Managing Cyber Risk in the Cloud

VMware Compliance & Cyber Risk Solutions

March 2016

vmware®

Table of Contents

Managing Cyber Risk in the Cloud

Today's government and business executives are familiar with the benefits that come from improving their information technology operations by using server virtualization when moving to the cloud. Those benefits–the ability to respond to change rapidly, isolate applications from one another during a cyber attack and maintain business continuity while keeping resource costs low–have been proven. However, executives chartered with maintaining continuous cyber security and compliance practices continue to be concerned about managing risk, particularly in regulated environments, such as PCI, FedRAMP, FISMA, HIPAA or CJIS just to name a few. The challenges stem from the potential for data to leak from a virtual machine (VM) when VMs share a physical host. And VMs migrating among hosts to improve performance or network accessibility can make it difficult to demonstrate physical location. The cloud presents some solutions as well as some challenges in meeting business, regulatory and policy demands.

Compliance and Cyber Security in Complex Environments

In today's world, there are many threats to secure and responsive operations. Executives are asked to meet a new regulatory requirement on a very tight deadline, ensure business operations meet tough Service Level Agreement commitments (e.g. low or no downtime for maintenance, 24 hour services), and provide evidence that data is consistently secure and meeting third party standards. Meeting these challenges requires flexibility and speed to market, while still meeting resource and budget restrictions.

To make matters more complicated, there are regulatory requirements. The Federal Trade Commission requires that promises to consumers be met. Additional requirements govern companies that are financial institutions, or process health and health-related information. Government agencies, as well as companies who provide services to government agencies, are required to meet specific standards.

Corporations or agencies which accept payment cards must meet PCI DSS standards consistently. Some companies are challenged to meet other trade association standards such as AICPA, AMA, CTIA and DMA as well, or to comply with Common Control Frameworks like COBIT and CSA. Investor Relations practices may demand reporting like Government Request Transparency Reports. Corporate governance procedures may require publicly-held and private companies to conduct privacy and security audits and report to their boards. Contractual commitments made to customers or required from vendors may require privacy and security assessments.

The list of requirements and restrictions to meet compliance policies is exhausting. And the risks of non-compliance can be very high. Data breaches, for example, are increasingly expensive to the enterprise that hasn't adequately protected its data. The Ponemon Institute[1] in its annual global Cost of Data Breach study found:

> *"…The average cost to a company was $3.5 million in US dollars and 15 percent more than what it cost last year. The research reveals that reputation and the loss of customer loyalty does the most damage to the bottom line. In the aftermath of a breach, companies find they must spend heavily to regain their brand image and acquire new customers."*

Enterprises that neglect their data protection responsibilities and do not meet or misstate their policies are often penalized by the US Federal Trade Commission (FTC), usually with a fine and then are required to provide third party audits of their practices for the next twenty (20) years. (See FTC v American Apparel http://www.ftc.gov/system/files/documents/cases/140625americanappareldo.pdf and FTC V. Fandango http://www.ftc.gov/system/files/documents/cases/140819fandangodo.pdf as examples.)

1 http://www.ponemon.org/blog/ponemon-institute-releases-2014-cost-of-data-breach-global-analysis

The Definition of Compliance

Compliance is defined as meeting these diverse obligations, be they regulatory requirements or internal and external policy commitments. Sometimes contractual commitments are made, too, such as service level agreements. In today's agency and business environments, compliance generally means providing adequate agreed-upon controls, according to specific guidelines, and then demonstrating via internal or external audit that you have and maintain those controls.

Assessing risks and then developing adequate controls can be difficult in evolving environments. The threats and the attack vectors increase. The regulations become more exacting. The changes you need in your environment to address threats and control gaps continue to grow as do the consequences of inadequate controls. With complexity comes rising costs: the costs of audits and remediating the findings; the longer time needed to develop and implement new offerings; and the costs of maintaining the environment as new vulnerabilities are discovered.

