

## Certification and Accreditation Solutions

### Information Security Becomes Law

As concern has grown about the integrity of the information systems utilized by public and private enterprise, federal policymakers have taken notice by passing several laws and regulations. On the Federal level, security Certification and Accreditation (C&A) is mandated by the Federal Information Security Management Act (FISMA) of 2002 for all Federal Information Systems, and DoD Directive 8500.1, "Information Assurance," for all DoD information systems. The directives establish policy to achieve information assurance (IA) through a defense-in-depth approach that integrates the capabilities of personnel, operations, and technology, and supports the evolution towards network-centric warfare.

The challenges of effective C&A within an agency or large enterprise are staggering, however. Even within a single agency or enterprise, C&A implementation will vary from site to site. At SAVVIS, we understand the challenges and organizational complexities that these new regulations bring, and to help address these challenges, SAVVIS has developed a unique approach that combines people, process, and technologies for agency-wide C&A implementation.

#### CERTIFICATION

- Standard, proven methodology
- All applicable tests systematically performed against each system & its components
- Tested in intended operating environment

#### ACCREDITATION

- Management decision by senior official in the organization
- Authorizes operation of IT systems based on results of the certification and relevant factors

#### SOLUTION HIGHLIGHTS

- Leveraging best practices from across the US Federal government & private sector
- Efficient, Repeatable Processes
- C&A Experienced Staff
- Public Trust Cleared Personnel

### Let SAVVIS Meet the Challenge

SAVVIS Security Services provides expert C&A solutions, delivered by experienced specialists in Federal IT systems security. We pride ourselves in providing a structured approach to C&A, providing consistent methodology and a complete understanding of the agency's business requirements.

SAVVIS Security experts understand that C&A processes are more than a mere exercise in generating paperwork, and must ensure that the dollars spent actually result in improved security by providing an effective avenue for managing agency-wide risks.

The SAVVIS Federal Security Team (SFST) enhances the quality of an agency's C&A program by ensuring that the processes used result in security programs that translate into an ongoing and comprehensive risk management practice across the entire agency.



## Managing Agency Risk with Proven Methodologies

The foundation of any C&A methodology is the assessment process, and SAVVIS has developed standardized assessment methods and procedures to promote more consistent, comparable, and repeatable security assessments of information systems. Moreover, SAVVIS' C&A assessment methodology is sufficiently flexible to evaluate systems in various life-cycle stages, systems under evolutionary development, and those single-purpose or legacy systems for as long as they exist.

The SAVVIS C&A methodology is based on an operational assessment process that incorporates the documentation required by FISMA and DoD Directive 8500.1. Our methodology is easily adapted to meet your own agency's internal Security Program Requirements, resulting in the creation of Certification documentation that will result in successful Accreditation decisions. SAVVIS offers C&A solutions that support both DoD- and non-DoD-based systems.

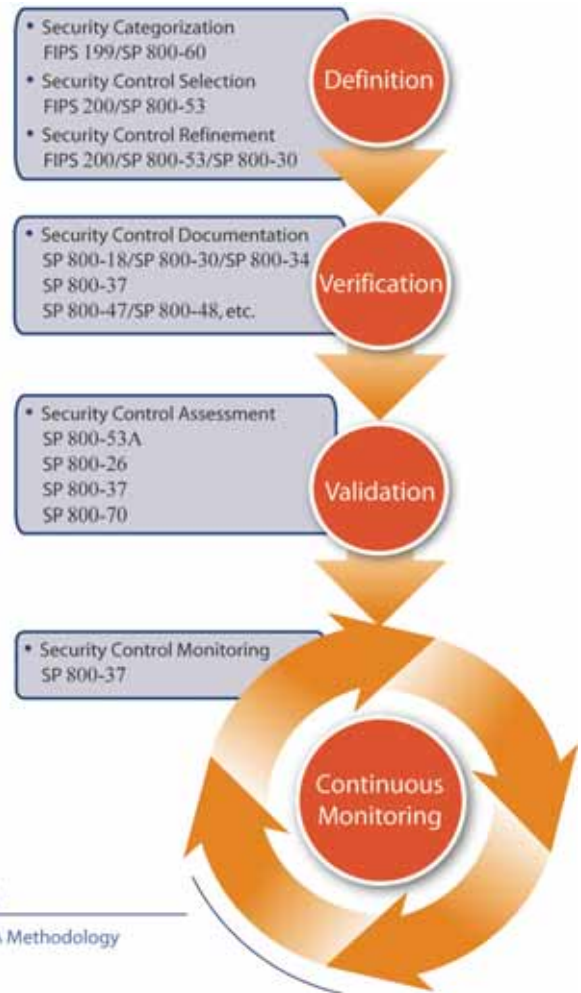
The SAVVIS methodology incorporates activities, general tasks, and a defined management structure to help agencies obtain and maintain enterprise-based C&A for their information system infrastructure and applications.

