Introducing Security and Compliance

21 AUG 2018

VMware Validated Design

vmware®

You can find the most up-to-date technical documentation on the VMware website at:

https://docs.vmware.com/

If you have comments about this documentation, submit your feedback to

docfeedback@vmware.com

VMware, Inc.
3401 Hillview Ave.
Palo Alto, CA 94304
www.vmware.com

Contents

About Introducing Security and Compliance

The *Introducing Security and Compliance* document provides general guidance for organizations that are considering VMware solutions to help them address compliance requirements.

Legal Disclaimer This document is intended to provide general guidance for organizations that are considering VMware solutions to help them address compliance requirements. The information contained in this document is for educational and informational purposes only. This document is not intended to provide regulatory advice and is provided “AS IS”. VMware makes no claims, promises or guarantees about the accuracy, completeness, or adequacy of the information contained herein. Organizations should engage appropriate legal, business, technical, and audit expertise within their specific organization for review of regulatory compliance requirements.

Intended Audience

Introducing Security and Compliance is intended for cloud architects, infrastructure administrators, and cloud administrators. Familiarity with VMware software is required. This guide introduces security and compliance as it relates to the VMware Validated Design for Software-Defined Data Center (SDDC).

Required VMware Software

The *Introducing Security and Compliance* document builds on top of VMware Validated Design for Software-Defined Data Center implementations. See *VMware Validated Design Release Notes* for more information about supported product versions.

Security and Compliance in VMware Validated Design

1

Security and compliance guidance outlines the built-in controls in the VMware Validated Design for Software-Defined Data Center and the additional controls that can be added by using enhanced guidance.

Currently, a subset of enhanced guidance controls is part of this document. The document also outlines the overall approach to be used in both the built-in controls and enhanced guidance.

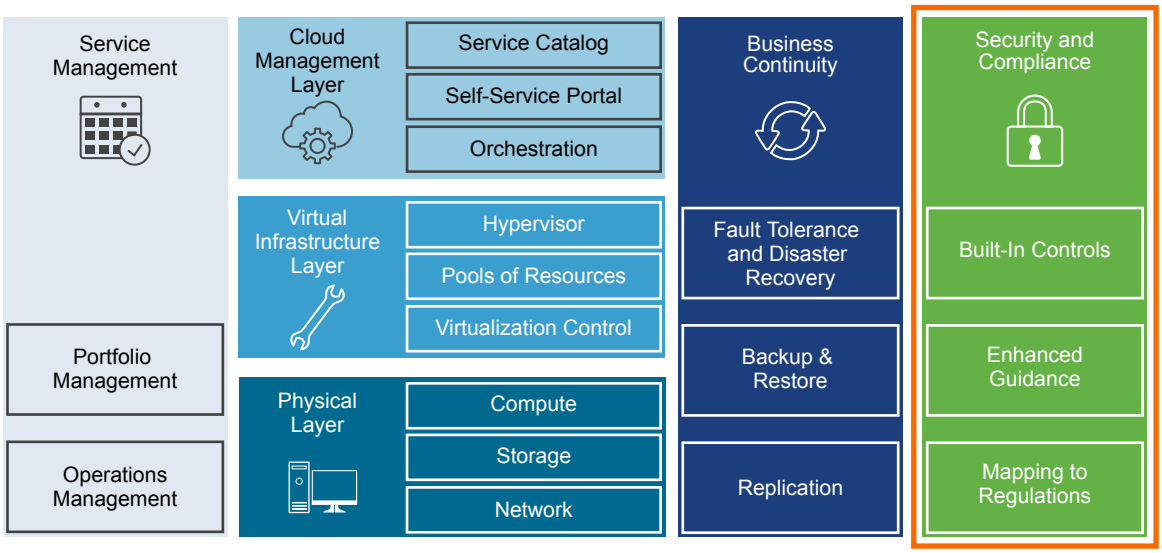
Built-in Controls	Security controls based on compliance requirements that are part of the VMware Validated Design for Software-Defined Data Center. Some controls might require additional configuration, but by design the capabilities are included in the current implementation.
Enhanced Guidance	Additional guidance on a per regulation, or standard basis includes a set of capabilities that can be added to the existing VMware Validated Design for Software-Defined Data Center implementations.

Security Architecture

2

Security in the VMware Validated Design is evaluated with a clear objective to balance best practices with usability and performance.

Figure 2-1. Security and Compliance in the VMware Validated Design for Software-Defined Data Center Layers



For VMware Validated Design for Software-Defined Data Center implementations, security must be handed over to a dedicated team (post-deployment) to augment and monitor the security posture. Attack vectors and compliance guidelines are constantly evolving so the information provided can be used to establish a baseline, not an absolute, or complete picture.

NIST 800-53 (Revision 4) forms the security baseline, backdrop, and security foundation used to evaluate the VMware Validated Design. It was selected because of its vast array of controls and because it is often used by other regulations as part of their reference framework.

