

## FISMA Solution

### Overview of FISMA

Government agencies face an ever-present risk of threats designed to access and misuse federal information systems. The Federal Information Security Management Act, more commonly known as FISMA, was designed to strengthen the government's information assurance infrastructure to improve IT performance, ensure operational continuity and support homeland security. Established in 2002 by Congress and passed into law in January 2003, FISMA requires each federal agency to develop, implement and continually report on a program to provide security for the information and systems that support agency operations.

To guide FISMA compliance, NIST publishes two types of security documents: (i) Federal Information Processing Standards (FIPS); and (ii) Special Publications (800-series guidance). FISMA requires federal agencies to comply with FIPS which is mandatory and non-waivable and the Office of Management and Budget (OMB) requires federal agencies to comply with NIST publications. Additional security standards, guidelines and best practices are being produced in support of FISMA on a continual basis.

Unlike many regulatory efforts in the past, FISMA holds Government Agency Executives accountable for their agencies' performance against the FISMA standards. Congress has the ability to publicly publish a "scorecard" grading an agency's compliance with FISMA. A low score card can severely impact an agency's reputation and threaten the jobs of those who are responsible for maintaining the information assurance architecture, in accordance with regulatory compliance within that agency. In addition, agencies' CIOs, CTOs and/or CFOs may have to testify before Congress explaining why they have scored poorly; and most importantly, the OMB can delay or deny funding for additional agency programs.

### The IT Security Solution Not Just FISMA

Complying with FISMA regulations and adapting rapidly to new regulations mandated by Information Assurance and Homeland Security presents a growing challenge for government agencies of all sizes. These are resource-intensive activities, and without an effective deployment, audit and reporting solution, IT managers will either have to obtain additional staff without obvious benefit, or see productivity reduced as current staff work to maintain systems effectively.

#### SOLUTION HIGHLIGHTS

- Assists agencies with achieving and maintaining FISMA regulatory compliance
  - Assures measurable and continuous security improvement across the federal enterprise
  - Demonstrates and documents multiple, diverse security policies and controls
  - Integrate IT security with business processes that leverage IT resources and investment
  - Achieve an economically sustainable security posture while effectively managing risk
- 
- Public security is on the line, every agency must do all it can to comply with e-government security mandates
  - Point technology solutions can only scratch the surface of a workable solution – most still require tedious, manual tasks that divert time and talent from accomplishing your mission
  - The only cost-effective way to satisfy FISMA is by using a rigorous, comprehensive and process-driven approach backed by built-in security controls



- SAVVIS addresses these challenges by enabling government agencies to provide regulatory bodies with comprehensive security policy assessments and implementations through its compliance consulting solution suite.

### **The SAVVIS Advantage**

SAVVIS offers a FISMA solution based on an integrated, end-to-end process that encompasses all aspects of risk analysis, security planning, management and reporting across an entire agency. Instead of simply providing technology tools to help agencies meet their compliance obligations, SAVVIS' FISMA solution involves a proven, proactive process-driven approach that closely examines all facets of agencies' existing assets and programs to significantly improve their overall state of security and help them meet their regulatory mandates.

SAVVIS' industry leading consulting solutions and assessment programs can discover, track and enforce security policies and pinpoint configuration and security holes before they are breached. Best of all, SAVVIS' process-driven approach is designed to address interdependencies-within and across agencies – for the significant IT security advancements NIST and NSA prescribe to ensure critical federal assets are secure.

### **Industry-Leading Security Experience**

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 U.S. Government. Our elite 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, SANS, GSEC, and GIAC.

SAVVIS also operates one of ten U.S. Government NVLAP accredited, CCEVS approved, Common Criteria Test Laboratory known as the Arca 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 facility

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 fire suppression systems.

### **SAVVIS at Work for Government Agencies**

Given that FISMA does not currently provide specific guidance, agencies must translate regulations into frameworks and standards that can be mapped to specific IT control policies across the entire agency. Once established, these controls must then be sustained on a continual basis to help assure compliance and remediate deficiencies.

### **The SAVVIS Methodology**

#### **A Proven Process Makes the Difference**

Many federal organizations have had to create separate labor-intensive manual processes to assess, document, and improve their compliance with a multitude of regulations including FISMA, Certification & Accreditation (DITSCAP, NIACAP), OMB Circular A-123, FPC 65, HIPAA and other internal and external requirements. This brute force approach may provide short term progress toward compliance, but the associated excessive and increasing costs required to manage compliance in this manner are unsustainable.

