VMware's Approach to Compliance

June, 2012

V 1.0

vmware®

Table of Contents

VMware, Inc. 3401 Hillview Avenue Palo Alto CA 94304 USA Tel 877-486-9273 Fax 650-427-5001 www.vmware.com

1. Introduction

Many organizations have initiatives to virtualize their Information Technology (IT) infrastructure, or to move to a Cloud Computing model. However, these initiatives are often complicated by the increasing number of regulatory compliance requirements, which require protection of data such as [1]PCI, [2]HIPAA, [3]FISMA, [4]DIACAP, [5]FedRAMP, [6]GLBA, and other State and Federal requirements. Organizations are increasingly concerned with the complexity, risk, and impact that a new technology can bring to their existing environment(s).

Historically, most organizations have had to gradually gather solutions from a variety of vendors and best practices in order to create an entire IT architecture that can meet their business compliance needs. While each vendor may have their own specific guidance on how to meet compliance, they often do not have guidance on how to meet controls which were not addressed by their specific solutions. This can lead to a delay in the adoption of cloud and virtualization initiatives as it often requires a significant investment in time, resources, and technical capabilities.

VMware is addressing these challenges by establishing a Reference Architecture Framework (RAF) that provides a consistent way for VMware, its partners, and organizations to assess and evaluate the impact of regulations on virtual and cloud environments. The intent of the RAF is to provide a single framework for VMware, its partners, and organizations to address a variety of compliance requirements across an IT infrastructure*. The RAF is comprised of four primary components:

1. **Use Case** - Provides a business description of an organization and how it has designed its IT architecture to meet specific regulatory and compliance requirements.

2. **VMware Product Suites** – VMware's recommended product suites designed to help meet compliance requirements

3. **VMware Partner Products** – Provides a framework for partners to address controls that are not covered by VMware's product suites.

4. **Organizational Requirements** - Provide guidance on control requirements not addressed by VMware or Partner solutionssuch as physical security.

VMware's goal is to deliver a complete solution that helps our customers meet compliance requirements as they look to migrate their business critical applications to cloud computing.

* VMware solutions are designed to help organizations address various regulatory compliance requirements. This document is intended to provide general guidance for organizations that are considering VMware solutions to help them address such requirements. VMware encourages any organization that is considering VMware solutions to engage appropriate legal, business, technical, and audit expertise within their specific organization for review of regulatory compliance requirements. It is the responsibility of each organization to determine what is required to meet any and all requirements. The information contained in this document is for educational and informational purposes only. This document is not intended to provide legal advice and is provided "AS IS". VMware makes no claims, promises or guarantees about the accuracy, completeness, or adequacy of the information contained herein. Nothing that you read in this document should be used as a substitute for the advice of competent legal counsel.

[1]PCI – Payment Card Industry - https://www.pcisecuritystandards.org/
[2]HIPAA – Health Insurance Portability and Accountability Act - http://www.hhs.gov/ocr/privacy/
[3]FISMA – Federal Information Security Management Act - http://csrc.nist.gov/groups/SMA/fisma/faqs.html
[4]DIACAP – Department of Defense Information Assurance Certification and Accreditation Process - http://www.diacap.net/whatisdiacap.html
[5]FedRAMP – Federal Risk and Authorization Management Program - http://www.gsa.gov/portal/category/102371
[6]FGLBA – Gramm-Leach-Bliley Act – http://business.ftc.gov/privacy-and-security/gramm-leach-bliley-act

VMware, Inc. 3401 Hillview Avenue Palo Alto CA 94304 USA Tel 877-486-9273 Fax 650-427-5001 www.vmware.com

2. Security, Compliance, and Guidelines

The terms security and compliance are often used interchangeably, however they are unique and distinct words. Many IT products are designed to be secure and have several published security features. However, there is substantially less guidance on compliance.

While there are several different definitions of information security, it is commonly defined as a set of technical, physical, and administrative controls that are implemented in order to provide confidentiality, integrity, and availability. Security is not an end state (i.e. you are never completely secure). Rather, organizations make risk based decisions in order to manage security to appropriate levels.