NIST is a risk-based framework, which requires each organization to assess their own risk posture and identify applicable controls. The VMware Validated Design does not remove this step. The VMware Validated Design security design and compliance mappings are presented to inform the reader of both design decisions, and security controls that can be leveraged.

It is important that the VMware Validated Design security design is not enough on its own. Each organization has a series of supporting security architecture, technology, processes, and people to evaluate.

Super users of the system inherit various technologies and typically work with security specialists to implement controls effectively. The VMware Validated Design has evaluated many design decisions that are incorporated with the overall design. Subsequent deployments benefit from post-implementation security health checks to enhance the organizations security posture as it relates to the VMware Validated Design.

Compliance Regulations and Standards

Organizations expect to keep data safe. They must often comply with one or more regulations from government standards to private standards such as:

- National Institute of Standards and Technology (NIST)
- Defense Information Systems Agency Security Technical Implementation Guides (DISA STIG)
- Federal Risk and Authorization Management Program (FedRAMP)
- Health Insurance Portability and Accountability Act (HIPAA)
- North American Electric Reliability Corporation - Critical Infrastructure Protection Committee (NERC CIP)
- Payment Card Industry (PCI)
- American Institute of Certified Public Accountants - Statement of Compliance (AICPA, SOC 1, or SOC 2)
- International Organization for Standardization number 27001 (ISO27001)

Security Versus Compliance

The VMware Validated Design approaches security and compliance concepts in a practical manner. Security supported by the VMware Validated Design reduces the risk of data theft, cyberattack, or unauthorized access. While compliance is the proof that a security control is in place, typically within a defined timeline. Security and compliance work with a broader set of considerations including people, processes, and technology. Security is primarily outlined in the design decisions and highlighted within the technology configurations. Compliance is focused on mapping the correlation between security controls and specific requirements. A compliance mapping provides a centralized view to list out many of the required security controls. Those controls are further detailed by including each security control's respective compliance citations as dictated by a domain such as NIST, PCI, FedRAMP, HIPAA, and so forth.

Infrastructure Provider Role and Multi-Tenant Consumer

The VMware Validated Design is deployed using multiple components, for more details see the *VMware Validated Design Architecture and Design* document. In instances of tenancy, either a single tenant or one of multi-tenancy, consumers must be restricted to their respective tenant environments. Access to certain components, or products, might provide visibility into the wider VMware Validated Design functions. These wider VMware Validated Design functions form the backdrop that the infrastructure service provider manages. Access must be assigned only to the levels desired and clearly articulated in group nomenclature to avoid adding consumers into group membership that can extend outside of their approved tenant environment. Components that might be considered for a restriction in layers include:

- Physical
- Virtual infrastructure
- Operations management
- Cloud management
- Business continuity

Typically, access to the virtual infrastructure layer must be further restricted to the tenant environments that the consumer must have access to.

For this guide, the scope is restricted to securing the infrastructure provider, or service provider. Security at the tenant level is not the focus.

NIST as a Security Baseline

The National Institute of Standards and Technology (NIST) works to promote innovation across all industries. In the realm of information security, cybersecurity, and technology, it has created a risk-based framework that provides a catalog of security controls for organizations to secure their systems. This catalog was used as a general guideline to evaluateVMware Validated Design for Software-Defined Data Center. In addition, many regulations cite NIST and build on its baseline. So, the NIST security baseline was deemed as a key building block to design VMware Validated Design security and provide compliance mapping to other regulations/standards.

Classification of Security Controls

3

VMware Validated Design security approach uses three categories to classify security controls.

The following classification identifies security controls, especially within the compliance mapping. This classification also provides a label to underscore each security control's applicability: partial applicability, or no applicability. Security controls were evaluated against each of the following categories to evaluate its scope and relevance to the VMware Validated Design.

Core technology	Security controls with matching VMware Validated Design capabilities that can be configured with minimal to no dependency on any technology outside of the SDDC. For example, the use of certificates to improve trust within systems falls into this category.
People or process administrative	Security controls that depend on other technology, depend on a wider process, and can be configured in the SDDC. This security control configuration might only be a step within a wider process. For example, assigning users into groups must be part of a wider Access Control process that might depend on other technology such as Active Directory.
Compliance mapping	Customers face varying degrees of compliance domains. For example, PCI for the credit card industry, HIPAA for healthcare, FedRAMP for government regulation in the cloud. We use NIST 800-53 as a mapping baseline to evaluate the population of eligible security controls. The compliance mapping serves to translate the foundation of VMware Validated Design capabilities to the compliance flavor per each enhance guide.

Security Principles

4

Across all regulations or standards, security principles dictate the mind set used when applying security controls within the VMware Validated Design.

Security Principles and Considerations

The following common concepts in separation of duties and privileges are considered:

- Infrastructure provider vs. multi-tenant consumer
- Least privilege
  - Super user
  - Developer
  - Operations team
  - Analyst
  - System account
- Separation of duties
  - Super user compared to non-super user
  - Service accounts compared to user accounts
  - System to system communication
  - Development environment compared to production environment
  - Create, edit, or delete compared to read-only.