Developing the controls necessary to reduce cyber risk in addressing today's and tomorrow's threats, while staying compliant with the many regulations or sets of standards confronting you, is a multi-faceted challenge. VMware® has developed solutions which can provide the guidance along with our reliable technology needed to manage compliance and cyber security more effectively. Because each agency or business operation manages risk differently, we have designed the **VMware Compliance and Cyber Risk Solutions (CCRS) Reference Architecture Frameworks** and the **VMware Secure and Compliance Capable Platform** which gives the customer the ability to confidently and quickly secure mission critical virtualized workloads in many critical industries. This approach helps customers to meet critical business needs specific to the regulatory schemes with which they must comply. These technologies and guidance make becoming and staying compliant much more straightforward.

A Strategy for Building and Maintaining Compliance and Cyber Security into your Operations

VMware have designed a holistic strategy for developing compliance and cyber security in a Software Defined Data Center (SDDC). SDDCs are logical constructs managed on physical infrastructure. An SDDC provides the ability to define environments using physical data center assets that can be managed to protect the environments from one another. The same physical assets can be shared, yet the rules and controls governing each environment can be customized for different needs.

The improved use of the physical assets begins with the Trusted Compute Pool. This core of your cloud environment is the integration of protected information about the host, stored in encrypted form, and used by VMware and other software to assure that the host on which you are running is the appropriate trusted one. This important foundation allows the remaining layers of protection, such as automated migration and provisioning and applying separate policies to each environment, to operate solely in trusted environments, enforced by the integration of hardware and software in the SDDC.

Our strategy approaches the tasks of design, planning, and operations from both an architectural and operational perspective and puts methods in place to address cyber security controls across all the environments. The VMware CSS Reference Architecture Framework consists of core architecture design documents, each providing guidance for a specific regulated environment, and each is independently validated by an independent third party auditor to ensure it meets the appropriate regulatory guidelines and requirements.

There are many products that can help with the challenges of compliance: configuration managers, patch management tools, authentication and authorization tools, security vulnerability assessment tools, data leak protection tools, encryption modules, etc. The challenge is to choose the ones that will work well in a particular environment to address specific requirements. The VMware CCRS Reference Architecture Framework provides guidance on how to choose the products that meet a particular environment's needs for agility and security.

The VMware CCRS Reference Architecture Framework also describe regulations, standards and best practices, while, outlining common control frameworks (e.g. that of the Cloud Security Alliance, CSA), requirements for capabilities in the infrastructures (e.g. access control, segmentation, auditability) and how to organize the information so organizations can construct their own architecture. Organizations can use the VMware CSS Reference Architecture Framework to help make thoughtful choices in assembling environments that are secure and compliant.

A VMware CCRS Reference Architecture Framework enables better usage of the physical foundation of servers and network connections by enabling improved networking, consistent and strong security controls like identity access management, and better operational oversight. Creating a SDDC with a hardware root of trust using one of the VMware CCRS Reference Architecture Frameworks provides organizations and agencies with the following advantages:

- Processing of data is more secure, faster and more efficient than because the storage, transmission, and processing of the data is done in a secure environment containing only the necessary components for the process.
- By utilizing trusted compute pools with known, good integrity as verified by a hardware root of trust, IT enables secure, dynamic migration of VMs from one trusted environment to another.
- Each environment is managed with its own policy, ensuring that the rules accompany the workload.
- Systems administrators are not able to view, move or amend protected data.
- Adding processing power or moving a workload for improved access or for business continuity is done automatically.
- Automatic management provides protection from the risk of programming errors or other human malfeasance.

Summary

The VMware CCRS Reference Architecture Framework and Secure and Compliance Capable Platform can help an organization meet and maintain regulatory and policy requirements by providing a method to link integrated software and hardware features to specific regulatory controls with independent audit validation. Each VMware CCRS Reference Architecture Framework includes design, configuration and deployment guidance and best practices selected to help you maximize the use of your hardware and software while meeting compliance requirements and managing cyber risk. Design and operation of environments based on a VMware CCRS Reference Architecture Framework will enable effective use of reliable virtualization and cloud technologies that are validated to work together to provide breakthrough speed, efficiency and agility while securing data in the cloud.