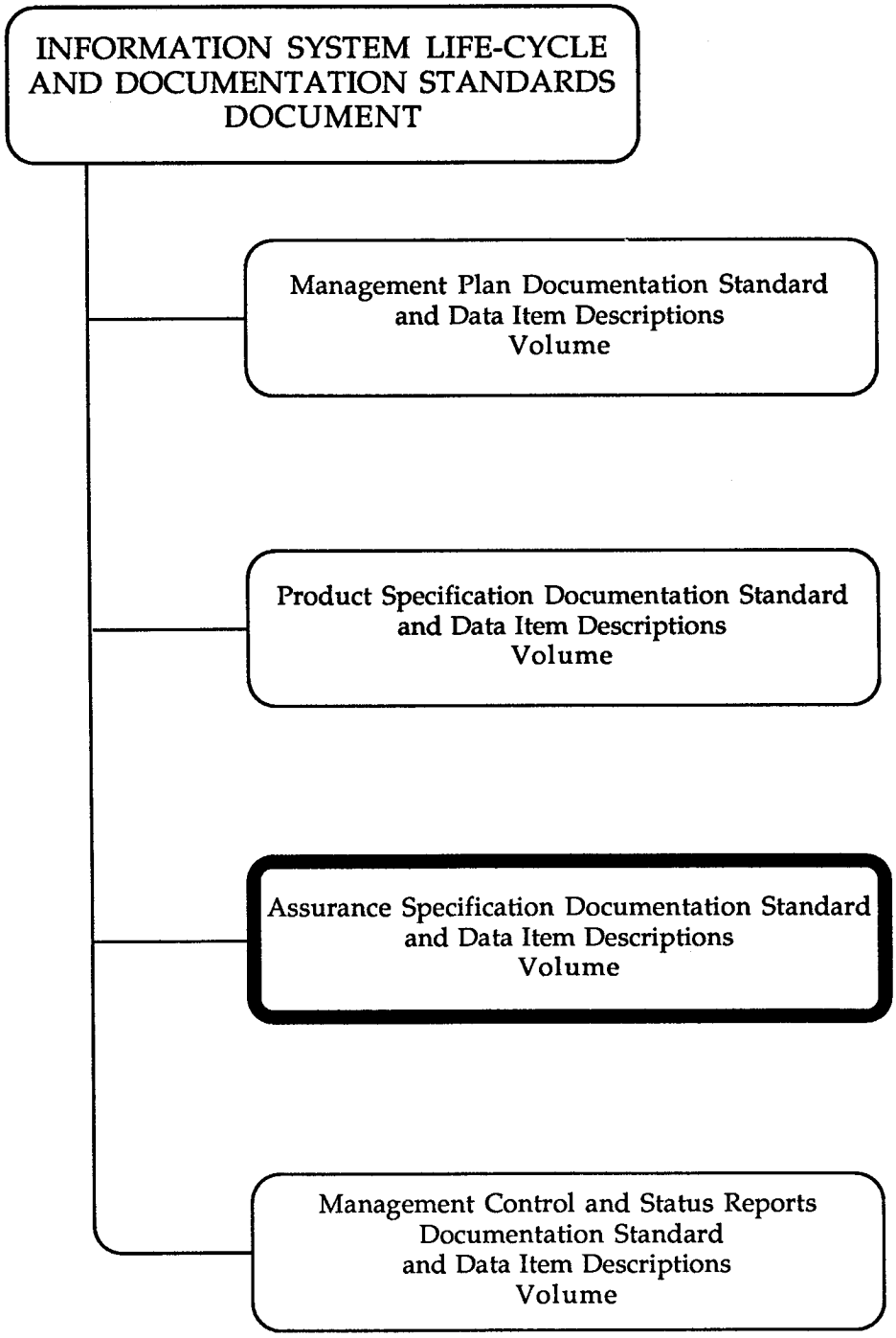
VOLUME OF THE

INFORMATION SYSTEM LIFE-CYCLE AND DOCUMENTATION STANDARDS

Release 4.3

2/28/89

NASA
Office of Safety, Reliability, Maintainability,
and Quality Assurance
Software Management and Assurance Program (SMAP)
Washington, DC



ACKNOWLEDGEMENTS

This document incorporates the extensive work of Dr. E. David Callender and Ms. Jody Steinbacher in specifying the documentation standards for information systems and their components. Their contributions are reflected especially in the concept and definition of the information system, the identification of the major categories of documentation, the definition and application of the roll-out concept, the specification of documentation frameworks, the concept of nested life-cycles for components of information systems, and the description of the relationship between information system acquirers and providers.

They have advanced the state-of-the-art for information systems life-cycle management by establishing simplifying principles for identifying needed documentation units to fit a particular system's environment and organization.

ASSURANCE SPECIFICATION DOCUMENTATION STANDARD

TABLE OF CONTENTS

LIST OF ILLUSTRATIONS

LIST OF TABLES

ASSURANCE SPECIFICATION DOCUMENTATION STANDARD

1.0 INTRODUCTION

1.1 Identification of Volume

This is the Assurance Specification Documentation Standard and Data Item Descriptions Volume rolled-out from the Information System Life-Cycle and Documentation Standards.

1.2 Scope of Volume

An assurance specification contains all technical information for performing and documenting the assurance plan for an information system or a hardware, software, or operational procedures component. This volume states the SMAP documentation standard for an assurance specification document applicable to all NASA information systems and software, hardware, and operational procedures components and related processes.

The selection, adaptation, and enforcement of these documentation standards is the responsibility of the cognizant program/project manager.

IT IS ASSUMED WITHIN THIS VOLUME THAT THE READER OF THIS STANDARD IS FAMILIAR WITH THE TERMS AND CONTENTS OF THE PARENT VOLUME CONCERNING INFORMATION SYSTEM LIFE-CYCLE AND DOCUMENTATION STANDARDS.

1.3 Purpose and Objectives of Volume

The purpose of this volume is to provide a well organized, easily used standard for assurance documentation for information systems and software, hardware, and operational procedures components and related processes. The specifications are developed in conjunction with the corresponding management plans specifying the assurance activities to be performed.

1.4 Volume Status and Schedule

Release 4.2C was the first complete release for Version 4 of the Information System Life-Cycle and Documentation Standards document. All five volumes of the document underwent a SMAP and agency review. Release 4.3 is an update to Release 4.2C based on the approved RIDs from this review. The RID review board determined that change bars will not be used to show the differences between Releases 4.2C and 4.3, as 4.3 is the first baselined release of the Version 4 standards.

1.5 Volume Organization and Roll-Out

Sections 1 and 2 of this volume identify it, describe its purpose, and cite other related documents. Section 3 provides the rationale and scope for this documentation standard. Section 4 presents the actual standard and related rules for documentation, and illustrates the roll-out concept. Section 5 offers guidelines for applying the standard to the needs of a particular application and organizational environment. Section 6 proposes means for assuring and enforcing the standard.

The Data Item Descriptions (DIDs) for the assurance specification are contained in Section 7.

Section 8 defines abbreviations and acronyms; Section 9 contains a glossary of significant terms used throughout the standards. Section 10 is available for notes. Section 11 contains an appendix depicting the detailed outline for an assurance specification written as a single volume.

2.0 RELATED DOCUMENTATION

2.1 Parent Documents

The following document is the parent of this volume:

1) Information System Life-Cycle and Documentation Standards, Release 4.3, 2/28/89. Washington: NASA Office of Safety, Reliability, Maintainability, and Quality Assurance.

2.2 Applicable Documents

The following volumes/documents are referenced herein and are directly applicable to this document:

1) Management Plan Documentation Standard and Data Item Descriptions (DID) Volume of the Information System Life-Cycle and Documentation Standards, Release 4.3, 2/28/89. Washington: NASA Office of Safety, Reliability, Maintainability, and Quality Assurance.

2) Product Specification Documentation Standard and Data Item Descriptions (DID) Volume of the Information System Life-Cycle and Documentation Standards, Release 4.3, 2/28/89. Washington: NASA Office of Safety, Reliability, Maintainability, and Quality Assurance.

3) Management Control and Status Reports Documentation Standard and Data Item Descriptions (DID) Volume of the Information System Life-Cycle and Documentation Standards, Release 4.3, 2/28/89. Washington: NASA Office of Safety, Reliability, Maintainability, and Quality Assurance.

4) IEEE Standard Glossary of Software Engineering Terminology. ANSI/IEEE Std 729-1983. New York: Institute of Electrical and Electronic Engineers, Inc.

2.3 Information Documents

The following documents, although not directly applicable, are referenced for historical continuity:

1) Military Standard for Defense System Software Development, DoD-STD-2167, 4 June 1985, and DoD-STD-2167A, 27 October 1987.

2) NASA Software Data Item Descriptions, Version 3, November 1986. Washington: NASA Office of Safety, Reliability, Maintainability, and Quality Assurance. (Additional Data Item Descriptions were published as Versions 3.1 - 3.5 in

1987.)

3) Space Station Program Software Management Policies, November 1986.

4) Information Processing Resources Management, NHB 2410.1D, April 1985.

3.0 OVERVIEW OF THE ASSURANCE SPECIFICATION DOCUMENTATION STANDARD

3.1 Scope of Standard

The SMAP Assurance Specification Documentation Standard is applicable to all NASA information systems and their software, hardware, and operational procedures components.

The selection, adaptation, and enforcement of these documentation standards is the responsibility of the cognizant program/project manager.

It is important to note that these documentation standards are not management, technical and engineering, or assurance standards. However, the life-cycle and documentation standards provide the mechanism to document the selected activities and related specifications supporting any management, technical and engineering, or assurance standards.

3.2 Rationale for Standard

The rationale for the documentation structure presented in this standard is to provide visibility and to allow management to assign responsibility for the generation of such documentation.

As specified by the Information System Life-Cycle and Documentation Standards, the documentation set for each information system and component consists of:

1) a management plan
2) a product specification
3) an assurance specification
4) a management control and status reports document

An assumption upon which the SMAP documentation standard is based is that it is the responsibility of program/project management to decide what information is to be formally recorded. The documentation standard merely indicates the organization for such information.

The function of the assurance specification documentation standard is to provide a uniform and effective method for correlating, integrating, and presenting all technical (non-planning) assurance information (except reports) for an information system and software, hardware, and operational procedures components. Reports on the results of assurance activities are documented in the management control and status reports document.

3.3 Interface With Other Standards

This documentation standard is derived from the NASA Version 3 software standards maintained by NASA Headquarters Code Q, Office of Safety, Reliability, Maintainability and Quality Assurance.

This documentation standards volume is one of four that augment and detail the life-cycle standards for information systems specified in the parent document. The other three documentation standards volumes are referenced in Section 2.2.

4.0 THE ASSURANCE SPECIFICATION DOCUMENTATION STANDARD

The assurance specification documentation standard describes the format and content of all formal assurance specifications at a single node in an information system's decomposition tree. (For more information on system decomposition, refer to the Information System Life-Cycle and Documentation Standards.)