User Roles Based on Least Privilege

Access to the VMware Validated Design must be tailored specifically to the type of work that is required. Where possible, access must be restricted to each role based on the user's job function, title, and authorization. The following roles have been established within the VMware Validated Design Security Architecture Design:

Super user — Charged with managing the system and performing elevated privilege actions.

Developer — Primarily creating functionality within the system and especially restricting access to the system of ownership (infrastructure vs. multi-tenant consumer).

Operations team — Design the architecture of the cloud, network, storage, and security, or possibly the maintenance of the system as required.

Analyst — Focused on viewing relevant system data, or auditing settings and restricting access as required, and providing system models and reports to the relevant teams ensuring effectiveness

The concept of an "average user" is not included. The SDDC components outlined in the architecture overview are part of the VMware Validated Design design and management. A typical user might be restricted to the use of an application, or other end-point solution, rather than have access to the SDDC infrastructure.

The following tables are a sample on least privilege in a roles matrix for the onfrastructure provider level.

Table 4-1. Physical Layer

	Infrastructure Provider Roles and Responsibilities			
Products	**Super User**	**Developer**	**Operations Team (Day 2)**	**Analyst**
■ VMware ESXi ■ Top of Rack Switches ■ Traditional Storage	ug-Physical-Admin	No access	ug-Physical-OpsTeam (Read Only)	No access

Table 4-2. Virtual Infrastructure Layer

	Infrastructure Provider Roles and Responsibilities			
Products	**Super User**	**Developer**	**Operations Team (Day 2)**	**Analyst**
■ vCenter Server ■ VMware Update Manager ■ VMware NSX for vSphere ■ VMware vSAN ■ Platform Services Controller	ug-VirtualInfra-Admin	No access	ug-VirtualInfra-OpsTeam	No access

Table 4-3. Operations Management Layer

	Infrastructure Provider Roles and Responsibilities			
Products	**Super User**	**Developer**	**Operations Team (Day 2)**	**Analyst**
■ vRealize Log Insight ■ vRealize Operations Manager	ug-OpsMgmt-Admin	ug-OpsMgmt-Developer (Read-Only)	ug-OpsMgmt-Engineer (Read-Only)	ug-OpsMgmt-Analyst

Table 4-4. Cloud Management Layer

	Infrastructure Provider Roles and Responsibilities			
Products	**Super User**	**Developer**	**Operations Team (Day 2)**	**Analyst**
■ vRealize Business Costing ■ vRealize Automation ■ vRealize Orchestrator	ug-CloudMgmt-Admin	ug-CloudMgmt-Developer	ug-CloudMgmt-OpsTeam	ug-CloudMgmt-Analyst

Table 4-5. Business Continuity

	Infrastructure Provider Roles and Responsibilities			
Products	**Super User**	**Developer**	**Operations Team (Day 2)**	**Analyst**
■ Backup software ■ VMware Site Recovery Manager ■ vSphere Replication	ug-BusContinuity-Admin	No Access	ug-BusContinuity-OpsTeam	No Access

Separation of Duties

Establishing trust in the system may require access controls to carve up the flow of work. By establishing a boundary between each key area of a wider process, a review with a focus on governance can be implemented. This approach is used to ensure that changes are not made without prior approval, unauthorized access can be contained, change management processes better monitored, and so on. Because risk tolerance and processes differ so widely, a few key roles are identified and woven into the fabric of the security architecture.

- Super user vs. non-super user
- Service accounts vs. user accounts
- System to system communication
- Development environment vs. production environment
- Create/edit/delete vs. read-only

Compliance Mapping

5

The VMware Validated Design establishes many security capabilities. Some capabilities can be traced to a compliance requirement, while others are best practice.

Where possible, examples of the audit artifacts as evidence can be included in a separate guide, focused on compliance and producing evidence to meet controls. The following is a broad mapping of the principles outlined in the security architecture section and the mapping to prominent compliance domains. The mapping was derived using the Unified Compliance Framework (UCF), a third-party lexicography tool that specializes in the realm of compliance mapping and compliance interpretation.

The compliance mapping is a subject of expansion, as more security controls are evaluated, including additional compliance domains/regulations.

Location of Guidance	Security Control	Category	Type	NIST 800-53 Mapping
Enhanced guidance	Active Directory groups/users	Access control	Administrative	AC-2
Enhanced guidance	Active Directory groups/users	Access control	Administrative	AC-5
Enhanced guidance	Separation of duties using Active Directory groups to assign product roles.	Access control	Administrative	AC-6
Enhanced guidance	Login notification banner	Access control	Technical	AC-8

Legal Disclaimer This document is intended to provide general guidance for organizations that are considering VMware solutions to help them address compliance requirements. The information contained in this document is for educational and informational purposes only. This document is not intended to provide regulatory advice and is provided “AS IS”. VMware makes no claims, promises or guarantees about the accuracy, completeness, or adequacy of the information contained herein. Organizations should engage appropriate legal, business, technical, and audit expertise within their specific organization for review of regulatory compliance requirements.