The Hands-Off Approach

Using Cisco's VMDC to reduce pain while achieving FISMA compliance

May 14, 2013

Synopsis

This whitepaper discusses how Cisco's Virtualized Multiservice Data Center (VMDC) validated architecture can help organizations reduce the overhead costs and implementation complications as they become compliant with the Federal Information Security Management Act (FISMA).

Table of Contents

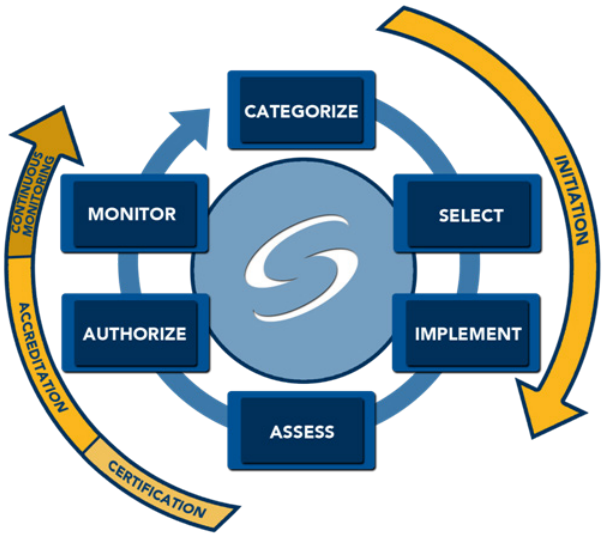
Foreword

Compliance with the Federal Information Security Management Act (FISMA) is a common problem that faces organizations within the Federal Government as well as commercial organizations that are looking to work with the US Federal Government. Described within this paper are the common struggles surrounding time, money and resources that organizations within both of these sectors face. With the architectural analysis provided by SecureState, Cisco has designed a virtual architecture, portable to any environment or system, which can ease those struggles and help organizations quickly and efficiently achieve FISMA Compliance.

Background

FISMA

Title III of the E-Government Act, also known as the Federal Information Security Management Act (FISMA), requires federal agencies to implement risk-based information security programs. This requirement extends to items provided or managed by other agencies, contractors, or other sources. To enable this, The National Institute of Standards and Technology (NIST) provides the Risk Management Framework using a series of Federal Information Processing Standards (FIPS) and Special Publications. To aid in a cost-effective, risk-based decision, information systems are categorized based on the type of information being processed. The resulting categorization is then utilized to select the appropriate security controls to be implemented. Once implemented, the controls are assessed and if appropriately applied, can then be authorized for operation within the federal sector. Continuous Monitoring activities take place to ensure security controls continue to operate and provide sufficient protection.



VMDC

The Cisco Virtual Multiservices Data Center (VMDC) is a tested and validated reference architecture for the Cisco Unified Data Center. It provides a set of guidelines and best practices for the creation and deployment of a scalable, secure, and resilient infrastructure in the data center. The Cisco VMDC architecture demonstrates how to bring together the latest Cisco routing and switching technologies, network services, data center and cloud security, automation, and integrated solutions with those of Cisco's ecosystem of partners to develop a trusted approach to data center transformation.

The Cisco (VMDC) architecture is based on foundation design principles that incorporate modularity, high availability, differentiated service support, secure multi-tenancy, and automated service orchestration. Specific benefits of VMDC include:

• Demonstrated solutions to critical technology-related problems in evolving IT infrastructure: Provides support for cloud computing, applications, desktop virtualization, consolidation and virtualization, and business continuance

