

The SAVVIS Approach to Security Risk Management

This document reviews the emerging changes in the IT risk landscape, the increasingly important role IT plays in Federal risk management, and how SAVVIS' infrastructure and security services can help address those risks cost effectively.

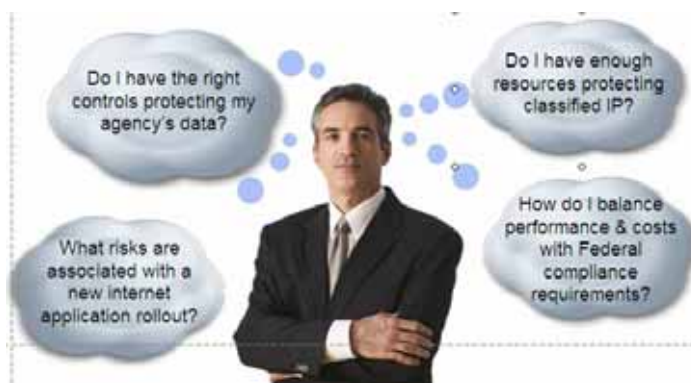
Table of Contents

- 3 What Is At Risk?
for enterprises and Federal agencies
- 5 What Choices Do We Have to Address Risks?
- 5 Costs Associated With Implementing
Risk Management Controls
- 8 About SAVVIS Federal Systems

What Is At Risk?

Much of what is driving organizational risk is the increasing value of information, and the increasing number of methods available to access it. The internet, VPNs, mobile & home-based work forces and extranets have all contributed to the ever-growing number of access vectors to enterprises' data. Malicious access may be for the purpose of using the data illegally, destroying it, altering it and thus compromising its integrity, and denying its availability to legitimate users.

Many senior IT executives struggle with managing a multitude of risks.



The value of data, as a share of a typical organization's overall asset portfolio, has grown exponentially in just the last ten years. The risks related to data compromise are significant. Examples of risk to a company include:

- Loss of funding
- Lost reputation, damaged image
- Legal (compliance, contractual)
- Loss of assets (customer data, intellectual property, classified data)
- Liability of the Board of Directors and senior management
- Random expenses associated with risk

Organizations are under increasing pressure to establish best practices to protect data, and can be held liable for failing to establish guidelines for adhering to regulatory requirements.

Who should care about risks and the development of a risk management program?

A risk management program is recommended by NIDS (sp800-30) for all Federal IT organizations. The ways in which a risk management program benefits an organization, which include improved security and operation efficiency, are well documented. Stakeholders of an IT risk management program include technical and non-technical individuals, data owners, data custodians, and senior management. Examples of job functions and their involvement can include:

Senior management: sponsors of the risk management program and approve the IT security budget.

- Federal Chief Information Officers, responsible for implementation of risk management for agency IT systems and the security provided for these IT systems
- Designated Approving Authority (DAA), responsible for the final decision on whether to allow operation of an IT system
- IT security program manager, implements the security program
- Information system security officers (ISSO), responsible for IT security

- IT system owners: managed system software and/or hardware used to support IT functions.
- Data owners of information that is stored, processed, and transmitted by the IT systems
- Data custodians: responsible for the availability of systems on which information resides, and the handling of that information
- Technical support personnel
- IT system and application programmers: develop and maintain code that could affect system and data integrity
- IT quality assurance personnel: test and ensure the integrity of the IT systems and data
- Information system auditors: audit IT systems
- IT consultants: support clients in risk management.

What are the components of risk?

Risk is the probability of a negative impact of an exploited vulnerability. Vulnerability by itself does not represent a risk. A vulnerability that is exploited by a given threat constitutes a risk situation. Thus IT risk is the result of vulnerabilities and threats related to information assets. The generally accepted theoretical formula used by risk managers is: Risk = Threat x Vulnerability x Asset Value (or $R = T \times V \times AV$). Risk management is the process of identifying, assessing, and taking steps to reduce risk to an acceptable level at an acceptable cost.

