



DATA SHEET

KEY FEATURES

VeriSign solutions for FISMA, OMB, and FIPS 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 memoranda and circulars
- The Privacy Act of 1974
- The National Institute of Standards and Technology (NIST) Special Publications 800 Series, including SP 800-53a, *Guide for Assessing the Security Controls in Federal Information Systems*
- The Federal Information Security Management Act (FISMA) of 2002
- Federal Information Processing Standards (FIPS) Publications (199 and 200)
- 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 17799/27001 as well as agencies' specific policies, standards, and procedures

VeriSign Information Assurance Federal Information System Certification and Accreditation

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 system security.

+ Federal Information System Certification and Accreditation (C&A) Support

VeriSign assists customers in meeting their regulatory and compliance requirements by conducting Certification and Accreditation (C&A) of general support systems and major applications. VeriSign provides an independent assessment of the System Security Plan (SSP) and its implementation to help ensure that security controls for the information system are adequate to meet all applicable security requirements.

+ VeriSign Certification and Accreditation (C&A) Methodology

The VeriSign C&A methodology is based on National Institute of Standards and Technology (NIST) Special Publication 800-37, *Guide for the Security Certification and Accreditation of Federal Information Systems*, and is easily adapted to meet agencies' own internal C&A process. The VeriSign methodology incorporates activities, general tasks, and a defined management structure to help agencies obtain and maintain enterprise-based C&A for their information system infrastructure and applications.

The methodology is sufficiently flexible to evaluate systems in various lifecycle stages, systems under evolutionary development, and single-purpose or legacy systems, for as long as they exist. Standardized assessment methods and procedures promote more consistent, comparable, and repeatable security assessments of federal information systems.



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.

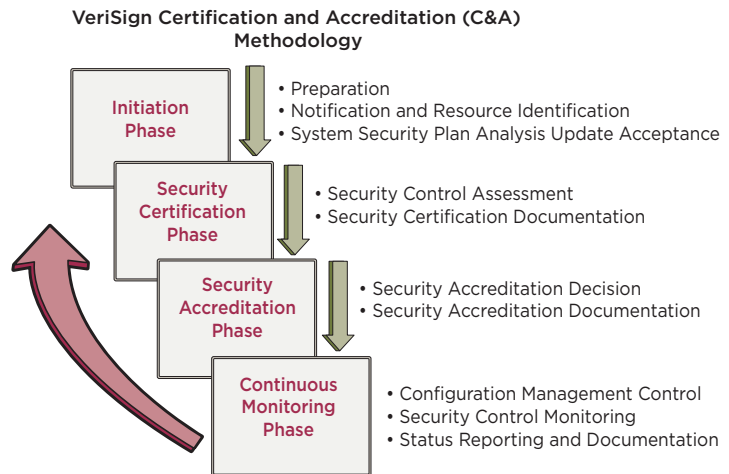
Informed Decision-Making

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

The assessment methods and procedures that VeriSign employs during the assessment of an information system include:

- Interviewing agency personnel associated with the security aspects of the system
- Reviewing and examining security-related policies, procedures, and documentation¹, including Federal Information Processing Standards (FIPS) 199² security categorization, e-authentication risk assessments³, and privacy impact assessments⁴
- 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

The following figure provides an overview of the VeriSign C&A methodology, including the tasks associated with each phase in the process. These phases map directly to NIST Special Publication 800-37, *Guide for the Security Certification and Accreditation of Federal Information Systems*.



VeriSign tailors these phases to apply a level of effort and rigor that is suitable for each information system undergoing C&A, based on agency priorities and the FIPS 199 impact categorization. For compliance, VeriSign ensures that the baseline security controls required by the Federal Information Security Management Act of 2002 (FISMA) and FIPS 200⁵ are addressed in the SSP and the Certification documents. Beyond the baseline and enhanced controls, VeriSign uses its expertise to create assessment methods and procedures for security controls employed by the agency that are not contained in NIST Special Publication (SP) 800-53, Recommended Security Controls for Federal Information Systems. Assessment methods and procedures may need to be tailored, in some instances, for specific information system implementations. VeriSign may also document and reconcile agency-specific controls against SP 800-53 guidance.

1 If any required security documents are found to be deficient or are not available, VeriSign can assist customers to update or create these documents as part of a pre-C&A consulting engagement.
 2 FIPS Publication 199, Standards for Security Categorization of Federal Information and Information Systems.
 3 The President's Office of Management and Budget (OMB) in its Memorandum M-04-04 requires an e-authentication risk assessment for every authenticated e-government transaction.
 4 The E-Government Act of 2002, section 208 requires agencies to conduct privacy impact assessments for electronic information systems and collections.
 5 FIPS Publication 200, Minimum Security Requirements for Federal Information and Information Systems.

VERISIGN DIFFERENTIATORS

- Leverages best practices from across the U.S. Federal Government and private sector
- Value-oriented, professional project management
- Efficient, repeatable processes
- Consultants experienced in C&A
- Consultants with active federal security clearances

The Initiation Phase

This phase helps ensure that the authorizing official and senior agency security officials are in agreement with the contents of the SSP, before VeriSign begins the assessment of the security controls in the information system. There are three tasks in this phase:

- Preparation
- Notification and resource identification
- System security plan analysis, update, and acceptance

The Security Certification Phase

This phase helps determine the extent to which the security controls in the agency's information systems are implemented correctly, operating as intended, and producing the desired outcome. This phase addresses specific actions taken or those planned to correct deficiencies in the agency's security controls. VeriSign provides the agency's authorizing official with the information needed to determine the risk to agency operations, agency assets, or individuals so the authorizing official will be able to render an appropriate security accreditation decision for the information systems.

There are two tasks in this phase:

- Security control assessment (risk assessment, and security test and evaluation)
- Security certification documentation

The Security Accreditation Phase

This phase helps determine whether the remaining known vulnerabilities in the agency's information system (after the verification of an agreed-upon set of security controls) pose a level of risk that is acceptable to the agency's operations, assets, and individuals. Upon completion, the agency's authorizing official may make one of the following three decisions:

- Authorization to operate the information system
- Interim authorization to operate the information system under specific terms and conditions
- Denial of authorization to operate the information system

There are two tasks in this phase:

- Security accreditation decision
- Security accreditation documentation

The Continuous Monitoring Phase

The purpose of this phase is to provide oversight and monitoring of the security controls in the agency's information systems on an ongoing basis and to inform the agency's authorizing official when changes occur that may impact system security. VeriSign works with agency officials to perform the activities in this phase continuously throughout the life cycle of the agency's information systems.

There are three tasks in this phase:

- Configuration management and control
- Security control monitoring
- Status reporting and documentation



Documentation

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

- Certification and Accreditation Plan
- System Security Plan
- Risk Assessment
- Security Test and Evaluation Plan and Report
- IT Contingency Plan
- Configuration Management Plan
- Certification Letter and Accreditation Letter

+ Learn More

For more information about VeriSign® Security Services, please call 650-426-5310, email enterprise_security@verisign.com, or visit us at 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.

Visit us at 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. All other trademarks are the properties of their respective owners.