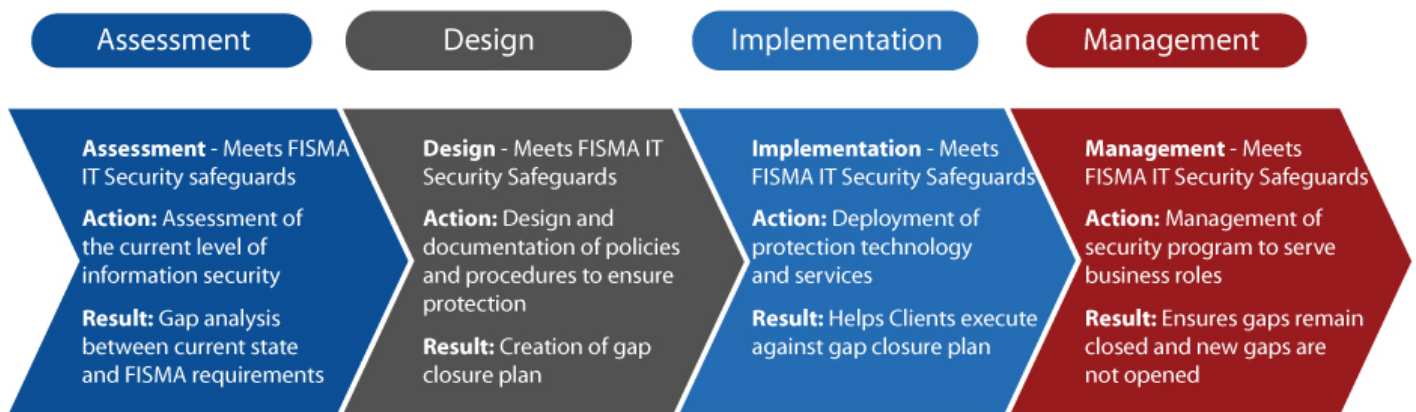
These manual methods and separate processes are not only costly and time-consuming, they cannot be easily audited for accuracy, and rarely provide the timely detail required for effective remediation. The result is often inconsistent measurement and reporting throughout the agency while not producing the improved security vital to protecting the nation's critical assets.



## SAVVIS Transformation Methodology<sup>SM</sup> (STM)

The SAVVIS Transformation Methodology is a broad propriety framework that incorporates a unique combination of research, people, processes and technologies. This methodology was developed to streamline security best practices and help agencies achieve their FISMA compliance. The STM framework incorporates a four-step process covering the complete compliance management lifecycle, including phases for Assessment, Design, Implementation and Management (ADIM).

The ADIM process identifies and analyzes gaps between current state and FISMA requirements, and then designs and implements solutions to close those gaps on a going forward basis as illustrated below:



### Assessment Phase

Knowing where you stand is the first critical step in any compliance program; our world-class security experts will work with your team utilizing a pragmatic approach to assess plans, procedures and infrastructure against regulations to determine risks and gaps. SAVVIS will also categorize systems, risks and gaps in accordance with the NIST 800 Series and perform a feasibility analysis of cost vs. criticality to prioritize action steps. SAVVIS will provide recommendations to minimize exposure to adverse regulatory and accreditation actions as well as security threats specific to your agency.

### Design Phase

SAVVIS Security experts will collaborate with you to design and plan an appropriate and cost-effective solution that fits your business needs and serves your goal to comply with FISMA requirements. This second phase culminates in a detailed roadmap for implementation of a robust Agency security and compliance program.

### Implementation Phase

This phase involves a collaborative effort with you to implement appropriate SAVVIS security products and services to assist your efforts to comply with FISMA requirements. SAVVIS's *Protection Technology* suite includes SAVVIS's Intelligent Hosting Solutions, Managed Security Services and Professional Security Services (see *related services section*). Our solutions are part of a component suite adapted from the Information Technology Infrastructure Library (ITIL) methodology that seeks to effectively and efficiently deliver all security solutions and products.

Additionally, our security experts will work with you to create a NIST 800 Series based Plan of Action and Milestones (POA&M) to track gap remediation and drive continuous improvement by remediating unsatisfactory conditions on an automated, closed loop basis.



## Audit Readiness is the Key to a Successful Compliance Program

Through both our own qualified staff and our partner provided audit program, SAVVIS is able to offer our government agencies a NIST 800 Series based auditing service that is independent of the remediation services performed by SAVVIS security personnel. Coordinated frameworks for audit and remediation are developed for FISMA requirements thus assisting your agency in achieving and maintaining its compliance using resources, staff and funding, more efficiently, compared to other methods available today in the market.