The purpose of an assurance specification document is to record the specifications, procedures, assurance data (such as test case data), results, and other technical (i.e., non-planning) information for all assurance activities including:

- Quality assurance
- Testing
- Quality engineering assurance
- Safety assurance
- Security and privacy assurance
- Verification and validation
- Certification

The assurance specification document is for the products of assurance activities as the product specification document is for engineering development activities. The definition of which activities are to be performed and the method by which such activities are to be performed are defined in the appropriate sections of the management plan.

4.1 Assurance Specification Structure

The structure of an assurance specification for an information system or component has a hierarchical structure of technical assurance information. The purpose of this hierarchy is to relate individual elements of assurance information to each other and to integrate them all into a coordinated whole. The hierarchical structure also provides a mechanism for partitioning the assurance specification document into multiple volumes when necessary.

Selection of the types of assurance required for an information system or component is specified in the management plan for that system or component. Therefore, the content of the assurance specification document is dependent upon the types of assurance specified in the management plan document.

The assurance specification hierarchical structure for an information system is illustrated in Figure 4-1. The structures for information systems and components are similar, differing only to the extent necessary to encompass the unique activities for an information system or component.

If the development of other support products (such as new standards or a facility for prototyping) is specified in the management plan, then assurance requirements are specified in the section for the development of such products. Thus, an assurance specification may be required for these products as well as for the information system or component to which they apply.

ACQUIRER'S ASSURANCE

- Quality Assurance
- Testing (Acceptance)
- Quality Engineering Assurance
- Safety Assurance
- Security and Privacy Assurance
- Verification and Validation (Independent)
- Certification

DEVELOPMENT PROVIDER'S ASSURANCE

- Quality Assurance
- Testing
- Quality Engineering Assurance
- Safety Assurance
- Security and Privacy Assurance
- Verification and Validation
- Certification

SUSTAINING ENGINEERING AND OPERATIONS PROVIDER'S ASSURANCE

- Quality Assurance
- Testing
- Quality Engineering Assurance
- Safety Assurance
- Security and Privacy Assurance
- Verification and Validation
- Recertification

Figure 4-1. Structure for Information System Assurance Specification

4.2 Responsibility for Preparation of the Assurance Specification

The assurance specification is prepared in accordance with the management plan for the information system or component. The acquirer has overall responsibility for the product assurance specification.

The acquirer's requirements are specified in the acquisition plan section of the management plan. The assurance provider(s) (i.e., the development or Independent Verification and Validation providers) are responsible for preparing their specific sections of the assurance specification as designated in the corresponding management plan sections.

Each assurance specification document is prepared for a particular information system or component; i.e., for a node in the decomposition tree. The physical organization (i.e., roll-out into separate volumes) and content for the assurance specification document is dependent upon the assurance specified in the management plan for that node.

4.3 Roll-Out Concept and Template

For a small information system or component, it is possible that each document of the documentation set (management plan, product specification, assurance specification, and management control and status reports document) can be written as a single physical volume. However, many information systems and components require that multiple volumes be used for each document. In the case where a documentation set document for an information system or component requires more than one volume, the concept of "roll-out" is employed.

The roll-out concept provides a mechanism whereby sections of the document are packaged as separate volumes. The parent document or volume contains pointers to each of the rolled-out sections. The rolled-out volume contains a pointer back to its parent. This preserves the overall integrity of the documentation set structure while offering the convenience of separately preparing a section of the document. (For convenience of packaging and traceability to Version 3, the DIDs for this document are presented in rolled-out format.) The decision on which sections of the document are rolled-out is stated in the management plan by the appropriate manager as identified in Section 4.2.

The assurance specification DIDs for information systems (SMAP-DID-A000-SY) and for any component (SMAP-DID-A000-CO) are the top-level DIDs for this document in the documentation set.

Additional DIDs in Section 7 provide the details for the document content. Each DID consists of: 1) a table of contents and 2) content description.

A separate DID (SMAP-DID-A999) is provided to describe the content of the Assurance Specification Template itself. The standard template (Figure 4-2) is used as part of the roll-out mechanism.

ASSURANCE SPECIFICATION TEMPLATE

1.0 INTRODUCTION

- 1.1 Identification of Volume
- 1.2 Scope of Volume
- 1.3 Purpose & Objectives of Volume
- 1.4 Volume Status & Schedule
- 1.5 Volume Organization & Roll-Out

2.0 RELATED DOCUMENTATION

- 2.1 Parent Documents
- 2.2 Applicable Documents
- 2.3 Information Documents

3.0 thru N.0 SECTIONS OF THE PARENT SPECIFICATION BEING ROLLED-OUT INTO A SEPARATE VOLUME

N+1.0 ABBREVIATIONS AND ACRONYMS

N+2.0 GLOSSARY

N+3.0 NOTES

N+4.0 APPENDICES

Figure 4-2. Assurance Specification Template.

Because the rolled-out volume represents a single section in its parent document or volume, sections 3.0 through N.0 of the rolled-out volume are actually the major subheadings for the section in the parent document or volume.

The Abbreviations and Acronyms section defines all acronyms and abbreviations used within the document or volume. The Glossary

section includes definitions of special terms used within the document or volume.

The Notes section is used for supplemental information that is not part of the formal, binding information presented elsewhere in the document or volume.

Appendices are considered to be an integral part of the document or volume. They may be separately page numbered, or included in the pagination for the volume as a whole. They may bear a section number within the overall volume, or may be separately identified.

Figure 4-3 illustrates the section numbering rules that are employed when material in a section is rolled-out into a separate volume.

4.4 The Assurance Specification Standard and Rules

All of the standards contained in the parent document (Information System Life-Cycle and Documentation Standards) shall apply to assurance specifications. This section contains additional rules that are specific to documentation.

For the information system itself, and for each subordinate information system (subsystem) and software, hardware, and operational procedures component identified in the decomposition tree, the following standards shall apply:

1) There shall be a single assurance specification document consisting of one or more volumes. Assurance specifications shall exactly follow the outline specified by the DIDs in Section 7.

2) The manager(s) of the assurance provider(s) shall be responsible for designating the sections to be rolled-out as separate volumes and shall record the structure and content for the assurance specification in the appropriate sections of the management plan for the information system or component for which the specification is being prepared.

3) The following rules shall be applied when generating an assurance specification:

   a) The roll-out of a section into a separate volume shall follow the standard format specified by the Assurance Specification Template DID (SMAP-DID-A999) given in Section 7.

Figure 4-3. Documentation Tailoring – Roll-Out Example.

b) The assurance provider(s) have responsibility for the generation of the assurance specification. This assurance specification shall be based on the specific product assurance planning sections of the management plan plus any relevant requirements in the acquisition plan section of the management plan. The acquirer shall have overall responsibility for the assurance specification document.

c) Each rolled-out volume shall be titled as illustrated below. This method supports the standard and enables one to place the volume in context with its parent(s).

< title of the rolled-out section >
Volume of the
[< parent volume title >
Volume of the]
< documentation set parent title >
Document

Note that the volume entry in brackets ([]) above is to be expanded zero or more times depending on the number of levels of roll-out from the documentation set parent. Additional information may be included on the title page as specified by delivery requirements.

d) When writing the assurance specification document, the outline specified by the assurance specification (top level) DID shall be used. If more detailed structuring is needed for a section than that shown in this DID, then the structuring shall follow the detailed, rolled-out, DID(s) for for that section. Additional substructure detail (i.e., below the lowest level DID outline) may be added at the discretion of the author.

Sections or subsections may be added if needed to convey assurance information additional to that specified in the DIDs. Added sections or subsections shall be inserted following those specified in the DIDs.

e) A section shall either:

- o contain information;
- o point to a lower level volume rolled-out from this document or volume;
- o point to another document (e.g., the contract governing the effort) that contains the information appropriate to the section;
- o be marked TBD (to be determined) if appropriate

information is not yet available; or

- o be marked "Not applicable" or "None."

If a section is "Not applicable" or "None," then none of its subordinate sections shall appear.

f) The documentation standard designates a unique place for each element of information. The same information shall not be incorporated in more than one place when generating a document or rolled-out volume.

g) The manager responsible for a plan may roll-out beyond the roll-out structure implied by the DIDs in Section 7 of this volume. In that case the Assurance Specification Template shall be used.

h) Any document that is to be placed under any level of an organization's configuration management shall be compatible with the appropriate electronic formats specified in applicable support environment(s) (such as the SSE and TMIS documentation formats for the Space Station Freedom Program.)

5.0 APPLICATION AND SUPPORT OF THE ASSURANCE SPECIFICATION DOCUMENTATION STANDARD

This section provides guidelines for tailoring and using this standard to prepare an Assurance Specification or portion thereof.

5.1 Guidelines

The following collection of guidelines is offered to assist in applying this standard.

5.1.1 How to Use the DIDs to Prepare an Assurance Specification

To prepare an assurance specification start with the Assurance Specification DID (SMAP-DID-A000). It is the responsibility of the manager of the specific assurance activity for an information system or component to determine for the assurance specification and to record in the appropriate section of the management plan:

1) Which sections are relevant and which should be marked "Not applicable" or "None."

2) What level of detail is required for each section.

3) Which sections will be rolled-out as separate volumes.

4) Who will be responsible for the activities covered by a section, and therefore will be also responsible for preparing that section or volume.

Thus the management plan provides overall direction as to the format of the assurance specification.

The DIDs in Section 7 of this volume are presented in a rolled-out format. If the assurance specification is to be contained in one volume, then prepare Sections 1, 2, and the Abbreviations and Acronyms, Glossary, Notes, and Appendices sections as specified in the Assurance Specification Template DID (SMAP-DID-A999). Then, for each section in the Assurance Specification DID (SMAP-DID-A000) to be included inline, determine:

a) If the amount of information to be included can be conveyed in a few paragraphs, without subsections, then do so. However, look over the detailed DID cited in that section of the top level DID to be sure that all appropriate information is included.

b) If the amount or detail of the information to be included warrants use of subsections, then use the structure of

the cited detailed DID as the substructure for that section. For example, section 3.0 in the detailed DID shall appear as Section N.1 in the document; Section 4.0 in the detailed DID shall appear as Section N.2 in the document, and so on (where N stands for the corresponding section in the top level DID). Similarly, Section 3.1 in the detailed DID shall appear as Section N.1.1 in the document. See Figure 5-1 for an example of incorporating substructure from detailed DIDs into the inline structure for a section.

Each document subsection specified in the detailed DID shall be included and shall be prepared in accordance with the rules stated in Section 4 of this documentation standard. If the detailed DID itself cites another detailed DID, it is necessary to follow the structure indicated by the latter DID only if further subsections are required.

c) Additional sections and subsections may be included as described by the rules in Section 4.

If the assurance specification is to be contained in multiple volumes, then for the sections that are rolled-out into separate volumes, use the appropriate DID in Section 7 or the rules for rolling-out a section.

