TEVORA™

VMware® Cloud Foundation Compliance Kit

Audit Guide for NIST 800-53 R4 (Moderate), PCI DSS 3.2.1, SOC 2, FedRAMP, HIPAA, FBI CJIS, DISA STIG, NERC CIP, NIST 800-171/CMMC, GDPR/ISO 27001:2013

January 10, 2022

CONFIDENTIAL: This report is confidential for the sole use of the intended recipient(s). If you are not the intended recipient, please do not use, disclose, or distribute.

Table of Contents

Revision History

Date	Rev	Author	Comments	Reviewers
Jan 2022	1.0	Tevora	Initial Draft	

Design Subject Matter Experts

Name	Author	Reviewers
Christina Whiting	cwhiting@tevora.com	Co-author
Elliot Carroll	ecarroll@tevora.com	Co-author
Carlos Phoenix	cphoenix1@vmware.com	Global Cyber Strategist, VMware

Trademarks and Other Intellectual Property Notices

VMware Cloud Foundation for the Software-Defined Data Center

VMware Cloud Foundation architecture strives to balance security and innovation without sacrificing one for the other. Together, this by-design approach strengthens customers' confidence that, when they implement VMware Cloud Foundation with VMware Validated Design for a Software-Defined Data Center (SDDC), they are getting a comprehensive software stack that not only supports compliance with the top ten security frameworks and any applicable regulatory requirements, but also aides in accomplishing the SDDC design objectives. In addition, the interoperability testing expected from a unified blueprint was extended to include compliance risk assurance through a comprehensive lifecycle development of the VMware Cloud Foundation Compliance Kit for the top 10 regulatory standards, as identified within this document.

VMware Cloud Foundation: Software-Defined Data Center Layer	Key Products
Virtual Infrastructure	VMware ESXi™, VMware vCenter Server® Appliance™, VMware NSX® Data Center for vSphere®, VMware vSAN™, VMware Cloud Builder™
Operations Management	VMware vSphere® Update Manager™ Download Service, VMware vRealize® Operations Manager™, VMware vRealize® Suite Lifecycle Manager, VMware vRealize Log Insight™, VMware Skyline
Business Continuity	VMware Site Recovery Manager™, VMware vSphere Replication™

Disclaimer (Tevora)

The opinions stated in this audit guide concerning the applicability of VMware products to the top 10 compliance frameworks are the opinions of Tevora. All readers are advised to perform individual product evaluations based on organizational needs.

For more information about the general approach to compliance solutions, please visit VMware Compliance Solutions or view the VMware Whitepapers published to the Tevora website. This audit guide has been reviewed and authored by Tevora's staff of information security professionals in conjunction with VMware, Inc.

Disclaimer (VMware)

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.

Executive Summary

Overview

The adoption of virtualization technologies across data centers is altering the audit landscape. Information technology assessors encounter VMware products without substantial technical guidance from regulators and standards bodies. The pace of innovation has caused assessors to develop their own best practices to assess virtualization technologies. VMware engaged Tevora to develop this audit guide to address compliance and technical concerns associated with virtual environments within the VMware Cloud Foundation hybrid cloud.

Implementing a virtual system is not the same as auditing a virtual system. The two viewpoints might have the technology in common, but they are often purposed with different objectives. To bridge this divide, VMware and Tevora are combining efforts to publish documentation and compliance kits to address both audiences. Each compliance kit is built to the address common regulations, standards, and framework3. The kit contains a configuration guide that supports the implementation of the VMware Cloud Foundation, while the audit guide supports the auditing of the deployed, underlying solutions.

Audit Guide Objective

The audit guide strives to empower key stakeholders with responsibilities for IT compliance (i.e., CISO, security administrator, internal audit, external audit) with information and guidance to evaluate security controls within the VMware Cloud Foundation for the Software-Defined Data Center (SDDC). The top 10 regulatory compliance frameworks encompass an organization's strategy, plan, policies, processes, and controls for information security. The goal of this document is to make diverse stakeholders feel confident that their SDDC will align with the requirements defined by the organizations' preferred regulatory framework defined within this document.

A key detail is that this guide supports but does not validate or concretely state an intended compliance outcome. The procedures outlined in the audit guide appendices can be used to produce evidence to audit different security configurations and leverage VMware's expertise to evaluate whether the SDDC is provisioned appropriately. Certifiable compliance is the responsibility of the organization and its designated parties.

How to Use This Audit Guide

This audit guide is constructed to be informative, comprehensive, and audit friendly. The authors are not only technologists but have also held positions responsible for IT compliance. The guide assumes knowledge of the auditing process flow. You can use this document to evaluate existing compliance requirements compared to the VMware Cloud Foundation Compliance Kit for the top ten regulatory compliance standards, and identify control requirements necessary to meet compliance, and test security configurations.

