



# ***Streamlining DITSCAP Documentation***

**Steve Welke**

Manager, Security Accreditation

[swelke@TrustedCS.com](mailto:swelke@TrustedCS.com)

January 2000

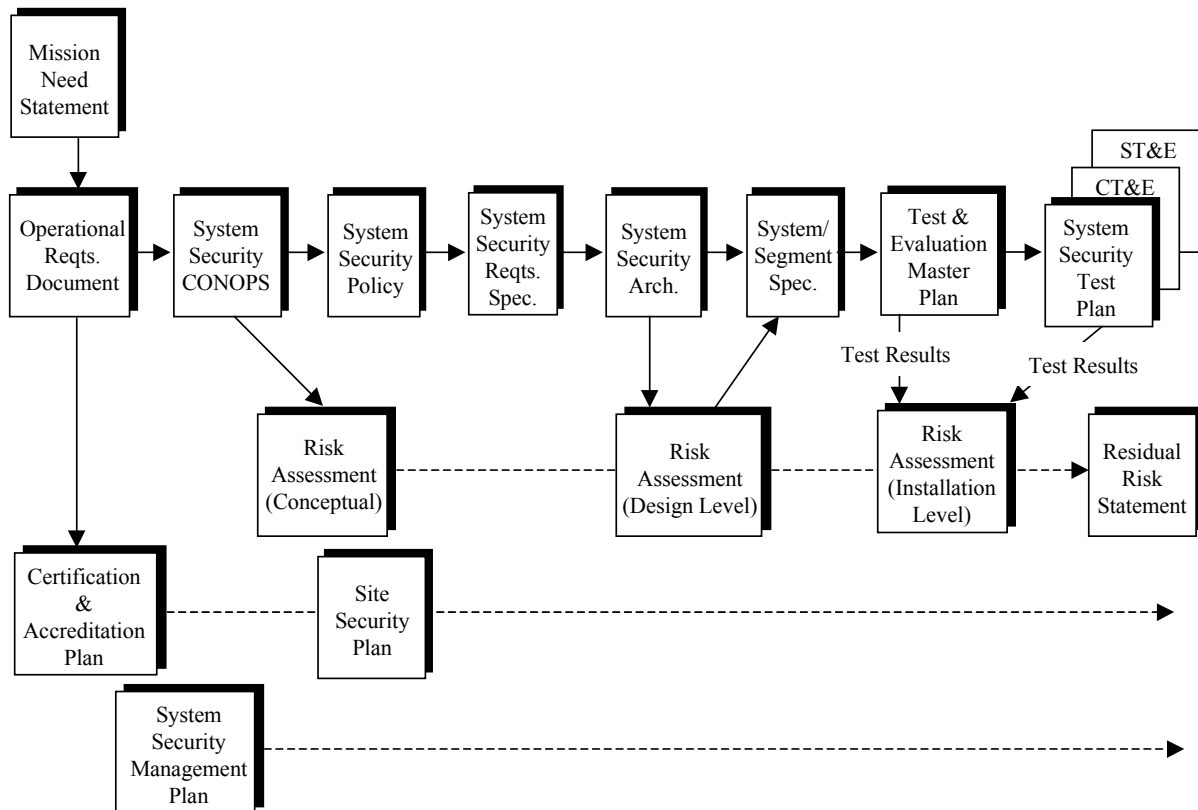
Trusted Computer Solutions, Inc.  
2350 Corporate Park Drive, Suite 500  
Herndon, VA 20171 USA  
+1.703.318.7134 (Phone)  
+1.703.318.5041 (Fax)  
[www.TrustedCS.com](http://www.TrustedCS.com)

***White Paper***

# Streamlining DITSCAP Documentation

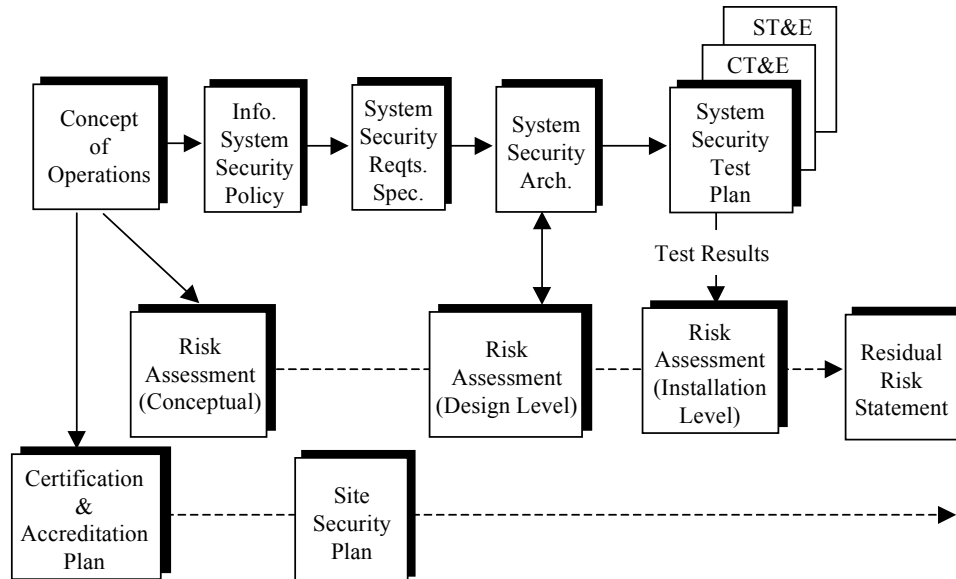
Steve Welke  
 Manager, Security Accreditation  
 Trusted Computer Solutions, Inc.  
 2350 Corporate Park Drive, Suite 500  
 Herndon, VA 20171 USA  
 +1.703.318.7134 (Phone)  
 +1.703.318.5041 (Fax)  
 swelke@TrustedCS.com