Compliance is a set of requirements necessary to meet the minimum controls established by different regulatory agencies or industry best practices. Compliance frameworks are usually broad frameworks that provide limited guidance on any specific type of technology, vendor, or configuration. However, as technology continues to advance, many compliance entities have issued supplemental guidance to address emerging technological risks and industry trends.

There has been an increasing amount of supplemental guidance and best practices issued specifically for cloud computing and virtualization technologies. These best practices provide a useful guide for organizations and auditors, assessors, and examiners when reviewing the appropriate controls and risks in cloud computing and virtual environments. Some of the recent guidance issued includes:

IRS

Safeguards Technical Assistance Memorandum Protecting Federal Tax Information (FTI) In Virtual Environments
www.irs.gov/pub/irs-utl/9.18.12.virtualenvironments.doc

PCI Security Standards Council

Payment Card Industry Data Security Standard Virtualization Guidelines
https://www.pcisecuritystandards.org/documents/Virtualization_InfoSupp_v2.pdf

NIST National Institute of Standards and Technology U.S. Department of Commerce

NIST SP 800-144 Guidelines on Security and Privacy in Cloud Computing
http://csrc.nist.gov/publications/nistpubs/800-144/SP800-144.pdf

CSA cloud security alliance SM

Cloud Security Alliance, Security Guidance for Critical Areas of Focus in Cloud Computing
https://cloudsecurityalliance.org/

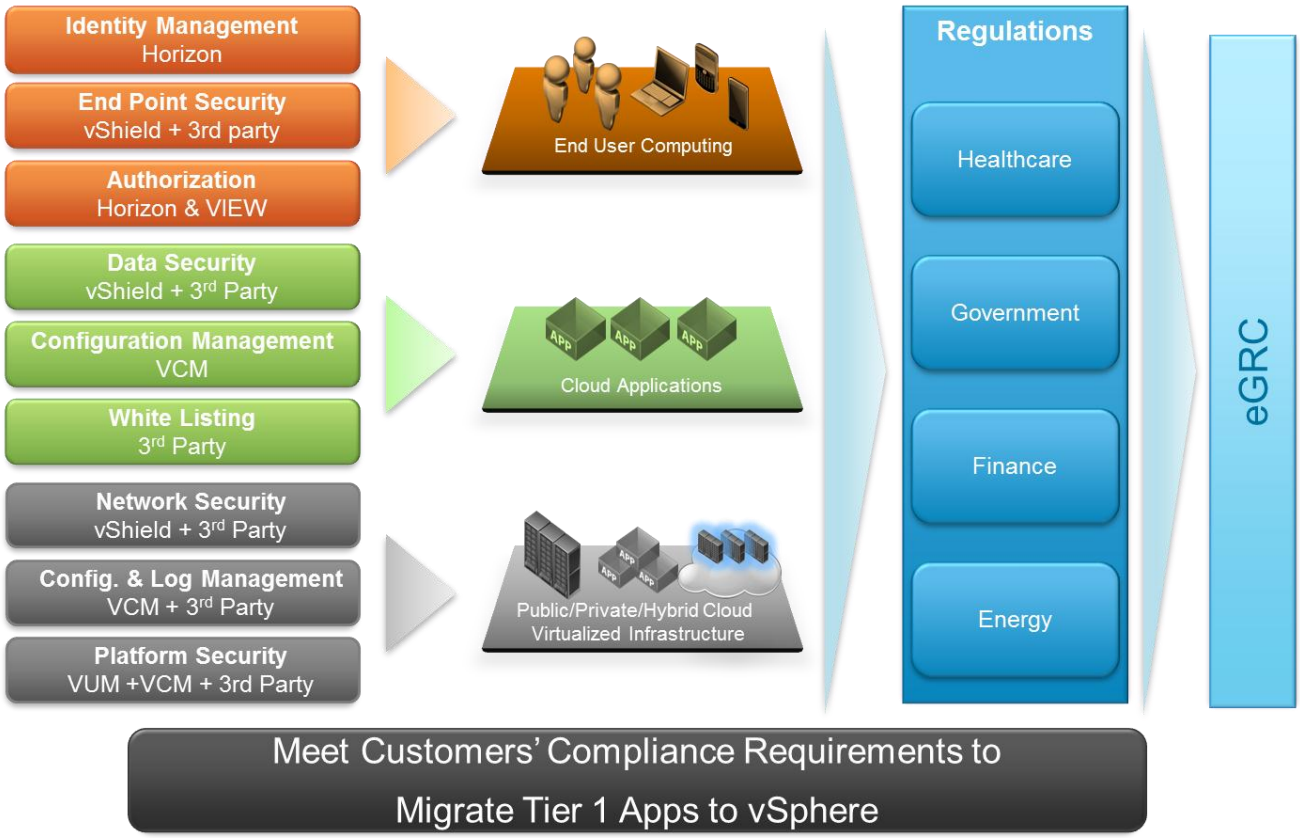
enisa European Network and Information Security Agency