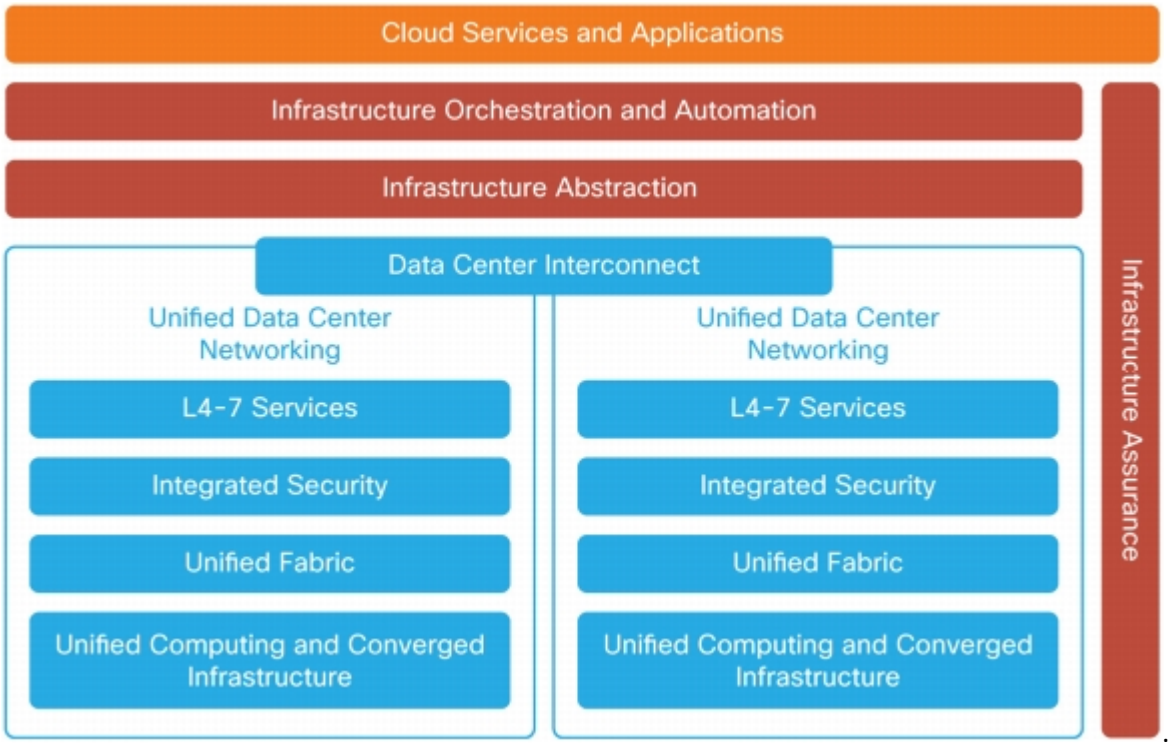
• Reduced time to deployment: Provides best-practice recommendations based on a fully-tested and validated architecture, enabling rapid technology adoption and deployment

• Reduced risk: Enables enterprises and service providers to deploy new architectures and technologies with confidence

• Increased flexibility: Enables rapid, on-demand, workload deployment in a multitenant environment using a comprehensive automation framework with portal-based resource provisioning and management capabilities

• Improved operating efficiency: Integrates automation with a multitenant pool of computing, networking, and storage resources to improve asset use, reduce operation overhead, and mitigate operation configuration errors

The Cisco VMDC architecture, consists of the Cisco Unified Data Center and Cisco Data Center Interconnect (DCI) together with other architectural components such as infrastructure abstraction, orchestration and automation, assurance, and integrated services and applications, as shown in Figure 1.