The Defense Information Systems Agency (DISA), in coordination with the National Security Agency (NSA) and the Services and Agencies throughout the Department of Defense (DoD), has developed a standard process to minimize the risks associated with non-standard security implementations across shared infrastructures and end systems. The DoD Information Technology Security Certification and Accreditation Process (DITSCAP) integrates security directly into the system lifecycle and is designed so that it can be applied uniformly across DoD. Figure 1 illustrates the relationships between the various information security (INFOSEC) documents that support the DITSCAP.



**Figure 1. Relationships Between the DITSCAP INFOSEC Documents.**

Trusted Computer Solutions (TCS) conducted an extensive review of the “preparation guides” that DISA developed to explain what information should be in each of the documents identified in Figure 1. Based on this review and on experience with reading and writing similar documents in the past, TCS developed an interpretation of the DITSCAP INFOSEC documents as shown in Figure 2. As described in the rest of this paper, this interpretation captures all of the information identified in the DISA guides. The benefits of the interpreted documentation set include elimination of redundancy and grouping of information in a more beneficial manner.



**Figure 2. TCS Interpretation of the DITSCAP Document Set.**

As a final introductory note, the Secret and Below Interoperability (SABI) initiative has developed its own set of appendices to meet the requirements in the DITSCAP. The TCS interpretation of the DITSCAP satisfies this set of SABI appendices as show in Table 1.

**Table 1: Audience and Purpose for Each C&A Document.**

SABI Appendix	SABI Name	TCS Mapping
A	Acronyms	same
B	Definitions	same
C	References	same
D	Security Requirements Traceability Matrix	SSRS
E	ST&E Plan and Procedures	same
F	Certification Results	same
G	Risk Assessment Results	RRA
H	CA Recommendation	same
I	System Rules of Behavior	same
J	Contingency Plan(s)	points to App S or M
K	Security Awareness and Training Plan	points to App S

**Table 1: Audience and Purpose for Each C&A Document.**

<b>SABI Appendix</b>	<b>SABI Name</b>	<b>TCS Mapping</b>
L	Personnel Controls and Technical Security Controls	points to App S
M	Incident Response Plan	same or points to App S
N	Memorandums of Agreement	same
O	Applicable Artifacts	same
P	Accreditation Documentation/Statement	same
[Q]	–	CONOPS
[R]	–	ISSP
[S]	–	SSP
[T]	–	SSA
[U]	–	CT&E P&P
[V]	–	SSTP (points to App E and U)
[W]	–	C&A Plan

## **1. Concept of Operations (CONOPS)**

The CONOPS describes the security-relevant information about the system that will influence the security policy, security architecture, security requirements, security design, and secure operation of the system. The mission needs statement, operational requirements, system CONOPS, and security CONOPS have been incorporated into this one document to provide clarity and avoid duplication. The CONOPS contains the following chapters:

1. Introduction
2. Mission Need [most info from the MSN (i.e., threat description, system criticality, and constraints)]
3. Operational Requirements [from the ORD]
4. System Description [high-level]
5. System Operation Considerations [formerly “Detailed Security Concepts”; includes integrated logistics support, infrastructure support, force considerations, and schedule considerations from the ORD]
6. Environment Operation Considerations [formerly “Environment Security Considerations”]

The CONOPS is the first of the required information system accreditation documents, and all remaining documents flow from, and are based on, the information it provides. The CONOPS is a dynamic document that will be updated as new information is captured.