5.1.2 Roll-Out Factors

Factors influencing a roll-out decision include:

a) When the activities to be accomplished are delegated to another organization, whether internal or external.

b) When the detail occasioned by the complexity of the activities to be accomplished is too great to be described within a single physical volume.

c) When it is desirable to apply configuration management and control to the section separately from other sections because of amount of change expected, time required to review before baselining, etc.

Figure 5-1. Incorporating DID Substructure In-Line.

5.1.3 Documentation Content

Documentation should be as brief and specific as possible while conveying all essential information. To aid in meeting this goal:

a) If a section has subsections, content information should, in general, be contained within the subsections rather than under the section heading. Reserve the use of text under section headings, in cases where detailed information is provided in subsections, for such essentials as:

   - o General explanatory information needed to aid the reader in understanding the detailed information following
   - o Information common to two or more of the subsections following

   Do not write "boilerplate" that does not contain any data of substance; e.g., a list of the topics covered in the subsections, or a promise to "do good things".

b) Avoid redundancy. The hierarchical structure specified by the documentation standard and the DIDs provides a unique place to put each item of information needed, for most cases.

c) Except where required by this standard, do not summarize the content of a rolled-out section in the parent document or volume. The summary might have to be changed each time the rolled-out section is changed.

5.1.4 Transition from Current Data Requirements Lists

During the period of transition while this standard is introduced into an ongoing NASA activity, the following considerations apply.

a) Documents specified by an existing Data Requirements List (DRL) may closely parallel rolled-out sections as described in this documentation standard. When revising the DRL, or if no specific outline is provided, it may be convenient to follow the appropriate DIDs presented in section 7.

b) As an aid to establishing an easily-managed documentation set for an application, if it does not currently exist, it may be desirable to prepare the top level documentation set document specified by this standard. This document can serve as an index to existing documentation by pointing to the appropriate DRL for each section. This provides then a relationship structure (or documentation tree) for pieces of

existing data. More importantly, preparation of the document may highlight gaps in coverage for information needed to manage and produce the information system or component.

5.1.5 Use of a Standards and Procedures Repository

Acquirer and provider managers are responsible for determining the need and establishing a repository for any additional procedures, guidelines, rules, and practices for documentation that are not already defined in an existing repository, (such as the ones maintained for the Space Station Freedom Program by TMIS and the SSE), or a parent information system or component repository. At the manager's discretion, procedural information for minor or unique matters may be included as added subsections in a documentation set document (per rule for additional sections).

5.2 Tools Supporting the Application and Use of the Documentation Standard

Support environments may provide tools for the application and use of the documentation standard. For example, TMIS and the SSE provide tools for the Space Station Freedom Program that support the documentation standards. Such tools are used when preparing, reviewing, revising, publishing, distributing, and configuration managing documents. Tools are also provided for preparing a WBS and schedules. Tool support of the standards is the responsibility of the program/project.

6.0 ASSURANCE AND ENFORCEMENT OF THE DOCUMENTATION STANDARD

If the SMAP information system life-cycle and documentation standards have been selected as standards by program/project management, then it is the responsibility of the acquiring manager of the information system or component to assure and enforce this documentation standard for all documentation written for that information system or component.

The assurance process is formally addressed in one of two ways:

1) As a quality assurance activity during the phase transition reviews indicated by the information system life-cycle.

2) As explicitly called for within any planning document. (For example, an assurance plan section of the management plan could call for special reviews of individual documents and volumes.)

The information system life-cycle specifies that the initial version of the assurance specification is to be generated by the end of the information system requirements phase. This version of the assurance specification is reviewed at the end of that phase.

The information system life-cycle also specifies when other portions of the assurance specification are to be prepared and reviewed during later phases of the life-cycle. This life-cycle standard also specifies that the assurance specification shall be reviewed as it is updated.

It is the responsibility of the reviewers of any assurance specification to be familiar with the assurance specification documentation standard and to question any deviations from this standard.

Because all sections specified in a DID must be included in the document or volume, managers and participants in management reviews can easily verify that all necessary information has been prepared. The structure for the document serves as a gross level checklist.

7.0 DATA ITEM DESCRIPTIONS (DIDS)

This section contains the specifications for the format, outline, and content of the assurance specification document and of rolled-out sections.

Because presenting the outline for the assurance specification as a single DID is overwhelming and unmanageable, major sections have been rolled-out into separate DIDs using the standard roll-out template. This provides traceability to Version 3 DIDs and ease of use and packaging. However, if it is desirable to create the assurance specification as a single document, a sample detailed table of contents for such a document is presented in Appendix A of this volume.

The number of assurance specification volumes generated for a specific information system or component need not mirror the number of DIDs presented in this section. Lower level detailed DIDs provide additional substructure and contain content discussion which should be reviewed even when the content is recorded in-line (i.e., not rolled-out). In general one would start with the appropriate SMAP-DID-A000 using the guidelines in Section 5. Documentation authors then decide to what level the assurance specification is to be rolled-out. (If no DID is cited, then additional substructure is at the discretion of the author.)

Tables 7-1 through 7-4 are provided to assist the users of these standards. Table 7-1 contains a listing of the DIDs by DID number (from the Table of Contents). Table 7-2 contains a listing of the DIDs by DID title. Table 7-3 depicts the relationships among the assurance specification DIDs for an information system. Table 7-4 shows the relationships among the assurance specification DIDs for a software, hardware, or operational procedures component. Each level of indentation in Tables 7-3 and 7-4 reflects an additional level of DID detail and substructure. Tables 7-3 and 7-4 are not to be taken as a roll-out structure for any particular assurance specification.

The Template DID (SMAP-DID-P999) provides detailed instructions for preparing the sections that are common to the document and all volumes rolled-out from the document. Note that this DID does not itself represent a particular separate document or volume, but is used to generate a volume format for a section that a manager wishes to document in a separate volume.

The Assurance Specification DIDs (SMAP-DID-A000-SY or -CO) provide an outline for the complete assurance specification document for an information system or a software, hardware, or operational procedures component. Major sections of the DID point to DIDs that contain a detailed description for the content of these sections.

The detailed DIDs in section 7 may be used as they stand to produce separate volumes of an assurance specification. If the section represented by a detailed DID is to be presented, instead, as an inline part of an assurance specification document, then only those sections from 3.0 to (but not including) the Abbreviations and Acronyms section are to be used. (See Section 5.1 for further explanation.)

TABLE 7-1. DID Index (Numeric Order).

TABLE 7-2. DID Index (Alphabetic Order).

TABLE 7-3. Complete DID Set for an Information System Assurance Specification.

SMAP-DID-A000-SY	Information System Assurance Specification
SMAP-DID-A100	Quality Assurance DID
SMAP-DID-A200	Testing DID
SMAP-DID-A300	Quality Engineering Assurance DID
SMAP-DID-A400	Safety Assurance DID
SMAP-DID-A500	Security and Privacy Assurance DID
SMAP-DID-A600	Verification and Validation DID
SMAP-DID-A700	Certification DID

TABLE 7-4. Complete DID Set for Component Assurance Specification.

SMAP-DID-A000-CO	Component Assurance Specification DID
SMAP-DID-A100	Quality Assurance DID
SMAP-DID-A200	Testing DID
SMAP-DID-A300	Quality Engineering Assurance DID
SMAP-DID-A400	Safety Assurance DID
SMAP-DID-A500	Security and Privacy Assurance DID
SMAP-DID-A600	Verification and Validation DID
SMAP-DID-A700	Certification DID

SMAP-DID-A000-SY

INFORMATION SYSTEM ASSURANCE SPECIFICATION

DATA ITEM DESCRIPTION

TABLE OF CONTENTS

ASSURANCE SPECIFICATION DOCUMENTATION STANDARD
INFORMATION SYSTEM ASSURANCE SPECIFICATION: SMAP-DID-A000-SY

EXPLANATORY NOTE

The purpose of the assurance specification document is to document all of the technical information (such as specifications and criteria) related to assuring a software, hardware, or operational procedures component. The types of assurance and the organizations responsible for performing that assurance are specified in the associated management plan.

1.0 INTRODUCTION

The structure and content description to be used when preparing this section is described in detail in the Assurance Specification Template DID (SMAP-DID-A999).

2.0 RELATED DOCUMENTATION

The structure and content description to be used when preparing this section is described in detail in the Assurance Specification Template DID (SMAP-DID-A999).

3.0 ACQUIRER'S ASSURANCE

3.1 Quality Assurance

The purpose of this section is to document the specifications, criteria, and results for quality assurance activities specified in the acquisition section of the management plan including reviews and configuration audits conducted by the acquirer (or designee reporting directly to the acquirer). In general, quality assurance activities focus on conformance to standards and plans. The assurance is of both processes and products (such as documentation, systems, standards, and the configuration management process) of the development and sustaining engineering and operations providers for the purpose of evaluating their quality.

The section also documents the specifications and criteria for audits and reviews performed in accordance with the management plan to assure the quality of the acquirer's processes and associated products; e.g., configuration management, management plan, status monitoring.

Refer to the Quality Assurance DID (SMAP-DID-A100) for a further description of the structure and content. (Note: If the quality assurance activity is based on testing, it may be more appro-

priate to use the Testing DID (SMAP-DID-A200).)

3.2 Testing

The purpose of this section is to document the test specifications, procedures, criteria, and expected and actual results of tests conducted by the acquirer to demonstrate that the information system delivered from a developer (or sustaining engineering and operations provider) meets requirements and is acceptable.

The primary topics for each testing subsection include:

- Test identification and specification
- Test criteria and procedures
- Test cases and expected results
- Actual test results

Refer to the Testing DID (SMAP-DID-A200) for a further description of the structure and content for each topic.

3.3 Quality Engineering Assurance

The purpose of this section is to document the specifications, procedures, criteria, and results directly related to quality engineering assurance conducted by the acquirer (or designee other than the developer) on products of the development and sustaining engineering and operations providers. In general, quality engineering assurance activities focus on assuring the proper implementation of quality factors or "ilities".

Refer to the Quality Engineering Assurance DID (SMAP-DID-A300) for a further description of structure and content.

3.4 Safety Assurance

The purpose of this section is to document the specifications, procedures, criteria, and results directly related to safety assurance conducted by the acquirer (or designee other than the developer) on products of the development and sustaining engineering and operations providers. In general, safety assurance activities focus on assuring the proper implementation of safety requirements.

Refer to the Safety Assurance DID (SMAP-DID-A400) for a further description of structure and content.

3.5 Security and Privacy Assurance

The purpose of this section is to document the specifications, procedures, criteria, and results directly related to security and privacy assurance conducted by the acquirer (or designee other than the developer) on products of the development and sustaining engineering and operations providers. In general, security and privacy assurance activities focus on assuring the proper implementation of security and privacy requirements.

Refer to the Security and Privacy Assurance DID (SMAP-DID-A500) for a further description of structure and content.

3.6 Verification and Validation

The purpose of this section is to document the verification and validation specifications, criteria, etc. for independent verification and validation conducted by the acquirer or by the acquirer's independent verification and validation provider.

Refer to the Verification and Validation DID (SMAP-DID-A600) for a further description of the structure and content for each topic.