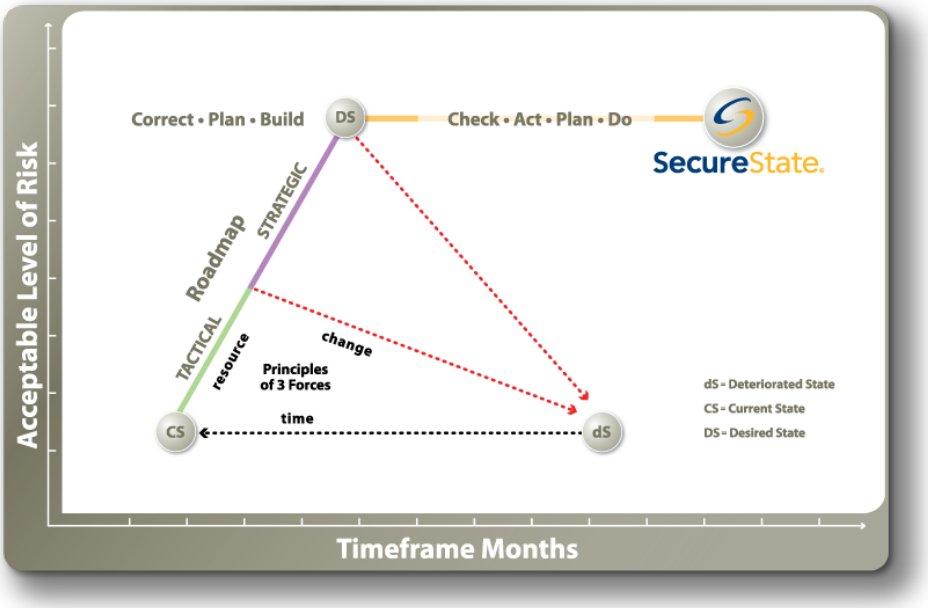


SecureState

SecureState is a management consulting firm that specializes in information security. Since 2001, SecureState has been providing services to organizations within the Federal Government as well as commercial customers, providing an unmatched expertise in the application of Federal regulations into commercial and Federal environments. Each year, SecureState's team performs more than 350 security consulting engagements for more than 200 customers including NASA, the Department of Treasury, USAF, Army, Federal Highway Administration, Federal Reserve, Rite Aid, Dick's Sporting Goods, North American Electric Reliability Corporation, and FirstEnergy to name a few.

Philosophy

SecureState believes in a different approach to security; understanding clients' business needs and aligning security to accomplish those objectives. This is done by offering technical services that facilitate strategic decisions. These services fit the business model that facilitates SecureState's clients' pursuit of their future goals (DesiredState) from where they are now (CurrentState). Ultimately, SecureState's goal is for clients to achieve a consistent, measurable and repeatable process that can be applied to any business environment, thus improving efficiency and accountability for everyone involved. In security it is referred to as the SecureState.



In terms of understanding FISMA, SecureState provides these services to Government and Commercial customers on a consistent basis, assisting organizations in identifying their CurrentState of compliance with FISMA and assisting them to achieve their DesiredState and SecureState. For this work SecureState builds Certification & Accreditation Packages, tests compliance and helps to configure systems for compliance.

SecureState's team of resources is consistently looked upon as thought leaders in information security, presenting at conferences such as InfoSec World, DefCon, BlackHat, and SecureWorld Expo. The team is also sought after by journalists for publications such as SC Magazine, InformationWeek, and Federal CIO Magazine. Recently, SecureState received the security industry's Global Excellence Award for Best Overall Security Company of the Year.

The FISMA Compliance Problem

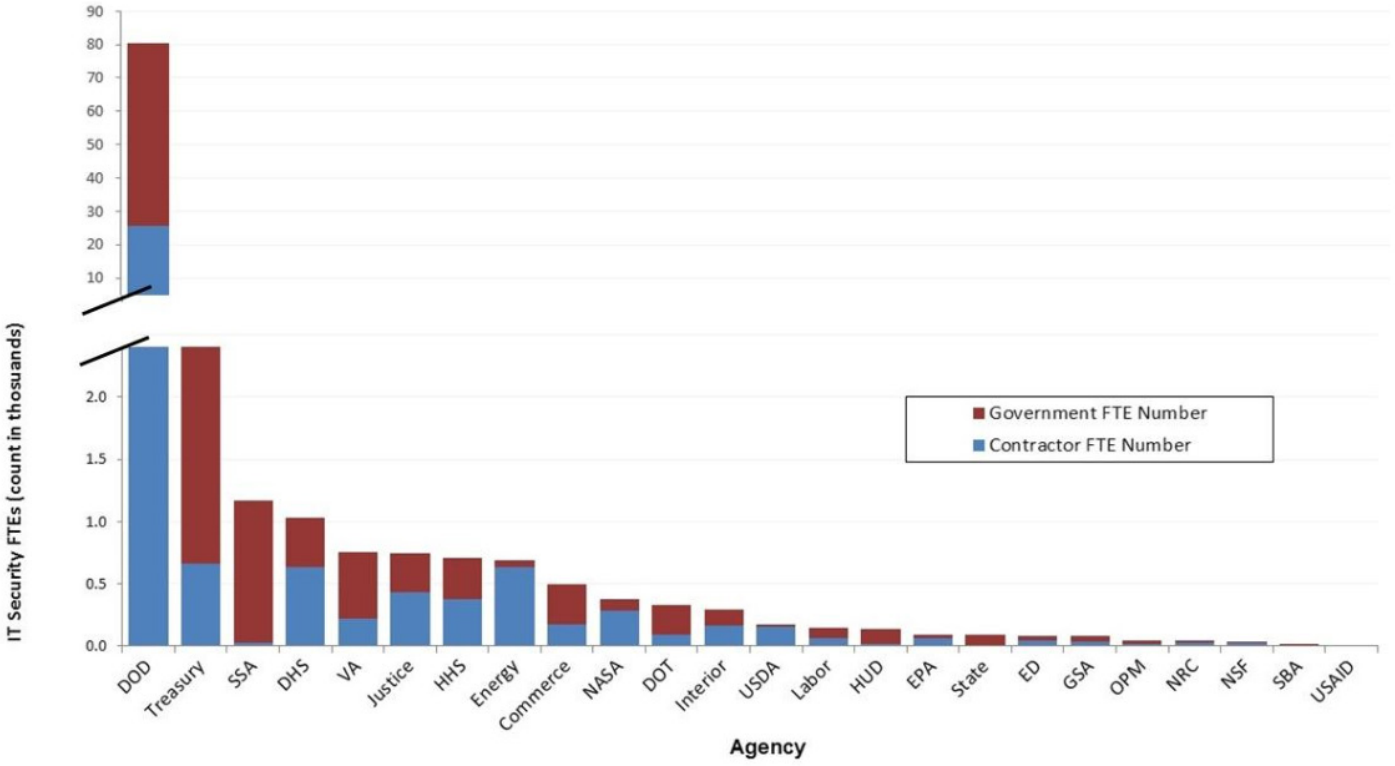
The Office of the Inspector General (OIG) states in their 2012 report "Continuous monitoring programs are most effective when combined with other agency initiatives to strengthen the underlying information technology infrastructure by integrating security requirements into organizational processes (e.g., enterprise architecture, acquisition/procurement, systems engineering, and the system development life cycle)," (Fiscal Year 2012 Report to Congress on the Implementation of The Federal Information Security Management Act of 2002, Pg. 5). However getting to a compliant state is a continual problem within FISMA. Though federal organizations have been working toward compliance since 2002, OIG audits indicate there remains a significant compliance gap for these organizations.