Cloud Computing Security Risk Assessment
http://www.enisa.europa.eu/act/rm/files/deliverables/cloud-computing-risk-assessment

3. A View of VMware's Compliance Solutions

VMware has a variety of solutions that are designed to help organizations meet security and compliance requirements. The framework below provides a visual representation of VMware's products that are designed to address a customer's compliance requirements. VMware's products can be grouped into three distinct areas: Products that address the virtualized infrastructure, Applications, and End user computing. Each of these areas provides a standard set of use cases for different regulations.

Figure 1: VMware Products

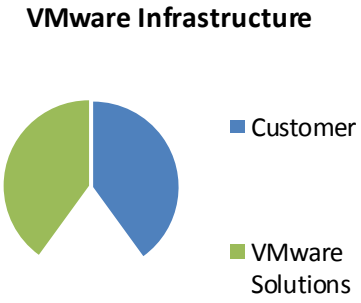


4. Mapping VMware, Partner Solutions, and End User Solutions to Meet Controls

One of the first steps an organization often takes when reviewing compliance initiatives, is to map the compliance requirements (usually control objectives) to their specific organizational needs. As mentioned earlier, this can be a difficult task, requiring a significant amount of time and resources. To streamline the process, VMware has established a single holistic approach that can be used to evaluate the VMware environment, Partner Solutions, and End User tools.

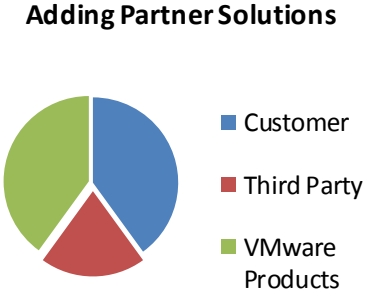
Establish Controls

Organizations establish control objectives in order to meet regulatory, security, and best practice objectives. These controls consist of a series of technical guidance, configuration requirements, policies, procedures, standards, and guidelines that must be satisfied. The controls are then mapped to processes, technology, and people to meet the objectives.



VMware Solutions

Organizations can significantly reduce the complexity of compliance, while simultaneously reducing costs and IT manpower by replacing traditional non-integrated solutions with integrated solutions. VMware has mapped its product suites to specific regulatory controls objectives. However, as with any product, no single product from any vendor can meet all of an organization's needs. This gap (white space) between VMware's solutions and the customer's other objectives can be addressed by VMware Partner Solutions.



Partner Solutions

By establishing a consistent way of mapping Partner Solutions to a comprehensive controls framework, VMware has established a standardized repeatable architecture for VMware Partner products. These Partner Products are tailored to integrate with the VMware architecture, thereby providing a single integrated solution. By building clouds and virtual environments based on a standardized reference architecture framework, the result is an environment which is more secure, less costly, and better equipped to meet the dynamic nature of today's IT and Compliance world. It also reduces the time and resources required to evaluate the different solutions and capabilities for any organization.