3.7 Certification

The purpose of this section is to document the certification specifications, procedures, criteria, and expected and actual results for all certification activities as specified in the acquirer's assurance section of the management plan to demonstrate that the information system has been certified.

Refer to the Certification DID (SMAP-DID-A700) for a further description of the structure and content for each topic.

4.0 DEVELOPMENT PROVIDER'S ASSURANCE

4.1 Quality Assurance

The purpose of this section is to document the specifications, criteria, and results for quality assurance activities specified in the acquisition section of the management plan including reviews and configuration audits conducted by the developer on processes and products of the developer for the purpose of evaluating quality. In general, quality assurance activities focus on conformance to standards and plans.

Refer to the Quality Assurance DID (SMAP-DID-A100) for a further

description of the structure and content. (Note: If the quality assurance activity is based on testing, it may be more appropriate to use the Testing DID (SMAP-DID-A200).)

4.2 Testing

The purpose of this section is to document the test specifications, procedures, and expected and actual results of the tests performed by the developer. A separate subsection shall be generated for each level of testing (including system integration testing and acceptance testing) specified in the management plan and for each major group of tests within a testing level.

The primary topics for each testing subsection include:

- o Test identification and specification
- o Test criteria and procedures
- o Test cases and expected results
- o Actual test results

Refer to the Testing DID (SMAP-DID-A200) for a further description of the structure and content for each topic.

4.3 Quality Engineering Assurance

The purpose of this section is to document the specifications, procedures, criteria, and results directly related to quality engineering assurance conducted by the developer (or designee reporting to developer) on products of the developer. In general, quality engineering assurance activities focus on assuring the proper implementation of quality factors or "ilities".

Refer to the Quality Engineering Assurance DID (SMAP-DID-A300) for a further description of structure and content.

4.4 Safety Assurance

The purpose of this section is to document the specifications, procedures, criteria, and results directly related to safety assurance conducted by the developer (or designee reporting to the developer) on products of the developer. In general, safety assurance activities focus on assuring the proper implementation of safety requirements.

Refer to the Safety Assurance DID (SMAP-DID-A400) for a further description of structure and content.

4.5 Security and Privacy Assurance

The purpose of this section is to document the specifications, procedures, criteria, and results directly related to security and privacy assurance conducted by the developer (or designee reporting to the developer) on products of the developer. In general, security and privacy assurance activities focus on assuring the proper implementation of security and privacy requirements.

Refer to the Security and Privacy Assurance DID (SMAP-DID-A500) for a further description of structure and content.

4.6 Verification and Validation

The purpose of this section is to specify the specifications, procedures, criteria, etc. for verification and validation conducted by the developer (or designee reporting to the developer) on products prior to delivery to the acquirer.

Refer to the Verification and Validation DID (SMAP-DID-A600) for a further description of the structure and content for each topic.

4.7 Certification

Certification is normally performed by the acquirer. If the development provider is required to perform certification, then refer to the Certification DID (SMAP-DID-A700) for a description of the structure and content for this section.

5.0 SUSTAINING ENGINEERING AND OPERATIONS PROVIDER'S ASSURANCE

5.1 Quality Assurance

The purpose of this section is to document the specifications, criteria, and results for quality assurance activities specified in the acquisition section of the management plan including reviews and configuration audits conducted by the sustaining engineering and operations provider on processes and products of the sustaining engineering and operations provider. In general, quality assurance activities focus on conformance to standards and plans.

Refer to the Quality Assurance DID (SMAP-DID-A100) for a further description of the structure and content. (Note: If the quality assurance activity is based on testing, it may be more appropriate to use the Testing DID (SMAP-DID-A200).)

5.2 Testing

The purpose of this section is to document the test specifications, procedures, criteria, and expected and actual results of the tests performed by the sustaining engineering and operations provider. Separate subsections shall be generated for each level of testing (including integration and acceptance) specified in the management plan and for each major group of tests within a testing level.

The primary topics for each testing subsection include:

- Test identification and specification
- Test criteria and procedures
- Test cases and expected results
- Actual test results

Refer to the Testing DID (SMAP-DID-A200) for a further description of the structure and content for each topic.

5.3 Quality Engineering Assurance

The purpose of this section is to document the specifications, procedures, criteria, and results directly related to quality engineering assurance conducted by the sustaining engineering and operations provider (or designee) on products of the sustaining engineering and operations provider. In general, quality engineering assurance activities focus on assuring the proper implementation of quality factors or "ilities".

Refer to the Quality Engineering Assurance DID (SMAP-DID-A300) for a further description of structure and content.

5.4 Safety Assurance

The purpose of this section is to document the specifications, procedures, criteria, and results directly related to safety assurance conducted by the sustaining engineering and operations provider (or designee) on products of the sustaining engineering and operations provider. In general, safety assurance activities focus on assuring the proper implementation of safety requirements.

Refer to the Safety Assurance DID (SMAP-DID-A400) for a further description of structure and content.

5.5 Security and Privacy Assurance

The purpose of this section is to document the specifications, procedures, criteria, and results directly related to security and privacy assurance conducted by the sustaining engineering and operations provider (or designee) on products of the sustaining engineering and operations provider. In general, security and privacy assurance activities focus on assuring the proper implementation of security and privacy requirements.

Refer to the Security and Privacy Assurance DID (SMAP-DID-A500) for a further description of structure and content.

5.6 Verification and Validation

The purpose of this section is to specify the review criteria, specifications, procedures, criteria, etc. for verification and validation conducted by the sustaining engineering and operations provider (or designee reporting directly to this provider) on products prior to delivery.

Refer to the Verification and Validation DID (SMAP-DID-A600) for a further description of the structure and content for each topic.

5.7 Recertification

Recertification is normally performed by the acquirer. If the sustaining engineering and operations provider must perform recertification, then refer to the Certification DID (SMAP-DID-A700) for a description of the structure and content for this section.

6.0 ABBREVIATIONS AND ACRONYMS

Refer to the Assurance Specification Template DID (SMAP-DID-A999) for the detailed description of content for this section.

7.0 GLOSSARY

Refer to the Assurance Specification Template DID (SMAP-DID-A999) for the detailed description of content for this section.

8.0 NOTES

Refer to the Assurance Specification Template DID (SMAP-DID-A999) for the detailed description of content for this section.

9.0 APPENDICES

Refer to the Assurance Specification Template DID (SMAP-DID-A999) for the specifications for appendices.

SMAP-DID-A000-CO

COMPONENT ASSURANCE SPECIFICATION

DATA ITEM DESCRIPTION

TABLE OF CONTENTS

6.0 GLOSSARY

7.0 NOTES

8.0 APPENDICES

ASSURANCE SPECIFICATION DOCUMENTATION STANDARD
COMPONENT ASSURANCE SPECIFICATION DID: SMAP-DID-A000-CO

EXPLANATORY NOTE

The purpose of the assurance specification document is to document all of the technical information (such as specifications and criteria) related to assuring a software, hardware, or operational procedures component. The types of assurance and the organizations responsible for performing that assurance are specified in the associated management plan.

1.0 INTRODUCTION

The structure and content description to be used when preparing this section is described in detail in the Assurance Specification Template DID (SMAP-DID-A999).

2.0 RELATED DOCUMENTATION

The structure and content description to be used when preparing this section is described in detail in the Assurance Specification Template DID (SMAP-DID-A999).

3.0 ACQUIRER'S ASSURANCE

3.1 Quality Assurance

The purpose of this section is to document the specifications, criteria, and results for quality assurance activities specified in the acquisition section of the management plan including reviews and configuration audits conducted by the acquirer (or designee reporting directly to the acquirer) on processes and products for the component delivered from a provider for the purpose of evaluating quality. In general, quality assurance activities focus on conformance to standards and plans.

The section also documents the specifications and criteria for audits and reviews performed in accordance with the management plan to assure the quality of the acquirer's processes and associated products; e.g., configuration management, management plan, status monitoring.

Refer to the Quality Assurance DID (SMAP-DID-A100) for a further description of the structure and content. (Note: If the quality assurance activity is based on testing, it may be more appropriate to use the Testing DID (SMAP-DID-A200).)

3.2 Testing

The purpose of this section is to document the test specifications, procedures, criteria, and expected and actual results of tests conducted by the acquirer to demonstrate that the component delivered from the developer meets requirements and is acceptable.

The primary topics for each testing subsection include:

- Test identification and specification
- Test criteria and procedures
- Test cases and expected results
- Actual test results

Refer to the Testing DID (SMAP-DID-A200) for a further description of the structure and content for each topic.

3.3 Quality Engineering Assurance

The purpose of this section is to document the specifications, procedures, criteria, and results directly related to quality engineering assurance conducted by the acquirer (or designee other than the developer) on products of the development and sustaining engineering and operations providers. In general, quality engineering assurance activities focus on assuring the proper implementation of quality factors or "ilities".

Refer to the Quality Engineering Assurance DID (SMAP-DID-A300) for a further description of structure and content.

3.4 Safety Assurance

The purpose of this section is to document the specifications, procedures, criteria, and results directly related to safety assurance conducted by the acquirer (or designee other than the developer) on products of the development and sustaining engineering and operations providers. In general, safety assurance activities focus on assuring the proper implementation of safety requirements.

Refer to the Safety Assurance DID (SMAP-DID-A400) for a further description of structure and content.

3.5 Security and Privacy Assurance

The purpose of this section is to document the specifications, procedures, criteria, and results directly related to security and privacy assurance conducted by the acquirer (or designee other than the developer) on products of the development and sustaining engineering and operations providers. In general, security and privacy assurance activities focus on assuring the proper implementation of security and privacy requirements.

Refer to the Security and Privacy Assurance DID (SMAP-DID-A500) for a further description of structure and content.

3.6 Verification and Validation

The purpose of this section is to document the verification and validation specifications, criteria, etc., for independent verification and validation conducted by the acquirer or the independent verification and validation provider reporting directly to the acquirer. Note that the decision to perform IV&V is specified in the management plan. In general, verification and validation is usually only conducted on information systems but may be applied to critical components.

Refer to the Verification and Validation DID (SMAP-DID-A600) for a further description of the structure and content.

3.7 Certification

The purpose of this section is to document the certification specifications, procedures, criteria, and expected and actual results for all certification activities conducted by the acquirer as specified in the management plan to demonstrate that the hardware, software, or operational procedures component has been certified. (Note that certification is usually done only at the information system level.)

Refer to the Certification DID (SMAP-DID-A700) for a further description of the structure and content.

4.0 DEVELOPMENT PROVIDER'S ASSURANCE

4.1 Quality Assurance

The purpose of this section is to document the specifications, criteria, and results for quality assurance activities specified in the acquisition section of the management plan including reviews and configuration audits conducted by the developer on processes and products of the developer for the purpose of evaluating quality. In general, quality assurance activities focus on conformance to standards and plans.

Refer to the Quality Assurance DID (SMAP-DID-A100) for a further description of the structure and content. (Note: If the quality assurance activity is based on testing, it may be more appropriate to use the Testing DID (SMAP-DID-A200).)