Agency	FY 2012 (%)
Nuclear Regulatory Commission	99
General Services Administration	99
Department of Homeland Security	99
Social Security Administration	98
Department of Justice	94
National Aeronautics and Space Administration	92
Department of Interior	92
National Science Foundation	90
Department of Labor	82
Department of Veterans Affairs	81
Department of Education	79
Office of Personnel Management	77
Environmental Protection Agency	77
Department of Treasury	76
Department of Energy	72
USAID	66
Department of Housing and Urban Development	66
Department of Commerce*	61
Small Business Administration	57
Department of Transportation	53
Department of State	53
Department of Health and Human Services	50
Department of Agriculture	34
Department of Defense**	N/A

**DOC OIG performed a risk assessment and focused its review on a limited number of attributes. The scoring is based on a modified methodology to reflect this.*
***DOD did not provide the answers with the detail required for scoring for FY 2012.*

FISMA Costs

During FY2012, reporting agencies accounted for $14.6 billion in IT security spending (OIG pg 35). Of that amount, over $400 million was spent on implementation of the Risk Management Framework. Across the federal government, this work is performed by over 60,000 federal employees and an additional 29,000 Support Service Contractors. Simply stated, the cost for FISMA compliance is financially labor intensive.



Finding Compliant Solutions

FISMA compliant solutions are not readily available for implementation into the federal Risk Management Framework. This lack of availability is largely due to a lack of understanding regarding FISMA technical requirements and how vendors may provide streamlined solutions. Solutions that are capable of becoming compliant frequently provide technical solutions which require a change or tailoring of operational and management controls to maintain compliance.

Root Cause

Difficult to Configure Solutions for Compliance

Without a thorough understanding of FISMA and security control implementations, many solutions do not integrate FISMA compliance into their development lifecycles. Without security integration, configuring solutions to comply with FISMA becomes a complicated and tedious process contributing to excessive financial and labor costs. Organizations will find implementing new solutions into an existing architecture is similar to fitting a square peg in a round hole for each individual control. In some instances, system customization must be performed to meet requirements. These complications add onto an existing high-dollar compliance program.

