



## DATA SHEET

### KEY FEATURES

*VeriSign solutions for DITSCAP compliance are based on standardized government processes, including regulations such as:*

- Office of Management and Budget (OMB) Circular A-130, Appendix III as well as other pertinent OMB memorandum and circulars
- The Computer Security Act of 1987
- The Privacy Act of 1974
- The National Institute of Standards and Technology (NIST) Special Publications 800 Series
- The Federal Information Security Management Act (FISMA) of 2002
- Presidential Decision Directive (PDD) 63 and 67
- FIPS Publications (102, 199, etc.)
- The Department of Defense (DoD) Information Technology Security Certification and Accreditation Process (DITSCAP)
- Director of Central Intelligence (DCI) Directive 6/3
- The National Security Agency Information Systems Certification and Accreditation Process (NISCAP)
- Commercial practices such as ISO 17799 as well as agencies' specific policies, standards, and procedures.

## VeriSign Information Assurance — DITSCAP

Government agencies are faced with a multitude of regulations that require efforts to ensure the confidentiality, integrity, and availability of information resources. VeriSign assists agencies in addressing industry best practices and provides expert Certification and Accreditation (C&A) solutions delivered by experienced specialists in federal IT security.

### + The VeriSign DITSCAP Methodology

The VeriSign DITSCAP (DoD Information Technology Security Certification and Accreditation Process) methodology incorporates activities, general tasks, and a defined management structure to help customers obtain and maintain enterprise-based C&A for their information system infrastructure and applications.

The assessment methodology is sufficiently flexible to evaluate systems in all lifecycle stages, systems under evolutionary development, and single-purpose or legacy systems, for as long as they exist.

Each phase in the VeriSign DITSCAP methodology consists of a set of well-defined tasks and subtasks. Standardized assessment methods and procedures promote more consistent, comparable, and repeatable security assessments of the information systems.

The assessment methods and procedures that VeriSign employs during the assessment include:

- Interviewing agency personnel associated with the security aspects of the system
- Reviewing and examining security-related policies, procedures, and documentation
- Observing security-related activities and operations
- Analyzing, testing, and evaluating the security-relevant and security-critical aspects of system hardware, software, firmware, and operations
- Conducting demonstrations and exercises



Where it all comes together.™

**KEY BENEFITS**

*Reliable Results*

Standardized assessment methods and procedures enable more consistent, comparable, and repeatable assessments of security controls in federal information systems.

*Global Picture*

Comprehensive assessment promotes a better understanding of agency-related mission risks resulting from the operation of information systems.

*Informed Decision-Making*

The VeriSign C&A methodology helps create more complete, reliable, and trustworthy information to facilitate authorizing officials in making more informed security accreditation decisions.

The following table provides an overview of the VeriSign DITSCAP Certification and Accreditation methodology, including the tasks associated with each phase in the process. These phases map directly to the DITSCAP phases.

PHASE 1 DEFINITION	PHASE 2 VERIFICATION	PHASE 3 VALIDATION	PHASE 4 POST ACCREDITATION
Analyze	Initial Certification Analysis • System Architecture • Software Design • Network Connection • Product Integrity • Lifecycle Management	Certification/Evaluation • Certification Test & Evaluation • Security Test & Evaluation • Penetration Testing • System Mgmt. Analysis • Site Accreditation Survey	Maintain Accreditation
Develop Mission	Vulnerability Assessment	Contingency Plan	System Changes
Needs Registration	Prepare Security and Certification	Risk Mgmt Review	Change Management
Negotiation	Test and Evaluation Plan	Develop Accreditation Recommendation	Compliance Validation

Table 1. The VeriSign DITSCAP Methodology

VeriSign tailors these phases to apply a level of effort and rigor that is suitable for each information system undergoing security certification and accreditation.

Frequently, VeriSign will use its expertise to create assessment methods and procedures for specific security controls employed by agencies. Assessment methods and procedures may need to be tailored, in some instances, for specific information-system implementations.

Phase 1 – Definition

In the Definition phase, VeriSign defines the levels of effort in the C&A; identifies the Certifying Authority (CA), the Designated Approval Authority (DAA), the system Program Manager (PM), and the user representative; and documents the system mission, target environment, architecture, and threats. Then, VeriSign identifies the security system requirements based on classification, data types, users, and threats.

Phase 2 – Verification

The activities performed by VeriSign in the Verification phase are designed to verify whether the developed system complies with the requirements agreed on in Phase 1.

Phase 3 – Validation

In Phase 3, VeriSign validates that the system operates as described with an acceptable level of risk. System testing occurs in this phase, and the System Security Authorization Agreement (SSAA) is updated to reflect any changes and the test results. This phase ends when the DAA issues a system accreditation and an Authority To Operate (ATO.) The ATO is issued only when the DAA is satisfied that the system is properly protected, as described in the SSAA.

Phase 4 – Post Accreditation

Phase 4 is the maintenance phase. An ATO is valid for three years unless there are significant changes that would warrant re-accreditation. VeriSign works with agencies to keep all C&A documentation current.



## DATA SHEET

### VERISIGN DIFFERENTIATORS

- Leverages best practices from across the Department of Defense
- Value-oriented, professional project management
- Efficient, repeatable processes
- Staff expertise in C&A
- Cleared personnel
- Operator of Critical Infrastructure, as designated by U.S. Department of Homeland Security

#### + Summary

Completing a security accreditation helps ensure that an information system will be operated with appropriate management review, that there is ongoing monitoring of security controls, and that re-accreditation occurs periodically in accordance with federal or agency policy or if a significant change to the system or its operational environment occurs.

#### + What You Get

VeriSign produces the following documents during the C&A process:

- Information System Security Policy (ISSP)
- Security Requirements Document/Traceability Matrix
- Certification Test and Evaluation (CT&E) Plan
- Security Test and Evaluation (ST&E) Plan
- Residual Risk Assessment Results
- Security Education, Training, and Awareness Plan
- Incident Response Plan
- Contingency Plan

#### Certification and Accreditation Statements

VeriSign prepares a Security Accreditation Statement, which documents the results of the security certification and provides the DAA with the essential information needed to make a credible, risk-based decision on whether to authorize operation of the information system.

#### + Learn More

For more information about VeriSign® Security Services, please call 650-426-5310, email [enterprise\\_security@verisign.com](mailto:enterprise_security@verisign.com), or visit us at [www.Verisign.com](http://www.Verisign.com).

#### + About VeriSign

VeriSign, Inc. (Nasdaq: VRSN) operates intelligent infrastructure services that enable and protect billions of interactions everyday across the world's voice and data networks. Additional news and information about the company is available at [www.verisign.com](http://www.verisign.com).

Visit us at [www.Verisign.com](http://www.Verisign.com) for more information.

©2006 VeriSign, Inc. All rights reserved. VeriSign, the VeriSign logo, "Where it all comes together," and other trademarks, service marks, and designs are registered or unregistered trademarks of VeriSign and its subsidiaries in the United States and in foreign countries. Microsoft is a trademark of Microsoft Corporation.

00020814 03-31-06