4.2 Testing

The purpose of this section is to document the test specifications, procedures, and expected and actual results of the component tests performed by the developer.

Separate subsections shall be generated for each level of testing (such as unit, integration, and acceptance) specified in the management plan and for each major group of tests within a testing level. The actual organization of this section, including the subsections on unit, integration, and acceptance testing, also depends upon incremental development and phased delivery requirements and the associated definition of the organization for the assurance specification stated in the management plan.

The primary topics for each testing subsection include:

- Test identification and specification
- Test criteria and procedures
- Test cases and expected results
- Actual test results

4.2.1 Unit Testing

The purpose of this section is to record the specifications, procedures, criteria, and expected and actual results of unit tests for the component. The specifications for unit tests are based on the detailed design of the components.

For each major group of unit tests, a subsection detailed according to the Testing DID (SMAP-DID-A200) should be generated.

4.2.2 Integration Testing

The purpose of this section is to record the specifications, procedures, criteria, and expected and actual results of integration tests for the component. The specifications for integration tests are based on the architectural design of the components.

For each major group of integration tests, a subsection detailed according to the Testing DID (SMAP-DID-A200) should be generated.

4.2.3 Acceptance Testing

This section is applicable only if acceptance testing is to be conducted by the developer. The purpose of this section is to record the specifications, criteria, procedures, and expected and actual results of acceptance tests for the component. The specifications for acceptance tests are based on the requirements for the components.

For each major group of acceptance tests, a subsection detailed according to the Testing DID (SMAP-DID-A200) should be generated.

4.3 Quality Engineering Assurance

The purpose of this section is to document the specifications, procedures, criteria, and results directly related to quality engineering assurance conducted by the developer (or designee reporting to developer) on products of the developer. In general, quality engineering assurance activities focus on assuring the proper implementation of quality factors or "ilities".

Refer to the Quality Engineering Assurance DID (SMAP-DID-A300) for a further description of structure and content.

4.4 Safety Assurance

The purpose of this section is to document the specifications, procedures, criteria, and results directly related to safety assurance conducted by the developer (or designee reporting to the developer) on products of the developer. In general, safety assurance activities focus on assuring the proper implementation of safety requirements.

Refer to the Safety Assurance DID (SMAP-DID-A400) for a further description of structure and content.

4.5 Security and Privacy Assurance

The purpose of this section is to document the specifications, procedures, criteria, and results directly related to security and privacy assurance conducted by the developer (or designee reporting to the developer) on products of the developer. In general, security and privacy assurance activities focus on assuring the proper implementation of security and privacy requirements.

Refer to the Security and Privacy Assurance DID (SMAP-DID-A500) for a further description of structure and content.

4.6 Verification and Validation

The purpose of this section is to document the review criteria, specifications, procedures, criteria, etc. for verification and validation conducted by the developer (or designee reporting directly to the developer.) In general, verification and validation is only conducted on information systems or critical components.

Refer to the Verification and Validation DID (SMAP-DID-A600) for a further description of the structure and content.

4.7 Certification

Certification is normally performed by the acquirer on information systems. If the development provider must perform certification on the component, then refer to the Certification DID (SMAP-DID-A700) for a description of the structure and content for this section.

5.0 ABBREVIATIONS AND ACRONYMS

Refer to the Assurance Specification Template DID (SMAP-DID-A999) for the detailed description of content for this section.

6.0 GLOSSARY

Refer to the Assurance Specification Template DID (SMAP-DID-A999) for the detailed description of content for this section.

7.0 NOTES

Refer to the Assurance Specification Template DID (SMAP-DID-A999) for the detailed description of content for this section.

8.0 APPENDICES

Refer to the Assurance Specification Template DID (SMAP-DID-A999) for the specifications for appendices.

SMAP-DID-A100

QUALITY ASSURANCE

DATA ITEM DESCRIPTION

TABLE OF CONTENTS

ASSURANCE SPECIFICATION DOCUMENTATION STANDARD
QUALITY ASSURANCE DID: SMAP-DID-A100

EXPLANATORY NOTE

The purpose of the quality assurance section is to record the specifications, procedures, results, and other technical information related to quality assurance activities for either a product or a process. In general, quality assurance activities focus on conformance to standards and plans. The title of the section or volume should indicate the type of quality assurance activity. For example, the "Quality Assurance Products Reviews Volume of the Assurance Specification Document for the XYZ Software."

This Quality Assurance DID is applicable for information system, hardware, software, and operational procedures quality assurance activities. This DID is used (either as a separate volume or inline) for each quality assurance activity or group of quality assurance activities for a specific information system or component product, or a related process.

1.0 INTRODUCTION

The structure and content description to be used when preparing this section is described in detail in the Assurance Specification Template DID (SMAP-DID-A999).

2.0 RELATED DOCUMENTATION

The structure and content description to be used when preparing this section is described in detail in the Assurance Specification Template DID (SMAP-DID-A999).

3.0 SPECIFICATIONS

Specify the object of the quality assurance activities, such as an information system or component product or a related process, and the specific quality attributes for which it is being evaluated. Trace these quality assurance activities to the appropriate section of the management plan where plans for such activities were described and methods to be employed were given. Also, when appropriate, trace these quality assurance activities to either the appropriate requirements or design section(s) of the product specification or the process description in the management plan.

4.0 EVALUATION CRITERIA

Describe the overall criteria used for pass/fail evaluation of this quality assurance activity. When appropriate give a range of acceptability or numerical measures. The criteria should include the pass/fail point(s).

5.0 EVALUATION PROCEDURES

Describe the details required to conduct the specific quality assurance activity. State environment and set-up procedures.

6.0 MEASUREMENT AND EXPECTED RESULTS

Describe the specific measurement criteria against which the product or process is to be evaluated, such as the checklist with ranges of values. Describe the expected results of the quality assurance activities based on the specifications and quality goals. Where possible, based on the evaluation technique, give quantitative, expected results.

7.0 ACTUAL RESULTS

Include the actual results of the quality assurance activities. Include any action items or qualifiers based upon the results of the quality assurance activities. Also state the final evaluation (pass/fail) of these quality assurance activities based on the evaluation criteria given in Section 4. Note that if specified in the management plan, a summary of the quality assurance evaluation should be recorded in the appropriate management control and status report.

8.0 ABBREVIATIONS AND ACRONYMS

Refer to the Assurance Specification Template DID (SMAP-DID-A999) for the detailed description of content for this section.

9.0 GLOSSARY

Refer to the Assurance Specification Template DID (SMAP-DID-A999) for the detailed description of content for this section.

10.0 NOTES

Refer to the Assurance Specification Template DID (SMAP-DID-A999) for the detailed description of content for this section.

11.0 APPENDICES

Refer to the Assurance Specification Template DID (SMAP-DID-A999) for the specifications for appendices.

SMAP-DID-A200

TESTING

DATA ITEM DESCRIPTION

TABLE OF CONTENTS

ASSURANCE SPECIFICATION DOCUMENTATION STANDARD
TESTING DID: SMAP-DID-A200

EXPLANATORY NOTE

The purpose of a testing section is to record the specifications, procedures, and other technical information related to a test or a group of tests. The title of the section or volume should indicate the level, and if appropriate, type of test and the product being tested. For example, the "Acceptance Tests of the Acquirer's Assurance Specification of the XYZ System," or the "Unit Tests for the Developer's Assurance Specification of the Power Software of the XYZ System."

This testing DID is applicable at all levels of testing (unit, integration, acceptance, and validation) and the DID is applicable for information system, hardware, software, and operational procedures testing. This DID is used (either as a separate volume or inline) for each test or group of tests associated with a specific level of testing for a specific information system or component.

Different categories of testing may be performed by either an engineering or an assurance organization. While testing does assure a product, it may be a large undertaking, which requires the development of its own set of products, such as test procedures and test cases. Whether test products are developed by an engineering or an assurance organization, provisions should be made to have assurance also performed on the test products.

1.0 INTRODUCTION

The structure and content description to be used when preparing this section is described in detail in the Assurance Specification Template DID (SMAP-DID-A999).

2.0 RELATED DOCUMENTATION

The structure and content description to be used when preparing this section is described in detail in the Assurance Specification Template DID (SMAP-DID-A999).

3.0 TEST IDENTIFICATION AND SPECIFICATION

Identify the test, or set of tests. Provide a link between this test specification and the tests specified in the relevant management plan for this information system or component.

Describe the test objectives. For example, for software unit testing a test objective is to demonstrate that the detailed

design has been correctly represented in the code. For acceptance testing at the system level, the objective might be to determine that the system meets a selected set of requirements from the system product specification.

Describe the specific product specifications (requirements, design, etc.) that are to be demonstrated by this test. This specification should provide the appropriate traceability in the product specification (i.e., to detailed design for unit test, to architectural design for integration test, to requirements for acceptance test).

4.0 TEST CRITERIA

Describe the criteria used to determine the success or failure of the test(s) in terms such as:

- Accuracy
- Precision
- Limits and range boundaries
- Response time
- Acceptable failure rate by classes of failure

5.0 TEST PROCEDURES

Describe the procedures necessary to support the test(s) in terms such as:

- Specification of environment (support software, hardware, operational procedures, simulators, models, etc. required to support this test)
- Installation of probes for collecting test data
- Initialization of environment and software to be tested, such as setting flags, breakpoints, pointers, data, or control parameters
- Use of test tools such as test generator(s)
- Data recording or reduction procedures or measurement techniques
- Any special instructions for the test
- Action(s) to be taken by test operator particularly in the case of failures
- Recovery action to be taken in the event of an anomaly

6.0 TEST CASES AND EXPECTED RESULTS

Describe the test case(s) to be used in this test or set of tests in terms such as:

- Input name, value, and source including user inputs
- Required environment such as database(s) and database(s) contents
- Timing or event sequence such as a scenario

Describe the expected results from the test(s) in terms such as:

- Output name and value including messages or displays
- Event sequence or timing
- Resource consumption such as time, power, or storage

If this information is available in electronic form, it should be maintained in that form for possible future regression testing.

7.0 ACTUAL TEST RESULTS

Identify the particular version of the product tested and the specifics of the environment (support software, hardware, etc.) in which it was tested and the actual test date.

Describe the actual results from the test(s). The content and format of this section should mirror that of expected test results for ease of comparison.

A statement of the success or failure of this test, or set of tests, based on the criteria defined in Section 4, is given in a test report to management. The relevant test report (or set of reports) should be referenced in this section.

8.0 ABBREVIATIONS AND ACRONYMS

Refer to the Assurance Specification Template DID (SMAP-DID-A999) for the detailed description of content for this section.

9.0 GLOSSARY

Refer to the Assurance Specification Template DID (SMAP-DID-A999) for the detailed description of content for this section.

10.0 NOTES

Refer to the Assurance Specification Template DID (SMAP-DID-A999) for the detailed description of content for this section.

11.0 APPENDICES

Refer to the Assurance Specification Template DID (SMAP-DID-A999) for the specifications for appendices.