VMware, Inc. 3401 Hillview Avenue Palo Alto CA 94304 USA Tel 877-486-9273 Fax 650-427-5001 www.vmware.com

5. Partner Solutions – Filling the Whitespace

As is the case for any software or hardware vendor offerings, there are no readymade solutions to meet every compliance requirement. Meeting all controls depends upon a variety of hardware and software providers. To help address these challenges, VMware has identified seven Partner Areas that are designed to fill the compliance gaps not addressed by VMware-only products, rather than leaving it up to an organization to choose which products to "mix and match." As part of VMware's Partner program, VMware has established a standardized process for Partners to map their solutions to VMware environments.

Table 1: VMware's Seven Partner Areas

VMware's- Seven Partner Areas	Description
1. Hardware	Partners solutions that address hardware requirements and form the backbone of a cloud environment, such as servers, storage, networking, etc.
2. Authentication	Partner solutions that assist in the management, reporting, and authentication processes used in a cloud environment.
3. Logging and Monitoring	Partner solutions that aggregate log information, extract logs from systems, applications, and appliances, and provide monitoring and notification services.
4. Endpoint Security	Partner solutions that secure endpoints such as anti-virus, encryption, VPN, IDS, etc.
5. Encryption	Partner Solutions that encrypt, tokenize, mask, or truncate data. These solutions may address data at rest or in transit.
6. Availability	Partner solutions that assist with business continuity, availability, disaster recovery, and other services that enable IT operations to continue during incidents.
7. Other	Partner solutions that address other requirements, technological gaps, or provide enhancements for controls that are addressed in the above six areas.

6. Solution Guides, Reference Architectures and Toolkits

In addition to mapping VMware and Partner solutions to regulatory requirement use cases, VMware is also building Solution Guides, Reference Architectures, Compliance Solution Toolkits and Implementation Plans (IP's). These solution credentials and IP's go beyond the hypothetical deployment scenarios and provide specific implementation and configuration guidance. They provide guidance for IT Architects, Administrators, and Auditors and thereby help organizations to properly design, deploy, and operate a more secure, compliant cloud.

Figure 2: VMware vCloud Architecture Toolkit

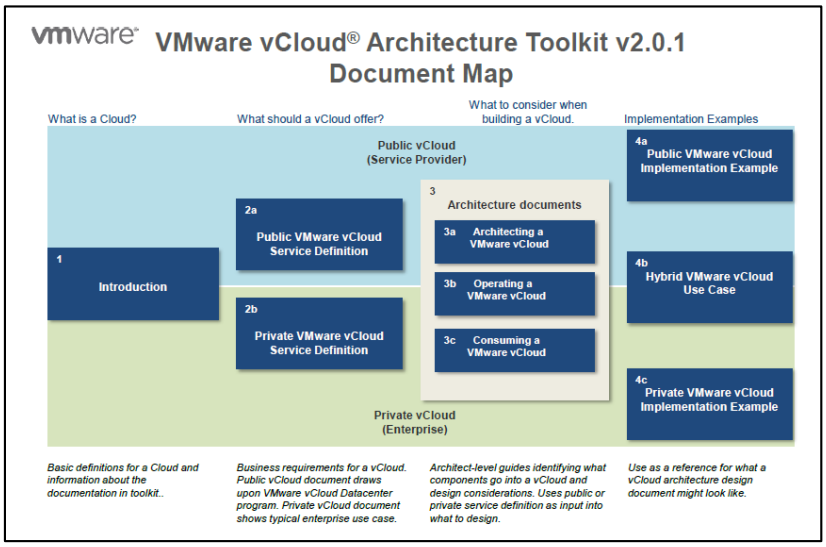
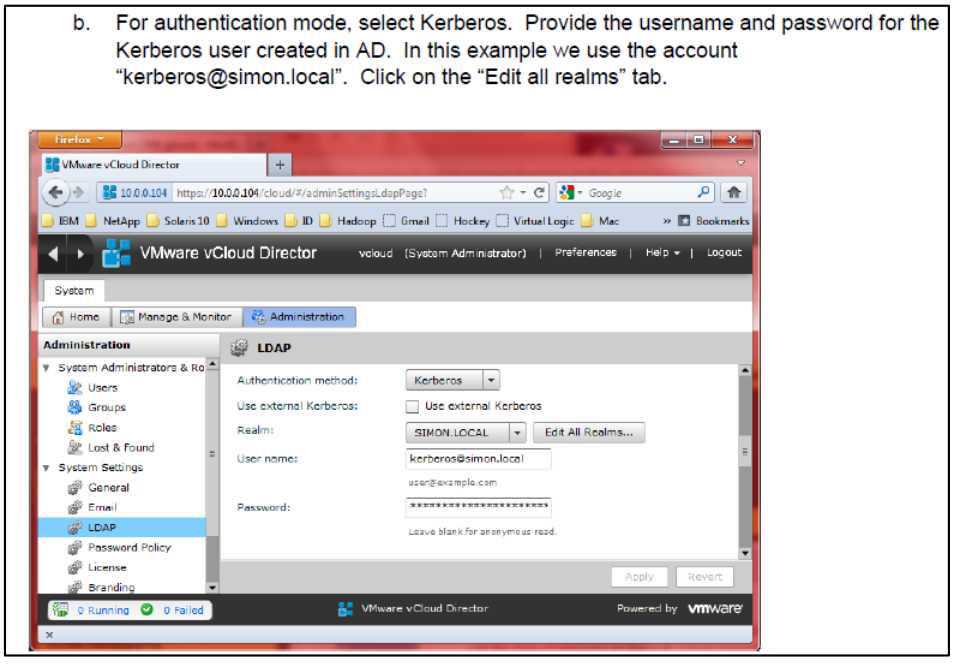