The assessment methods and procedures that SAVVIS employs during the C&A assessment include:

- Interviewing agency personnel associates 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 security-relevant and security-critical aspects of system hardware, software, firmware, and operations

SAVVIS C&A methodology includes four phases: Definition, Verification, Validation, and Continuous Monitoring.

Figure 1 illustrates an overview of SAVVIS Certification and Accreditation methodology, including the tasks associated with each phase in the process, as well as all corresponding Federal guidelines.



**Figure 1**  
SAVVIS C&A Methodology

**PHASE 1**  
**Definition**

During the Definition phase, SAVVIS will assist agency officials in the categorization of information systems according to potential impact of loss. SAVVIS will then identify the security system requirements, planned or in place, based on classification, data types, users, and threats. SAVVIS will conduct a risk assessment to adjust the minimum control set based on local conditions, required threat coverage, and specific agency requirements.



**PHASE 2  
Verification**

During the Verification phase, SAVVIS will conduct verification of security control documentation

including Security Plans, Contingency Plans, Risk Assessments and other policies, procedures and records to determine whether the documentation complies with the requirements agreed upon in Phase 1: Definition.

**PHASE 3  
Validation**

During the Validation phase, SAVVIS 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. The agency's authorizing official can then render an appropriate security accreditation decision for the information systems.

**PHASE 4  
Continuous Monitoring**

During the Continuous Monitoring phase, SAVVIS provides oversight and monitoring of the security

controls in the agency's information systems on an ongoing basis. In this phase, the agency's authorizing official is informed when changes occur that may impact system security. SAVVIS' Federal Security Team (SFST) will work with agency officials to perform the activities in this phase continuously, throughout the life cycle of the agency's information system.

**C&A Package  
Preparation**

At strategic points during each phase, SAVVIS can provide agency officials with comprehensive

documentation to support planning and decision making, accompanied by high-level summaries, and backed by the professional expertise of the SAVVIS Federal Security Team. Document preparation can include core documents as well as security controls, planned or in place, for the information system.

As part of C&A Package Preparation, SAVVIS can assist with Security Control Implementation within new or legacy information systems consistent with NIST SP 800-70.

**Figure2.** Sample of reports provided by SAVVIS.



**Security Control Implementation**

**Purpose**

The purpose of this document is to report recommendations to *Federal Client Agency* regarding security controls identified in the Security Plan. This report has been produced in support of Federal Client Agency Security Accreditation and Certification.

**Scope**

The comprehensive scope of this Security Control Implementation report addresses the disposition

**Industry-Leading Security Experience:  
Partner with the Best**

SAVVIS has spent many years building our security credentials, and working with many government agencies in the process. Today, we can offer comprehensive experience in identifying threats, risks and vulnerabilities, and building the counter-measure solutions that agencies should demand when it comes to ensuring the security of their IT systems.

Our security experts have been at the forefront of designing and securing the most complex networks in the world, and have secured sites for many of the Fortune 1000 and the United States government. Our team of security experts is comprised of senior security professionals who have honed their skills through corporate security leadership, security consulting, investigative branches of the government, law enforcement, and research and development.

Many of SAVVIS' security personnel hold advanced technical degrees, as well as a wide array of industry-recognized security certifications including CISSP, CISA, and numerous SANS/GIAC certifications.



SAVVIS also operates one of ten United States Government NVLAP-accredited, CCEVS-approved, Common Criteria Test Laboratories known as the Common Criteria Testing Lab (CCTL). We have experience evaluating an array of security products from devices, appliances, and general-purpose products to distributed applications. Our lab is located in a SAVVIS Internet Data Center with world-class features including 24/7 secured biometric access, video camera surveillance, raised floors, HVAC temperature control, advanced smoke detection, and advanced fire suppression systems.

### **Related Services**

The SAVVIS Federal Security Team (SFST) enhances the quality of an agency's Certification and Accreditation program by ensuring that the processes used result in a comprehensive risk management approach that translates into a solid security program across the entire agency. In an effort to support this, SAVVIS Security Services offers a wide array of professional and managed security services aimed at reducing the complexity, improving your agency's overall security posture, and ensuring compliance with myriad federal regulations.

### **Architecture & Design Services**

The network architecture design service helps you plan a secure, customized network that meets organizational goals, both now and into the future. Our security experts develop a sound network architecture that enhances your business operations while improving your security posture through the effective integration of protection solutions from SAVVIS.