Our audit program is based on methodologies conforming to the NIST security standards and supports Homeland Security initiatives designed to protect critical infrastructure, including vital government services. Moreover, our audit services address additional regulations mandating rigorous IT controls, such as the Health Insurance Portability and Accountability Act (HIPAA), the Gramm-Leach-Bliley Act (GLBA) and the Sarbanes-Oxley Act; as well as preparation for potential state-level legislative trends, evidenced by California State Bill 1386, that require protection of personal information communicated through the public Internet.

### Related Services

We pride ourselves on providing a comprehensive compliance consulting solution that covers every aspect of the compliance management lifecycle from assessment and design to implementation and management. SAVVIS Security Services is committed to helping federal agencies secure their information and continuously develop information security solutions that will keep pace with the aggressive deployment of information technologies. The following SAVVIS Security Services can help reduce the complexity and help the Agency improve its compliance with FISMA:

### Architecture and Design Services

The network architecture design service helps you plan a secure, customized network that meets organizational goals 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.

### Management Phase

Management is critical to the success of any security or compliance program. Not unlike any business process, security processes and procedures require effective management to ensure that all aspects of security are running according to plan. Management works in variety of ways, either as direct line management, project management or executive oversight. As such it is critical that effective monitoring, reporting, and management decisions are being made on a timely basis. To support this effort, SAVVIS offers a variety of solutions to aid government agencies; including Security/Compliance Assurance Managers (SAM), staff augmentation; reporting, audit trails and managed security services (see *Related Services section*).

### Simplify FISMA Readiness

By incorporating the ADIM methodology into the development of our market leading suite of compliance consulting and security solutions, SAVVIS can essentially aggregate all of your existing policies into one security architecture that eliminates redundancies, inefficiencies, and complexities. SAVVIS accelerates completion times, lowers costs, documents progress and elevates your security posture:

- Document, categorize and classify IT assets for Confidentiality, Integrity and Availability
- Develop or verify security plans, policies and procedures
- Complete quarterly Self-Assessment Questionnaires
- Create POA&M's and submit Score Card Summary data
- Perform feasibility analysis; cost vs. criticality; prioritize actions
- Apply industry controls to enforce adherence
- Certify assets per risk categories and submit for accreditations
- Certify backend access controls and user access authority
- Audit security controls and remediate gaps and confirm proper completion

A photograph of the U.S. Capitol building in Washington, D.C., showing its iconic dome and neoclassical architecture under a clear blue sky.

### Security Policy Development

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

### SAVVIS Security Utility

In addition to the Security Consulting Services outlined above, SAVVIS offers Customers a vast array of Security Utility Services that are meant to providing ongoing protection to the Customer's infrastructure. Essentially, 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, which 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 infrastructure security, yet are transparent to IT resources.

### Application Security Review

This service allows you to balance time-to-market demands with security best practices. It includes technical and non-technical security review 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 advisor and single point of contact for all compliance related issues. The Compliance Assurance Manager is responsible for: 1) reviewing whether your IT infrastructure adheres to internal or industry security policies and procedures and recommending appropriate controls; 2) managing changing security requirements as infrastructure evolves and; 3) responding to incidents in accordance with approved plans.

### Penetration Testing

SAVVIS will conduct a real-life demonstration of a network attack to determine your current vulnerability and analyze how an attack can significantly impact your business. The result is a detailed roadmap 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 document the results to create a cost-effective roadmap for mitigating identified risks and improving your overall security posture.



### **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, industry leading 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 infrastructure security while lowering the overall cost to you.

Let SAVVIS meet the challenge by leveraging SAVVIS's 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.

### **Important Notice**

SAVVIS does not in any way guarantee and makes no representation or warranty that any of its services comply with any applicable data security law or satisfy any particular requirement of FISMA or NIST 800-53. SAVVIS does not purport to provide any customer or potential customer with legal or regulatory or compliance advice and nothing herein shall be interpreted as such advice. SAVVIS does not assume any liability for any good faith classification of any potential risk or control. The customer and potential customer is advised that there are inherent limitations in any such classifications as well as any assessments and audits and SAVVIS does not guarantee that any such classification, assessment or audit is adequate or appropriate. Full responsibility for all regulatory compliance, including without limitation that relating to FISMA and NIST 900-53 remains the sole and exclusive responsibility of the customer or potential customer and not SAVVIS.

### **About SAVVIS Federal Systems (SFS)**

The affiliated company, SAVVIS Communications Corporation (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 focus on their 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 customer base, please visit us at: [www.savvis.net/federal](http://www.savvis.net/federal).