Typical examples of threats include:

- Accidents
- Malicious attacks
- Theft and fraud
- System failure
- Network and power outages
- Employee or service provider errors
- Force majeure

Government and industry organizations continually collect data on IT security threats. Some of the available sources of current threat information include:

- Intelligence agencies (for example, the Federal Bureau of Investigation's National Infrastructure Protection Center)
- Federal Computer Incident Response Center (FedCIRC)
- Mass media, particularly Web-based resources such as SecurityFocus.com, SecurityWatch.com, SecurityPortal.com, and SANS.org.

Examples of vulnerabilities to an organization include:

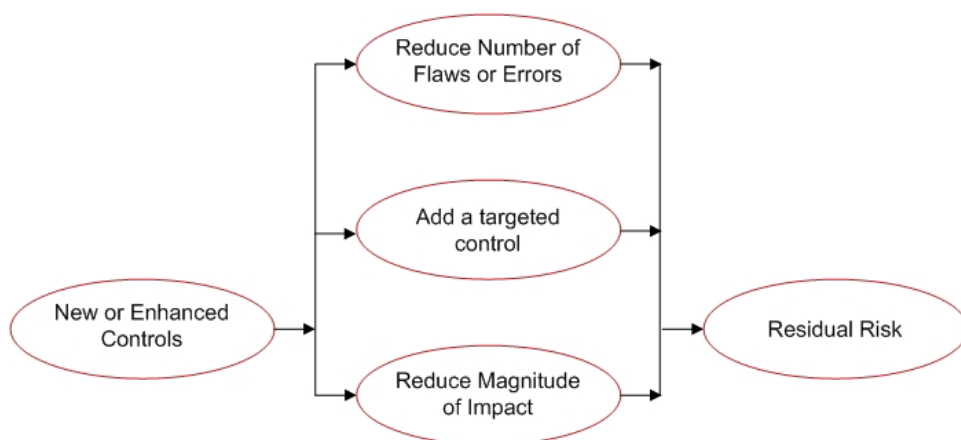
- Lack of compliance enforcement
- Lack of security policies and procedures
- Insufficient security controls
- Lack of a business continuity program
- Lack of redundancy
- Lack of maintenance and patch management process
- Poorly trained or inadequate staff
- Poorly-written software
- Configuration mistakes
- Poorly-designed architecture
- Poor password control

What Choices Do Organizations Have in addressing risks?

Organizations can never completely eliminate risk and still remain in viable. The objective is to reduce risk to an acceptable level at an acceptable cost, through the application of a risk mitigation process. There are four primary methods for mitigating risk:

- Organizations can transfer the risk, such as financial risk, to a third-party – an insurance company, for example.
- They can cease the activity that causes the risk.
- They can accept the risk.
- Or, they can treat the risk with controls. A cost-effective way of doing that is by using a third-party to manage those controls. For example, an infrastructure services company like SAVVIS can assume some of the responsibility for managing the security and operational controls of an IT infrastructure.

The relationship between control implementation and residual risk is graphically represented as follows:



Organizations must understand that there will always be residual risk, and that they cannot transfer all risk to a third-party. Managing risk is a cooperative process, and businesses will always be partly accountable for the security of their infrastructures and data, regardless of how much is outsourced.

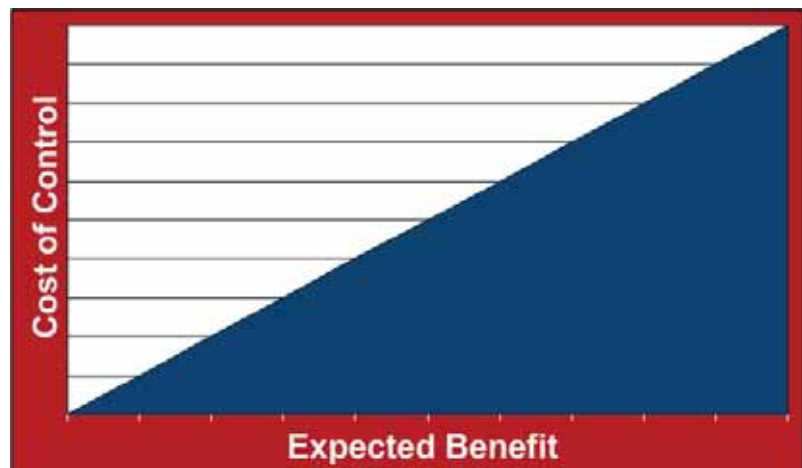
IT managers who use a risk management approach know how much of their infrastructure and controls they want managed by a third-party infrastructure services provider, such as SAVVIS, and how much they need to manage themselves.