### **Application Security Review**

This service allows you to balance time-to-market demands with security best practices. It includes technical and non-technical security reviews of custom applications to determine your security weaknesses, as well as recommend improvements.

### **Compliance Assurance Manager**

A Compliance Assurance Manager is an experienced security consultant and compliance expert who will act as your trusted advisor and single point of contact for all compliance-related issues. The Compliance Assurance Manager is responsible for first, ensuring that your IT infrastructure adheres to internal or industry security

policies and procedures, and recommends appropriate controls; second, manages changing security requirements as infrastructure evolves; third, responding to incidents in accordance with approved plans.

### **Penetration Testing**

SAVVIS will conduct a simulation of a real-life network attack to determine your current vulnerability, and analyze how an attack could significantly impact your business. The result is a detailed report that prioritizes areas of weakness within your networking environment.

### **Remediation Services**

SAVVIS security experts will review control gaps identified by an independent audit source and provide a Remediation Roadmap that will prioritize all necessary actions, and incorporate remediation activities into a comprehensive project plan.

### **Risk Assessment Services**

Security assessment provides the foundation for any security program. This comprehensive evaluation of your information security posture is based on the Federal Information Processing Standards (FIPS). Our experts analyze your administrative, technical, and physical security controls, and then document the results to create a cost-effective roadmap for mitigating identified risks and improving your overall security posture.

### **Security Policy Development**

Policy development provides you with security policies and procedures designed to meet organizational business objectives, regulatory issues, and industry best practices. Our security experts work closely with you to determine your unique business needs, and design a policy framework that enhances your security posture, regulatory compliance, and ongoing business practices.

#### **RELATED SERVICES**

- Architecture & Design Services
- Application Security Review
- Compliance Assurance Manager
- Penetration Testing
- Remediation Services
- Risk Assessment Services
- Security Policy Development



## About SAVVIS Federal Systems (SFS)

## SAVVIS Security Utility

In addition to Security Consulting Services, SAVVIS offers a wide range of Security Utility Services that are meant to provide ongoing protection to our customers' infrastructure. The SAVVIS Security Utility is a flexible and scalable managed security offering that does not require hardware or software to be installed or managed at the customer's premise.

The SAVVIS Security Utility leverages both "In the Cloud" security components such as in-network firewalls, Distributed Denial of Service (DDoS), and worm attack mitigation for a wide area network, as well as virtualized security components such as hosted firewalls and intrusion detection systems. All services are managed by SAVVIS, and can be monitored by customers via SAVVIS' web portal. The SAVVIS web portal allows users to monitor activity in their environment, directly and conveniently. The result is a set of advanced managed security utility services that are ubiquitous to all IT operations and provide for compliance, yet are transparent to IT resources.

## Get Ahead

Although many vendors offer professional services to Federal agencies and their contractors seeking general security, compliance and auditing solutions, few providers can offer exceptional regulatory knowledge, many years of experience, best-of-breed solutions, and a world-class global hosting and network infrastructure that routinely meets or exceeds the internal security requirements of our extensive customer base.

SAVVIS can provide the solutions that enable your agency to build defensible, standards-based IT security policies and procedures for continuous, measurable improvements in audit success and regulatory compliance, while lowering the overall cost to you. Let SAVVIS meet the challenge by leveraging SAVVIS' team of highly-skilled security professionals, who have been in the forefront of designing and securing some of the most complex networks in the world.

The parent company, SAVVIS, Inc. (NASDAQ: SVVS) is a global IT Utility provider that leads the industry in delivering secure, reliable and scalable hosting, network, and application services. SAVVIS' strategic approach combines the use of virtualization technology, a utility services model, and an increased usage of automation software management and provisioning systems for enhanced customer performance.

As one of the world's largest providers of IP computing and communications services, one of the world's largest providers of comprehensive hosting services, and one of the world's largest providers of digital content services, SAVVIS allows customers to focus on their missions rather than on its IT infrastructure.

SFS offers the entire SAVVIS solution set to Federal agencies and their contractors via the GSA Schedule 70. We are pleased to be a subcontractor to small and large businesses, with proven performance credentials for providing best-value solutions to Federal clients. Our solutions approach is to collaborate openly and honestly with our clients and partners to design and implement end-to-end IT infrastructure solutions to support mission critical applications.

For more information about the broad range of services that SAVVIS Federal Systems offers to its customers, please visit us at [www.savvis.net/federal](http://www.savvis.net/federal)

### BE SECURE WITH SAVVIS

- Exceptional Regulatory Knowledge
- Years of Experience
- Best-of-Breed Solutions
- World-class Global Hosting & Network Infrastructure
- Routinely Meets or Exceeds Internal Security Requirements of Extensive Customer Base