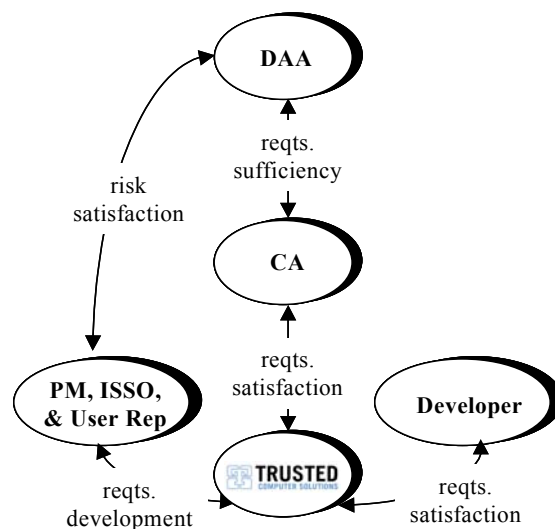
## **2. Certification and Accreditation Plan (C&A Plan)**

The C&A Plan identifies the roles and responsibilities for accrediting the system. The C&A Plan forms the basis for what activities will be performed and what documents will be produced by

whom at different stages of the DITSCAP. It contains all of the information in the System Security Management Plan (SSMP), so the SSMP can be eliminated. The C&A Plan contains the following chapters:

1. Introduction
2. C&A Approach
3. C&A Roles and Responsibilities [not sure if the roles identified capture the DAA, CA, PM, and User Representative – at least these four must be captured]
4. C&A Activities [formerly “Certification and Accreditation Plan”]
5. Document Responsibilities [eliminate configuration management]
6. Schedule and Milestones

Figure 3 illustrates the relationships between the four key roles in the DITSCAP.



**Figure 3. Relationships Between the Four Key DITSCAP Roles.**

### 3. Information System Security Policy (ISSP)

The ISSP defines the set of security rules that must be enforced by the system and its environment. It is derived from the information presented in the CONOPS and from DoD, Service, and Agency policy. The ISSP contains the following chapters:

1. Introduction [eliminated System Description (see CONOPS)]
2. General INFOSEC Policy Statements [combines “System Policy Implementation” section from CONOPS with “System Security Objectives” section in this doc]
3. Specific INFOSEC Policy Statements [new section to capture the policy statements that are specific to the particular system user]
4. Security Policy Interface Considerations

The ISSP is the second of the required information system accreditation documents. It is independent from the design and implementation of the system, and its set of rules is static throughout the system's life cycle.

#### **4. System Security Requirements Specification (SSRS)**

The SSRS consolidates system functional and security requirements as documented by the system's CONOPS, ISSP, and SSP. The SSRS contains the following chapters:

1. Introduction
2. INFOSEC Requirements [eliminate applicable documents, qualifications, preparation for delivery, and threats]
3. Rationale for Selected Requirements [new section to validate identified requirements]
4. Requirements Traceability Tables [track requirements to tests]

#### **5. Site Security Plan (SSP)**

The SSP overviews the system's security procedures and the agency's plan for providing those procedures at a specific site. The system PM develops the SSP early in the life cycle to define the basic security parameters for the system. Because the early system concept may need further refinement, the initial SSP may be incomplete. At a minimum, however, the organizational descriptions, user clearance issues, classifications of data, and proposed mode of operation should be included in the earliest version of the plan. The SSP contains the following chapters:

1. Introduction [eliminate background and requirements]
2. Administrative Procedures
3. Environment Procedures
4. Technical Procedures

#### **6. Residual Risk Assessment (RRA)**

The RRA quantifies the level of risk associated with operating the system. Vulnerabilities and countermeasures of the system are accounted for when determining the level of risk. The RRA evolves as the C&A process proceeds. It contains the following chapters:

1. Introduction
2. Risk Assessment [eliminate system description and vulnerabilities]
3. Recommendations, Plans, and Countermeasures

#### **7. System Security Architecture (SSA)**

The SSA flows from the CONOPS, the ISSP, the SSP, and the SSRS. The SSA maps security policy statements, security requirements, and operational capabilities and functionality from these documents to specific architecture components. The System/Segment Specification (SSS) is too detailed, so it can be eliminated. The SSA contains the following chapters:

1. Introduction

2. Approach
3. Security Functions
4. System Components

## **8. System Security Test Plan (SSTP)**

The SSTP defines the high-level security testing approach, objectives, and procedures for a system. This document can also serve as a program management tool for scheduling activities and resources and as a technical specification for the execution of security testing (e.g., CT&E or ST&E). The SSTP contains all of the information in the Test and Evaluation Master Plan (TEMP), so the TEMP can be eliminated. The SSTP contains the following chapters:

1. Introduction
2. Test and Evaluation Approach
  - Developmental Test and Evaluation (DT&E) [functional/development tests in lab]
  - Certification Test and Evaluation (CT&E) [technical tests in lab]
  - Security Test and Evaluation (ST&E) [non-technical tests at site]
  - Operational Test and Evaluation (OT&E) [operational tests at site]
3. Test and Evaluation Summary

## **9. Certification Test and Evaluation (CT&E) Plan**

The CT&E Plan defines the approach to conducting CT&E (technical testing) and contains the CT&E test cases. The CT&E Plan contains the following chapters:

1. Introduction
2. CT&E Planning
3. CT&E Execution

## **10. Security Test and Evaluation (ST&E) Plan**

The ST&E Plan defines the approach to conducting ST&E (non-technical testing) and contains the ST&E test cases. The ST&E Plan contains the following chapters:

1. Introduction
2. ST&E Planning
3. ST&E Execution