Figure 3: Example of DIACAP Implementation Plan



7. Conclusion

VMware recognizes that security and compliance are critical areas that must be addressed by all organizations. By standardizing an approach to compliance and expanding the approach to include Partners, VMware aims to provide customers a proven solution that more fully addresses their compliance needs. This approach provides management, IT architects, administrators, and auditors a high degree of transparency into risks, solutions, and mitigation strategies for moving critical applications to the cloud in a secure and compliant manner.

If you are an organization or partner that is interested in more information on the VMware Compliance Program, please email us at compliance@vmware.com

Acknowledgements:

VMware would like to recognize the efforts of the VMware Center for Policy & Compliance, VMware Partner Alliance, and the numerous VMware teams that contributed to this paper and to the establishment of the VMware Compliance Program. VMware would also like to recognize the Coalfire Systems Inc. VMware Team www.coalfire.com/Partners/VMware for their industry guidance. Coalfire®, a leading PCI QSA firm, provided PCI guidance and control interpretation aligned to PCI DSS v. 2.0 and the Reference Architecture described herein.

The information provided by Coalfire Systems and contained in this document is for educational and informational purposes only. Coalfire Systems makes no claims, promises or guarantees about the accuracy, completeness, or adequacy of the information contained herein.

About Coalfire®

Coalfire Systems is a leading, independent information technology Governance, Risk and Compliance (IT GRC) firm that provides IT audit, risk assessment and compliance management solutions. Founded in 2001, Coalfire® has offices in Dallas, Denver, Los Angeles, New York, San Francisco, Seattle and Washington, D.C., and completes thousands of projects annually in retail, financial services, healthcare, government and utilities. Coalfire® has developed a new generation of cloud-based IT GRC tools under the Navis™ brand that clients use to efficiently manage IT controls and keep pace with rapidly changing regulations and best practices. Coalfire's solutions are adapted to requirements under emerging data privacy legislation, the PCI DSS, GLBA, FFIEC, HIPAA/HITECH, NERC CIP, Sarbanes-Oxley and FISMA. For more information, visit www.coalfire.com.

VMware, Inc. 3401 Hillview Avenue Palo Alto CA 94304 USA Tel 877-486-9273 Fax 650-427-5001 www.vmware.com