SMAP-DID-A300

QUALITY ENGINEERING ASSURANCE

DATA ITEM DESCRIPTION

TABLE OF CONTENTS

ASSURANCE SPECIFICATION DOCUMENTATION STANDARD
QUALITY ENGINEERING ASSURANCE DID: SMAP-DID-A300

EXPLANATORY NOTE

The purpose of the quality engineering assurance section is to record the specifications, procedures, results, and other technical information related to quality engineering assurance activities for products. In general, quality engineering assurance activities focus on assuring the proper implementation of quality factors or "-ilities." The title of the section or volume should indicate the type of quality engineering assurance activity. For example, the "Quality Engineering Reliability Volume of the Assurance Specification Document for the XYZ Software."

This Quality Engineering Assurance DID is applicable for information system, hardware, software, and operational procedures quality engineering assurance activities. This DID is used (either as a separate volume or inline) for each quality engineering assurance activity or group of quality engineering assurance activities for a specific information system or component product.

1.0 INTRODUCTION

The structure and content description to be used when preparing this section is described in detail in the Assurance Specification Template DID (SMAP-DID-A999).

2.0 RELATED DOCUMENTATION

The structure and content description to be used when preparing this section is described in detail in the Assurance Specification Template DID (SMAP-DID-A999).

3.0 SPECIFICATIONS

Specify the object of the quality engineering assurance activities, such as an information system or component product and the specific quality attributes for which it is being evaluated, such as maintainability, reliability, or other of the "ilities" quality factors or design goals. Trace these quality engineering assurance activities to the appropriate section of the management plan where plans for such activities were described and methods to be employed were given. Also, when appropriate, trace these quality engineering assurance activities to either the appropriate requirements or design section(s) of the product specification.

4.0 EVALUATION CRITERIA

Describe the overall criteria used for pass/fail evaluation of this quality engineering assurance activity. When appropriate give a range of acceptability or numerical measures. The criteria should include the pass/fail point(s).

5.0 EVALUATION PROCEDURES

Describe the details required to conduct the specific quality engineering assurance activity. State environment and set-up procedures.

6.0 MEASUREMENT AND EXPECTED RESULTS

Describe the specific measurement criteria against which the product or process is to be evaluated, such as the checklist with ranges of values. Describe the expected results of the quality engineering assurance activities based on the specifications and quality goals. Where possible, based on the evaluation technique, give quantitative, expected results.

7.0 ACTUAL RESULTS

Include the actual results of the quality engineering assurance activities. Include any action items or qualifiers based upon the results of the quality engineering assurance activities. Also state the final evaluation (pass/fail) of these quality engineering assurance activities based on the evaluation criteria given in Section 4. Note that if specified in the management plan, a summary of the quality engineering assurance evaluation should be recorded in the appropriate management control and status report.

8.0 ABBREVIATIONS AND ACRONYMS

Refer to the Assurance Specification Template DID (SMAP-DID-A999) for the detailed description of content for this section.

9.0 GLOSSARY

Refer to the Assurance Specification Template DID (SMAP-DID-A999) for the detailed description of content for this section.

10.0 NOTES

Refer to the Assurance Specification Template DID (SMAP-DID-A999) for the detailed description of content for this section.

11.0 APPENDICES

Refer to the Assurance Specification Template DID (SMAP-DID-A999) for the specifications for appendices.

SMAP-DID-A400

SAFETY ASSURANCE

DATA ITEM DESCRIPTION

TABLE OF CONTENTS

ASSURANCE SPECIFICATION DOCUMENTATION STANDARD
SAFETY ASSURANCE DID: SMAP-DID-A400

EXPLANATORY NOTE

The purpose of the safety assurance section is to record the specifications, procedures, results, and other technical information related to assuring that a product meets the safety classification specified in the management plan. The product is assured against the safety requirements specified in the product specification. The title of the section or volume should indicate type of safety assurance activity. For example, the "Safety Review Volume of the Assurance Specification Document for the Flight Software for the XYZ System."

This DID is used (either as a separate volume or inline) for each safety assurance activity or group of such assurance activities for a specific information system or component.

1.0 INTRODUCTION

The structure and content description to be used when preparing this section is described in detail in the Assurance Specification Template DID (SMAP-DID-A999).

2.0 RELATED DOCUMENTATION

The structure and content description to be used when preparing this section is described in detail in the Assurance Specification Template DID (SMAP-DID-A999).

3.0 SPECIFICATIONS

Specify the object of the safety assurance activities, such as an information system or component product and the specific quality attributes for which it is being evaluated. Trace these safety assurance activities to the appropriate section of the management plan where plans for such activities were described and methods to be employed were given. Also, when appropriate, trace these safety activities to either the appropriate requirements or design section(s) of the product specification (Note that one appropriate type of assurance activity is to review the safety requirements of an information system for completeness.)

4.0 EVALUATION CRITERIA

Describe the overall criteria used for the pass/fail evaluation of this safety assurance activity. When appropriate give a range of acceptability or numerical measures. The criteria should include the pass/fail point(s).

5.0 EVALUATION PROCEDURES

Describe the details required to conduct the specific safety assurance activity. State environment and set-up procedures.

6.0 MEASUREMENT AND EXPECTED RESULTS

Describe the specific measurement criteria against which the product is to be evaluated such as the safety check list with ranges of values. Describe the expected results of the safety assurance activities based on the specifications and safety goals. Where possible, based on the evaluation technique, give quantitative, expected results.

7.0 ACTUAL RESULTS AND EVALUATION

Include the actual results of the safety assurance activities. Include any action items or qualifiers based upon the results of the safety assurance activities. Also state the final evaluation (pass/fail) of these safety assurance activities based on the evaluation criteria given in Section 4. Note that if specified in the management plan, a summary of the safety assurance evaluation should be recorded in the appropriate management control and status report.

8.0 ABBREVIATIONS AND ACRONYMS

Refer to the Assurance Specification Template DID (SMAP-DID-A999) for the detailed description of content for this section.

9.0 GLOSSARY

Refer to the Assurance Specification Template DID (SMAP-DID-A999) for the detailed description of content for this section.

10.0 NOTES

Refer to the Assurance Specification Template DID (SMAP-DID-A999) for the detailed description of content for this section.

11.0 APPENDICES

Refer to the Assurance Specification Template DID (SMAP-DID-A999) for the specifications for appendices.

SMAP-DID-A500

SECURITY AND PRIVACY ASSURANCE

DATA ITEM DESCRIPTION

TABLE OF CONTENTS

ASSURANCE SPECIFICATION DOCUMENTATION STANDARD
SECURITY AND PRIVACY ASSURANCE DID: SMAP-DID-A500

EXPLANATORY NOTE

The purpose of the security and privacy assurance section is to record the specifications, procedures, results, and other technical information related to assuring that a product meets the security and privacy classification specified in the management plan. The product is assured against the security and privacy requirements specified in the product specification. The title of the section or volume should indicate type of security and privacy assurance activity. For example, the "Security Review Volume of the Assurance Specification Document for the Flight Software for the XYZ System."

This DID is used (either as a separate volume or inline) for each security and privacy assurance activity or group of such assurance activities for a specific information system or component.

1.0 INTRODUCTION

The structure and content description to be used when preparing this section is described in detail in the Assurance Specification Template DID (SMAP-DID-A999).

2.0 RELATED DOCUMENTATION

The structure and content description to be used when preparing this section is described in detail in the Assurance Specification Template DID (SMAP-DID-A999).

3.0 SPECIFICATIONS

Specify the object of the security and privacy assurance activities, such as an information system or component product, and the specific security and privacy attributes for which it is being evaluated. Trace these security and privacy assurance activities to the appropriate section of the management plan where plans for such activities were described and methods to be employed were given. Also, when appropriate, trace these security and privacy activities to either the appropriate requirements or design section(s) of the product specification. (Note that one appropriate type of assurance activity is to review the security and privacy requirements of an information system for completeness.)

4.0 EVALUATION CRITERIA

Describe the overall criteria used for the pass/fail evaluation of this security and privacy assurance activity. When appropriate give a range of acceptability or numerical measures. The criteria should include the pass/fail point(s).

5.0 EVALUATION PROCEDURES

Describe the details required to conduct the specific security and privacy assurance activity. State environment and set-up procedures.

6.0 MEASUREMENT AND EXPECTED RESULTS

Describe the specific measurement criteria against which the product is to be evaluated such as the security and privacy checklist with ranges of values. Describe the expected results of the security and privacy assurance activities based on the specifications and security and privacy goals. Where possible, based on the evaluation technique, give quantitative, expected results.

7.0 ACTUAL RESULTS AND EVALUATION

Include the actual results of the security and privacy assurance activities. Include any action items or qualifiers based upon the results of the security and privacy assurance activities. Also state the final evaluation (pass/fail) of these security and privacy assurance activities based on the evaluation criteria given in Section 4. Note that if specified in the management plan, a summary of the security and privacy assurance evaluation should be recorded in the appropriate management control and status report.

8.0 ABBREVIATIONS AND ACRONYMS

Refer to the Assurance Specification Template DID (SMAP-DID-A999) for the detailed description of content for this section.

9.0 GLOSSARY

Refer to the Assurance Specification Template DID (SMAP-DID-A999) for the detailed description of content for this section.

10.0 NOTES

Refer to the Assurance Specification Template DID (SMAP-DID-A999) for the detailed description of content for this section.

11.0 APPENDICES

Refer to the Assurance Specification Template DID (SMAP-DID-A999) for the specifications for appendices.

SMAP-DID-A600

VERIFICATION AND VALIDATION

DATA ITEM DESCRIPTION

TABLE OF CONTENTS

ASSURANCE SPECIFICATION DOCUMENTATION STANDARD
VERIFICATION AND VALIDATION DID: SMAP-DID-A600

EXPLANATORY NOTE

The purpose of the verification and validation section is to record the specific verification and validation technical assurance information (including criteria and expected and actual results) for an information system or component. The definition of the specific verification and validation activities to be conducted and the format of this section are specified in the product assurance planning section of the management plan.

1.0 INTRODUCTION

The structure and content description to be used when preparing this section is described in detail in the Assurance Specification Template DID (SMAP-DID-A999).

2.0 RELATED DOCUMENTATION

The structure and content description to be used when preparing this section is described in detail in the Assurance Specification Template DID (SMAP-DID-A999).

3.0 VERIFICATION SPECIFICATIONS

The purpose of this section is to record the specific technical verification information for an information system or a component. The organization of this section is dependent on the verification activities specified in the management plan. Verification is the process of demonstrating that the products and processes of a phase in the life-cycle are consistent with the products and processes of the previous phase (i.e. the job is being done right). Therefore, the internal organization of this section may be structured by life-cycle phases. The following topics should be covered for each major verification activity:

- Traceability specifications
- Verification criteria and procedures
- Measurement and expected results
- Actual results

If appropriate, the Quality Assurance DID (SMAP-DID-A100) can be used for substructure.