Costs Associated With Implementing Risk Management Controls

The changing value of information and the resulting demand for controls designed to protect that information has dramatically increased the importance of the IT function within the enterprise. And this influence is not just security-related, but also cost-related.

Controls, which include policies, procedures, and technologies, along with the individuals who are trained to implement these controls, can be extremely expensive to implement.

SAVVIS commonly encounters companies that have to trim back on IT expenditures due to the costs of implementing these controls. That's unfortunate, because controls should never negatively impact the bottom line. If implemented properly, security controls should improve the bottom line by making companies more secure, more efficient, and less likely to incur a loss of high-value data assets.



But some controls can still be very capital-intensive. Creating extensive sub-nets to isolate sensitive information assets from lower-value assets, or elaborate data encryption, archiving and key management infrastructure, can involve a great deal of capital and management resources, especially if architected poorly. Organizations too often resort to throwing money and other resources at to overcome IT control and compliance deficiencies.

It's well documented that implementing too many controls will actually make an organization less secure, less efficient, and ultimately more prone to a data breach.

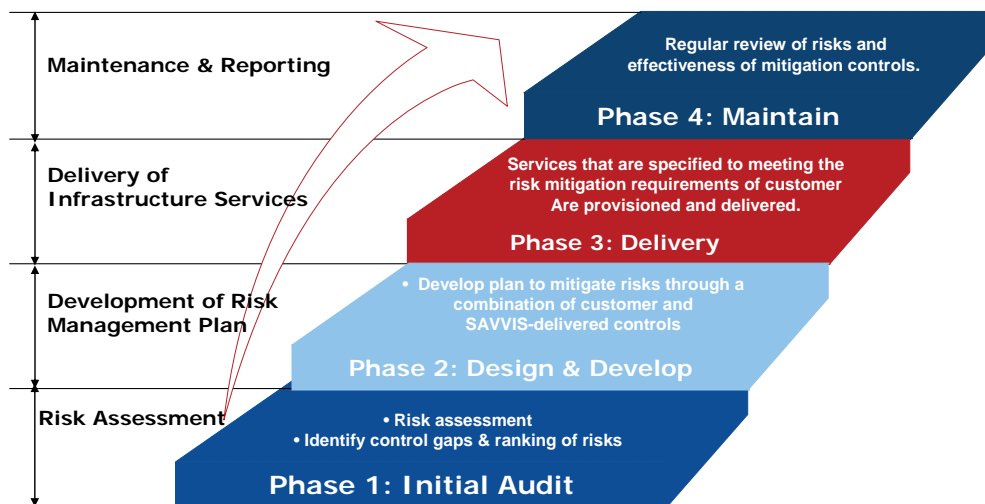
The list of recommended IT controls can be daunting for an organization to execute. There are a number of sources that can be used to detail required controls, including:

- CSA of 1987
- Federal Information Processing Standards Publications
- OMB November 2000 Circular A-130
- Privacy Act of 1974
- System security plan of the IT system assessed
- The organization's security policies, guidelines, and standards
- Industry practices.

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. Gartner recently published a study indicating that organizations who have a formal risk management program in place were able to reduce the number of compliance-related controls they had to implement by up to 70%. And again, reducing the number of controls reduces cost.