In an increasingly dynamic environment facing advanced persistent threats, the challenge of effectively achieving and maintaining FISMA compliance can be significant. The additional reporting requirements of continuous monitoring can overwhelm organizations that have not aligned security controls to achieve operational efficiencies where possible, and implemented automation where practical. This is especially critical in the modern data center where some – possibly a majority of – assets are virtual rather than physical in nature, and yet maintaining a proper inventory of those assets and associated security configurations despite a changing environment remains a requirement.

Some Solutions Cannot Become Compliant

Solutions are frequently released to market with a shortened development lifecycle to improve the bottom line. As a result, these solutions are engineered by compromising security features and at times have an inability to integrate security after deployment. For a FISMA-compliant organization, these solutions present a complicated and long-term risk decision. If competitive solutions exist, the competitor may be chosen at the sacrifice of functionality. In many instances however, competitive solutions do not exist, resulting in a functional investment at a level of long-term risk.

The Cisco VMDC Solution

The Cisco VMDC secures the Unified Data Center that hosts mission-critical applications and sensitive data. The Cisco Unified Data Center changes the economics of the data center by unifying computing, storage, networking, virtualization, and management into a single, fabric-based platform, designed to increase operating efficiency, simplify IT operations, and provide business agility. Unlike other solutions, which add layers of management software to achieve integration, the Cisco Unified Data Center is specifically designed for virtualization and automation and enables on-demand provisioning from shared pools of infrastructure across physical and virtual environments.

Cisco contracted SecureState to perform a FISMA Gap Assessment of Cisco VMDC architecture and technical capabilities. The gap assessment was conducted to determine the architecture's capability to support FISMA compliance against NIST controls as they are applied in accordance with FISMA law.

The FISMA Gap Assessment process focused on the security of information systems by determining whether Cisco has effectively implemented the capabilities required to apply adequate security measures to comply with the requirements as outlined by NIST. A tailored FIPS Moderate baseline was identified to ensure appropriate technical controls could be implemented under FISMA requirements.

VMDC assessed to a moderate baseline. 78 of 252 controls were applicable, including controls within Access Control, Audit and Accountability, Identification and Authentication, System and Services Acquisition, System and Communication Protection, and System and Information Integrity families.

Likelihood of Passing FISMA Audits with VMDC

The VMDC assessment found all 78 of the controls identified above as being satisfied when an organization implements the Cisco VMDC architecture in accordance with Cisco's configuration documentation. These controls aid organizations by providing guidance with numerous NIST control families including Access Control, Audit and Accountability, Identification and Authentication, System and Services Acquisition, System and Communication Protection, and System and Information Integrity. Leveraging the technical controls defined by and audited within the Cisco VMDC architecture provides a greater likelihood of passing FISMA audits. This enables organizations to retain control of the operational and management controls while capitalizing on the thought leadership of the VMDC technical controls.

How It Can Be Implemented

FISMA Technical controls can be implemented by integrating the Cisco VMDC solution within the overall data center infrastructure. The Cisco VMDC is tested and validated reference architecture and falls within the Cisco Validated Design (CVD) Program that provides guidance for implementing different deployment models. Cisco Validated Designs consist of systems and solutions that are designed, tested, and documented to facilitate and improve customer deployment. VMDC allows organizations the ability to adopt technical control implementations as provided by the Cisco VMDC solution. Existing management and operational controls remain unaffected allowing implementing organizations the ability to directly integrate the VMDC solution into an existing environment with minimal impact due to FISMA compliance requirements.

Alleviate the FISMA Pain

Integration of the VMDC solution into a FISMA compliant architecture will allow organizations to mitigate impacts on two levels. First, adopting organizations will be capable of implementing predefined configurations which are known to be compliant and more importantly, secure. The overhead of trying to identify what these configurations are will be mitigated as the integration roadmap of 78 controls has been predefined. The second level of impact exists where organizations will be capable of integrating the VMDC solution into a secure environment and adopt existing operational and management controls. This two-tiered benefit relieves FISMA impacts for system integration and management within the environment.

The secure Cisco VMDC Validated Design enables a transparent network flow from the physical to the virtual network, enabling agile operations and simpler management. It can create multiple security zones that logically separate tenant resources from one another in the virtual network and allow fault-tolerant virtual machine movement. Edge security protects the data center from external threats and offers secure contextual access to data center resources. All the inbuilt security features within VMDC provides a seamless mapping and integration of FISMA controls and the VMDC architectural framework.