4.0 VALIDATION SPECIFICATIONS

The purpose of this section is to record the specific technical validation activities specified in the management plan for an information system or a component. The organization of this section is dependent on the validation activities specified in the management plan. Validation is the process of demonstrating that the final product meets the users or customer requirements (i.e. the right job was done). Emphasis is usually on independent testing. The following topics should be covered:

- o Specifications of the validation activities
- o Validation criteria and procedures
- o Validation expected and actual results

If appropriate (i.e., the emphasis is on testing), the Testing DID (SMAP-DID-A200) should be used for a detailed description of the content of this section. If testing is not the major activity, then the Quality Assurance DID (SMAP-DID-A100) can be used for substructure. Note that the Testing DID (SMAP-DID-A200) format should be used for each level or major class of tests.

5.0 ABBREVIATIONS AND ACRONYMS

Refer to the Assurance Specification Template DID (SMAP-DID-A999) for the detailed description of content for this section.

6.0 GLOSSARY

Refer to the Assurance Specification Template DID (SMAP-DID-A999) for the detailed description of content for this section.

7.0 NOTES

Refer to the Assurance Specification Template DID (SMAP-DID-A999) for the detailed description of content for this section.

8.0 APPENDICES

Refer to the Assurance Specification Template DID (SMAP-DID-A999) for the specifications for appendices.

SMAP-DID-A700

CERTIFICATION

DATA ITEM DESCRIPTION

TABLE OF CONTENTS

Section

ASSURANCE SPECIFICATION DOCUMENTATION STANDARD
CERTIFICATION DID: SMAP-DID-A700

EXPLANATORY NOTE

The purpose of the certification section is to record the specifications, procedures, results, and other technical information related to the certification of a product. The title of the section or volume should indicate the type of certification and object being certified. For example, the "Flight Certification Volume of the Assurance Specification Document for the XYZ System."

This Certification DID is applicable for information system, hardware, software, and operational procedures certification. This DID is used (either as a separate volume or inline) for each certification activity or group of certification activities for a specific information system or component.

1.0 INTRODUCTION

The structure and content description to be used when preparing this section is described in detail in the Assurance Specification Template DID (SMAP-DID-A999).

2.0 RELATED DOCUMENTATION

The structure and content description to be used when preparing this section is described in detail in the Assurance Specification Template DID (SMAP-DID-A999).

3.0 SPECIFICATIONS

Specify the object of the certification activities, such as an information system or component product, and the specific certification attributes for which it is being evaluated. Trace these certification activities to the appropriate section of the management plan where plans for such activities were described and methods to be employed were given. (The information in the management plan should include the granting agency and form of certification.) Also trace to appropriate product specification.

4.0 CRITERIA

Describe the overall criteria used for pass/fail evaluation of this certification activity. When appropriate give a range of acceptability or numerical measures. The criteria should include the pass/fail point(s).

5.0 PROCEDURES

Describe the details required to conduct the specific quality assurance activities. State environment(s) and give set-up procedures.

6.0 MEASUREMENT AND EXPECTED RESULTS

Describe the specific measurement criteria against which the product is to be evaluated such as the checklist with ranges of values. Describe the expected results of the certification activities based on the specifications and safety or security goals. Where possible, based on the evaluation technique, give quantitative, expected results.

7.0 ACTUAL RESULTS

Include the actual results of the certification activities. Include any action items or qualifiers based upon the results of the certification activities. Also state the final evaluation (pass/fail) of these certification activities based on the evaluation criteria given in Section 4. Note that if specified in the management plan, a summary of the certification evaluation should be recorded in the appropriate management control and status report.

8.0 ABBREVIATIONS AND ACRONYMS

Refer to the Assurance Specification Template DID (SMAP-DID-A999) for the detailed description of content for this section.

9.0 GLOSSARY

Refer to the Assurance Specification Template DID (SMAP-DID-A999) for the detailed description of content for this section.

10.0 NOTES

Refer to the Assurance Specification Template DID (SMAP-DID-A999) for the detailed description of content for this section.

11.0 APPENDICES

Refer to the Assurance Specification Template DID (SMAP-DID-A999) for the specifications for appendices.

SMAP-DID-A999

ASSURANCE SPECIFICATION TEMPLATE

DATA ITEM DESCRIPTION

TABLE OF CONTENTS

ASSURANCE SPECIFICATION DOCUMENTATION STANDARD
ASSURANCE SPECIFICATION TEMPLATE DID: SMAP-DID-A999

EXPLANATORY NOTE

The purpose of the template is to describe the set of common sections that are to appear in the document specified by this documentation standard and in any rolled-out volumes. When using this template for the document itself, rather than for a rolled-out volume, substitute "Document" for "Volume" in the following.

1.0 INTRODUCTION

1.1 Identification of Volume

Identify this physical volume in terms of its relationship to the parent document(s) in the documentation set for this information system or component. For documentation set documents, identify the parent(s) in the decomposition tree for the information system. For example:

"This is the Assurance Specification for the XYZ Information System."

"This is the Independent Verification and Validation Volume of the XYZ Information System Assurance Specification."

1.2 Scope of Volume

Describe the area of cognizance, responsibility, and applicability for this volume.

1.3 Purpose and Objectives of Volume

Describe the purpose and objectives for this volume concisely and in specific terms.

1.4 Volume Status and Schedule

Describe the status, including goals and dates, for production or revision of the volume. Documentation is often generated incrementally or iteratively. If this is the case for this volume, also summarize here the planned updates and their release dates.

1.5 Volume Organization and Roll-Out

Briefly describe what is presented in each major section within this version of the volume and what is in each appendix.

If any sections are rolled-out into subordinate volumes of this volume, then cite those volumes and provide a documentation tree pointing to the subordinate volumes and relating them to the parent.

2.0 RELATED DOCUMENTATION

The purpose of this section is to provide the references or bibliography for this volume.

Cite documents by short or common title (if any), full title, version or release designator (if appropriate), date, publisher or source, and document number or other unique identifier.

2.1 Parent Documents

Begin this section as follows, depending upon whether this is a volume of a document or the document itself:

> "The following document(s) is (are) parent to this volume:"
>
> or:
>
> "The following document(s) is (are) the parent from which this document's scope and content derive:"

If this is a document, cite the appropriate document at the next higher level. For example, an Information System Management Plan would cite the management plan for the next higher level information system, or the Software Product Specification would cite the Software Management Plan and the parent's product specification. If there is no higher level, state "None." here.

If this is a volume rolled-out from a document, cite that document. If this is a volume rolled-out from another volume, cite each volume in the hierarchical path back to the parent document, starting with the volume immediately superior to this one.

2.2 Applicable Documents

Begin this section as follows:

> "The following documents are referenced herein and are directly applicable to this volume:"

Provide the citations for every document (other than the parent) referenced within this volume, or which are directly applicable, or contain policies or other directive matters that are binding upon the content of this volume.

2.3 Information Documents

Begin this section as follows:

> "The following documents, although not directly applicable, amplify or clarify the information presented in this volume, and are not binding:"

or, use an appropriate introduction to indicate the relationship of the documents listed here to this volume.

3.0 - N.0 CONTENT FOR ROLLED-OUT SECTION

Each major subsection of the section of an information system or component assurance specification, or of a volume thereof, being rolled-out into a separate subordinate volume becomes a major section in the rolled-out volume.

N+1.0 ABBREVIATIONS AND ACRONYMS

This section follows the sections containing the content for the rolled-out section.

The abbreviations and acronyms section contains an alphabetized list of the definitions for abbreviations and acronyms used in this volume.

N+2.0 GLOSSARY

The glossary contains an alphabetized list of definitions for special terms used in the volume; i.e., terms used in a sense that differs from or is more specific than the common usage for such terms.

N+3.0 NOTES

Use this section to present information that aids in understanding the information provided in previous sections, and which is not contractually binding.

N+4.0 APPENDICES

The appendices contain material that is too bulky, detailed, or sensitive to be placed in the main body of text. Refer to each appendix in the main body of the text where the information applies. Appendices may be bound separately, but are considered to be part of the volume and shall be placed under configuration control as such.

8.0 ABBREVIATIONS AND ACRONYMS

AR - Acceptance Review

CDR - Critical Design Review

COTS - Commercial off-the-shelf

DID - Data Item Description

DoD - Department of Defense

DRL - Data Requirements List

ECP - Engineering Change Proposal

EPROM - Erasable Programmable Read-Only Memory

FCA - Functional Configuration Audit

FMEA - Failure Modes and Effects Analysis

GFE - Government-furnished equipment

IV&V - Independent Verification and Validation

LRU - Line (or Lowest) Replaceable Unit

MTBF - Mean Time Between Failures

MTTR - Mean Time to Repair

NASA - National Aeronautics and Space Administration

NHB - NASA Handbook

NRCA - Nonconformance Reporting and Corrective Action

PCA - Physical Configuration Audit

PDR - Preliminary Design Review

PROM - Programmable Read-Only Memory

RFP - Request for Proposal

RID - Review Item Discrepancy

ROM - Read-Only Memory

RR - Requirements Review

SMAP - Software Management and Assurance Program

SOW - Statement of Work

SRM&QA - Safety, Reliability, Maintainability, and Quality Assurance

SSE - Software Support Environment of the Space Station Freedom Program

SSFP - Space Station Freedom Program

STD - Standard

TBD - To be determined (at a later date)

TMIS - Technical and Management Information System of the Space Station Freedom Program

TRR - Test Readiness Review

V&V - Verification & Validation.

WBS - Work Breakdown Structure

9.0 GLOSSARY

For terms not appearing in this glossary, refer to the IEEE Standard Glossary (as referenced in Section 2.2).

Acceptance Review - The phase transition review for the Acceptance and Delivery life-cycle phase.

Acquirer - An organization that acquires a capability, such as an information system.

Adaptation - The tailoring of the life-cycle and documentation standards (within the specifications of the rules and guidelines) for a specific program/project, information system, or component.

Allocation - The process of apportioning requirements at one level in the decomposition tree to the subsystems or subcomponents at the next lower level in the decomposition.

Assembly - A physical element of a hardware component consisting of one or more line replaceable units. A hardware component is composed of one or more physical assemblies.

Assurance - Includes any and all activities, independent of organization conducting the activity, that demonstrate the conformance of a product to a prespecified criteria (such as to a design or to a standard).

Assurance Specification - One of the four documents in the documentation set for an information system or component; it encompasses all the technical (i.e., non-planning) aspects of the assurance activities for an information system or component.

Baselining - The official acceptance of a product or its placement under configuration management as defined in the management plan.

Code Q - (NASA) Office of Safety, Reliability, Maintainability, and Quality Assurance

Component - 1) One of the three parts making up an information system: software, hardware, or operational procedures. 2) A portion of a higher-level component of the same type; e.g., a component of the software component (of an information system).

Critical Design Review - The phase transition review for the Detailed Design life-cycle phase.

ASSURANCE SPECIFICATION DOCUMENTATION STANDARD GLOSSARY

Data Item Description - The table of contents and associated content description of a document or volume.

Design Element - An identifiable part of a component's architectural design.