The Right Approach

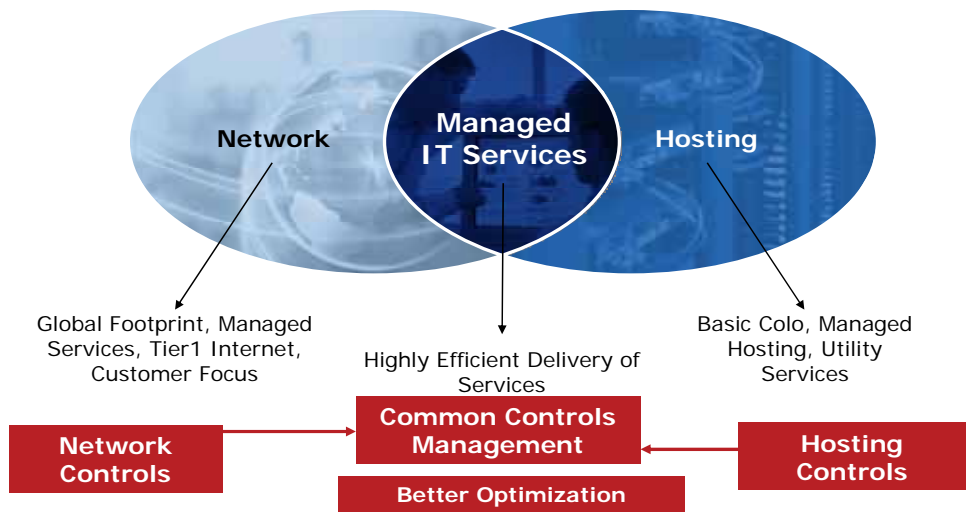
The first step is to develop a formal risk-management program that begins with a comprehensive risk assessment. It is believed that a solid risk-management program can improve a company's business efficiency, reduce its risk exposure, and thus improve its performance and bottom line. The key benefit of a risk assessment is that it can actually help enterprises *reduce* the number of controls they are required to implement. It does this by identifying those IT assets that need to have strong controls (which are often very expensive), and those assets which, based on their risk ratings, require less stringent controls.



Since controls are required by Federal guidelines and mandates, trade, and industry compliance regulations, they are a fact of life. Furthermore, these controls must often be audited by third-parties for the purpose of validating their existence and effectiveness. Again, the key is to reduce the cost of these controls.

- SAVVIS can reduce the cost of implementing and maintaining the controls that help reduce risks to an acceptable level through an effective risk management program that is tailored to your IT infrastructure.
- SAVVIS can design a security management plan that balances the necessary expenditure with the value of the information to be protected.
- We've built an efficient Infrastructure-as-a-Service portfolio that consists of data centers, managed systems, network, storage, backup and security services.
- Our professional services team's risk-management practice can assess risks, and work with clients to develop a formal risk management program.
- We use best-in-class technology as the basis of our cloud-based, and premise-based, security, network, and infrastructure services.
- To support these services, SAVVIS provides full, 24x7 management, which can free-up our customers' internal resources to devote more time to other activities.
- SAVVIS has audited its services against a framework of industry-standard controls to make it easier for our customers to work with third-party audits of the infrastructure that we host and manage.
- Building controls that are documented, and ready for an auditor's scrutiny, can be a grueling task. SAVVIS can greatly assist this process through the design of our controls-oriented managed services.

Optimized Risk Management for Networking AND Hosting Services



SAVVIS' services provide solid, global solutions for customers seeking to manage risks to an acceptable level at an acceptable cost. It's very important to choose a service provider that understands the language of risk management and IT audit controls. SAVVIS understands these requirements and designs its services with the requirements in mind.

About SAVVIS Federal Systems (SFS)

SFS is business unit of SAVVIS, Inc. (NASDAQ: SVVS) a global IT infrastructure services company that leads the industry in delivering secure, reliable and scalable hosting, network, security 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

The NIST SP 800-26, Security Self-Assessment Guide for Information Technology Systems, details specific control objectives against which a system or group of interconnected systems can be tested and measured.

These control objectives are derived from long-standing requirements found in statute, policy, and guidance on security and privacy.

SAVVIS Federal Systems

703-667-6880

www.savvis.net/federal