Developer - The provider organization responsible for development of an information system or of a hardware, software, or operational procedures component.

Document - One of the four basic types of information for each information system or component: 1) Management Plan, 2) Product Specification, 3) Assurance Specification, and 4) Management Control and Status Reports Document. A document consists of one or more volumes.

Documentation Set - The four basic documents for each information system or component thereof.

Evolutionary Acquisition - The acquisition of an information system over a relatively long period of time in which two or more complete iterations of the life-cycle will be employed to revise and extend the system to such an extent as to require a major requirements analysis and therefore subsequent life-cycle iterations.

Increment - A pre-defined set of units integrated for integration testing by the development organization in response to incremental development plans.

Incremental Development - The process of developing a product before delivery in a series of segments. These segments remain internal to the development organization. The process is used to avoid the big bang approach to software development and help minimize risk. The segments are defined based on the design and documented in the design section of the product specification. The process leads to a single delivery unless used in conjunction with "phased delivery."

Independent Verification and Validation - Verification and validation performed by an independent organization. In general, this is intended to be independent of the development organization. For complete independence, the IV&V organization must report directly to or be funded directly by the acquirer.

Information System - 1) Any system composed of hardware, software, and operational procedures components required to process, store, and/or transmit data. 2) An integrated combination of software, hardware, and operational procedures components that provides a useful capability. An information system is generally software-intensive.

Inheritables - Existing software or hardware to be drawn upon in developing a new information system. The inheritables may be modified to meet the new system's requirements.

Instantiate - 1. To represent an abstraction by a concrete instance (e.g., heroes instantiate ideals). 2. Within Ada, the process of creating an instance of a generic subprogram or package.

Line Replaceable Unit - A hardware unit that is part of an assembly that is defined to be the lowest replaceable element of a hardware component. An assembly is composed of one or more LRUs.

Management Control and Status Reports Document - One of the documents in the documentation set for an information system or component; it represents a "logical" home for all report and request forms.

Management Plan - One of the four documentation set documents; it encompasses all planning information for an information system or component, including management, engineering, and assurance planning.

Partitioning - The process of determining the content for each delivery when using the phased delivery approach, or for determining the content of each segment when using incremental development.

Phase (of a life-cycle) - A set of activities and associated products and reviews that make up one step of a multi-step process for developing systems and their component. An information system life-cycle has seven standard phases: 1) Concept and Initiation; 2) Requirements; 3) Design; 4) Implementation Coordination (or Implementation or Fabrication); 5) Integration and Test; 6) Acceptance Test; and 7) Sustaining Engineering and Operations. In some cases, phase 3 contains multiple levels of design, such as architectural and detailed.

Phase Transition Review - The review at the end of a phase triggering transition to the next phase.

Phased Delivery - The process of developing and delivering a product in stages, each providing an increasing capability for an information system or component. The process may be employed to provide an early operational capability to users, for budgetary reasons, or because of risk, size, or complexity Each delivery must undergo acceptance testing prior to release for operational use. The capabilities provided in each delivery are determined by prioritizing and partitioning

the requirements. This must be documented in the requirements section of the product specification.

Preliminary Design Review - The phase transition review for the Architectural Design life-cycle phase.

Product Specification - One of the four documentation set documents for an information system or component; it encompasses all the engineering and technical support information related to the development of an information system or component.

Prototyping - A process used to explore alternatives and minimize risks. Prototyping can be used in any life-cycle phase. The product of the process is a report. By-products (such as software, hardware, and models) of the process can be preserved for subsequent use.

Provider - An organization providing a capability to an acquirer; e.g., the developer or an organization providing independent verification and validation.

Quality Assurance - A subset of the total assurance activities generally focused on conformance to standards and plans. In general, these assurance activities are conducted by the SRM&QA organization.

Quality Engineering - The process of incorporating reliability, maintainability, and other quality factors into system, hardware, software, and operational procedures products.

Repository - A collection of standards, procedures, guides, practices, rules, etc. that supplements information contained in the documentation set for an information system or component. In general, the documentation set describes "what" is to be done and the repository provides the "how-to" instructions. A repository usually contains information that is applicable to multiple information systems and components.

Requirements Allocation - The process of distributing requirements of an information system or component to subordinate information systems (subsystems) or components.

Requirements Partitioning - The process of distributing requirements of an information system or component to different deliveries in support of phased delivery.

Requirements Review - The phase transition review for the Requirements life-cycle phase.

Review Item Discrepancy - A type of discrepancy report used when reviewing documentation.

Risk - The combined effect of the likelihood of an unfavorable occurrence and the potential impact of that occurrence.

Risk Management - The process of assessing potential risks and reducing those risks within dollar, schedule, and other constraints.

Roll-out - A mechanism for recording sections of a document in physically separate volumes while maintaining traceability and links. When using roll-out, a volume is subordinate to a parent document or volume.

Software Management and Assurance Program - Sponsored by NASA Code Q to foster more effective and productive software engineering methodologies.

Subsystem - In the information system decomposition context, a subsystem is an information system that is subordinate to a higher level information system and is parent to software, hardware, and operational procedures components, or to other (lower level) information systems.

Template - Within these Standards, a template is a DID framework used in the roll-out process for defining the specific format of a section rolled-out into a physically separate volume.

Test Readiness Review - The phase transition review for the Integration and Testing life-cycle phase.

Testing - The process of exercising or evaluating an information system or component by manual or automated means to demonstrate that it satisfies specified requirements or to identify differences between expected and actual results.

Tool - A hardware device or computer program used to help develop, test, analyze, or maintain another device or computer program or its documentation. (IEEE Std 729-1983)

Unit - An identifiable part of a detailed design. A level of decomposition for the purpose of physical design and implementation for a software or hardware component.

Validation - 1) Assurance activities conducted to determine that the requirements for a product are correct; i.e. to build the right product. 2) (IEEE Std 729-1983) The process of evaluating software at the end of the software development process to ensure compliance with software requirements.

Verification - 1) Assurance activities conducted to determine that a product is being built correctly in accordance with design and requirements specifications; i.e., to build the product right. 2) (IEEE Std 729-1983) "The process of determining whether or not the products of a given phase of ... development ... fulfill the requirements established during the previous phase."

Volume - A physically separate section of one of the four documents in a documentation set.

10.0 NOTES

None.

11.0 APPENDICES

APPENDIX A

ASSURANCE SPECIFICATION DOCUMENT SAMPLE OUTLINE

EXPLANATORY NOTE

The purpose of the assurance specification document is to document all the technical information (such as specification and criteria) related to assuring an information system or component. The types of assurance and the organizations responsible for performing that assurance are specified in the associated management plan.

This sample outline contains the complete substructure of all the Section 7 DIDs "rolled-up" into a document that consists of a single volume. Note that this instantiation only provides one level of testing each for acquirer and providers. All levels of substructure may not be required for a single-volume assurance specification.

TABLE OF CONTENTS

3.2 Testing
3.2.1 Test Identification and Specification
3.2.2 Test Criteria
3.2.3 Test Procedures
3.2.4 Test Cases and Expected Results
3.2.5 Actual Test Results
3.3 Quality Engineering Assurance
3.3.1 Specifications
3.3.2 Evaluation Criteria
3.3.3 Evaluation Procedures
3.3.4 Measurements and Expected Results
3.3.5 Actual Results
3.4 Safety Assurance
3.4.1 Specifications
3.4.2 Evaluation Criteria
3.4.3 Evaluation Procedures
3.4.4 Measurements and Expected Results
3.4.5 Actual Results
3.5 Security and Privacy Assurance
3.5.1 Specifications
3.5.2 Evaluation Criteria
3.5.3 Evaluation Procedures
3.5.4 Measurement and Expected Results
3.5.5 Actual Results
3.6 Verification and Validation
3.6.1 Verification Specifications
3.6.2 Validation Specifications
3.7 Certification
3.7.1 Specifications
3.7.2 Certification Criteria
3.7.3 Certification Procedures
3.7.4 Measurement and Expected Results
3.7.5 Actual Results

4.0 DEVELOPMENT PROVIDER'S ASSURANCE

4.1 Quality Assurance
4.1.1 Specifications
4.1.2 Evaluation Criteria
4.1.3 Evaluation Procedures
4.1.4 Measurement and Expected Results
4.1.5 Actual Results
4.2 Testing (note only one level of testing)
4.2.1 Test Identification and Specification
4.2.2 Test Criteria
4.2.3 Test Procedures
4.2.4 Test Cases and Expected Results
4.2.5 Actual Test Results
4.3 Quality Engineering Assurance
4.3.1 Specifications
4.3.2 Evaluation Criteria
4.3.3 Evaluation Procedures

4.3.4 Measurements and Expected Results
4.3.5 Actual Results
4.4 Safety Assurance
4.4.1 Specifications
4.4.2 Evaluation Criteria
4.4.3 Evaluation Procedures
4.4.4 Measurements and Expected Results
4.4.5 Actual Results
4.5 Security and Privacy Assurance
4.5.1 Specifications
4.5.2 Evaluation Criteria
4.5.3 Evaluation Procedures
4.5.4 Measurement and Expected Results
4.5.5 Actual Results
4.6 Verification and Validation
4.6.1 Verification Specifications
4.6.2 Validation Specifications
4.7 Certification
4.7.1 Specifications
4.7.2 Certification Criteria
4.7.3 Certification Procedures
4.7.4 Measurement and Expected Results
4.7.5 Actual Results

5.0 SUSTAINING ENGINEERING AND OPERATIONS PROVIDER'S ASSURANCE
(This section is included in the Assurance Specification Document only for an information system)

5.1 Quality Assurance
5.1.1 Specifications
5.1.2 Evaluation Criteria
5.1.3 Evaluation Procedures
5.1.4 Measurement and Expected Results
5.1.5 Actual Results
5.2 Testing
5.2.1 Test Identification and Specification
5.2.2 Test Criteria
5.2.3 Test Procedures
5.2.4 Test Cases and Expected Results
5.2.5 Actual Test Results
5.3 Quality Engineering Assurance
5.3.1 Specifications
5.3.2 Evaluation Criteria
5.3.3 Evaluation Procedures
5.3.4 Measurements and Expected Results
5.3.5 Actual Results
5.4 Safety Assurance
5.4.1 Specifications
5.4.2 Evaluation Criteria
5.4.3 Evaluation Procedures

5.4.4 Measurements and Expected Results
5.4.5 Actual Results
5.5 Security and Privacy Assurance
5.5.1 Specifications
5.5.2 Evaluation Criteria
5.5.3 Evaluation Procedures
5.5.4 Measurement and Expected Results
5.5.5 Actual Results
5.6 Verification and Validation
5.6.1 Verification Specifications
5.6.2 Validation Specifications
5.7 Recertification
5.7.1 Specifications
5.7.2 Certification Criteria
5.7.3 Certification Procedures
5.7.4 Measurement and Expected Results
5.7.5 Actual Results

6.0 ABBREVIATIONS AND ACRONYMS

7.0 GLOSSARY

8.0 NOTES

9.0 APPENDICES