The auditor may use the information within this guide, and any related VMware informational documentation, to better assess the efficacy and accuracy of the audit guide and its contained processes.

The Audit Guide Appendices outline how the SDDC can address the top 10 regulatory compliance standards and their requirements, helping to ensure that the organization is adequately managing risk. The Audit Guide Appendix can be used to inform values for both "default" and "non-default" configurations based upon the applicable Top 10 regulatory frameworks.

Within the scope of this audit guide, regulatory compliance and proper risk management are synonymous and symbiotic functions. This audit guide can be used as an important tool to address regulatory compliance needs, and aides in applying compliance knowledge to documentation gathering, which is used to support security configurations that are required to complete audit tasks.

The appendices are structured to support an audit strategy that focuses on evaluating the security configuration details on how the SDDC features conform to the control sets defined within. You should marry this approach and details to exhume product configurations that provide evidence for use in formal audits. It is important to reiterate that although VMware Cloud Foundation for the Software-Defined Data Center provides some capabilities to meet the top 10 regulatory compliance standards, it does not carry responsibility for certifying compliance.

By performing detailed reviews at multiple stages of the implementation process, you will find yourself well positioned to align your program with the top 10 regulatory standards. No two organizations, industries, or frameworks are identical. Different needs, deployments, and configuration possibilities mean that there is no "one-size-fits-all" approach to securing or auditing an environment. This audit guide should be leveraged in addition to your internal Governance, Risk Management, and Compliance (GRC) program rather than substituted for it.

Internal reviews should follow a similar pattern to what is shown in the following figure:

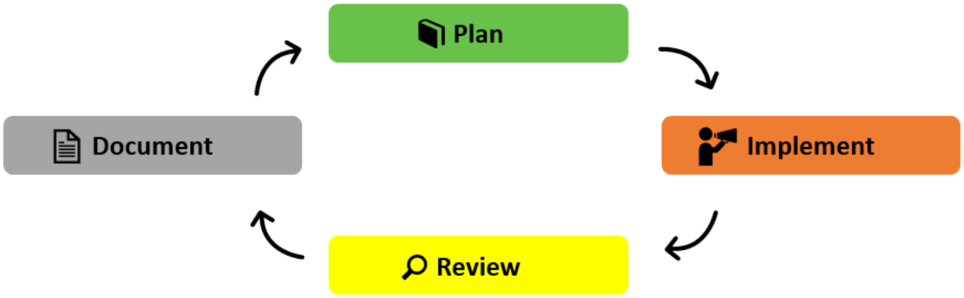

Figure 1 - Internal Review Process

Anyone using this audit guide should make sure that they conduct regular internal reviews and understand internal requirements outlined by their organization as well as the requirements of outside assessors. You should also be aware of any specific details relating to software deployments and the regulatory compliance needs of their organization. This guide should be leveraged throughout the implementation process, and then again post deployment to foster continuous alignment with the top 10 regulatory compliance standards.

Because no two environments or organizations are the same, this audit guide should be used in a manner that is sensitive to the distinction between controls that have been categorized as “non-default” or “default”. These labels denote distinct meanings that should be considered during the audit process. A “default” configuration is a configuration that is present during the initial deployment and was designed into the product. A “non-default” configuration is actively configured to a specific value, based on the organization’s determination. This may include controls that are People and Process oriented or have integration with other technology besides just VMware Cloud Foundation products. Consequently, an auditor must take great care to ensure that the control type is adequately considered when phrasing discovery questions during the configuration assessment procedure.

Top 10 Regulations

NIST 800-53 R4 (Moderate)

The National Institute of Standards and Technology Special Publication 800-53 Revision 4 (NIST SP 800-53 Rev. 4) is a catalog of security and privacy controls used for all U.S. federal information systems except those related to national security. It is published by the National Institute of Standards and Technology, which is a non-regulatory agency of the United States Department of Commerce. NIST SP 800-53 is broken down into 18 control families as follows:

- Access Control
- Audit and Accountability
- Awareness and Training
- Configuration Management
- Contingency Planning
- Identification and Authentication
- Incident Response
- Maintenance
- Media Protection
- Personnel Security
- Physical and Environmental Protection
- Planning
- Program Management
- Risk Assessment
- Security Assessment and Authorization
- System and Communications Protection
- System and Information Integrity
- System and Services Acquisition

NIST SP 800-53 works in conjunction with other NIST publications, risk management frameworks, and security frameworks to set guidelines and baselines for system security. It is a robust and well-accepted standard. This standard can also be interpreted for a High or Low risk ratings with minimal mapping because NIST control families are consistent across High/Moderate/Low. Non-default controls could vary and within the NIST family and specific control, enhancement controls can be further explored by an organization.

PCI DSS 3.2.1

The Payment Card Industry Data Security Standard (PCI DSS) is an information security standard for organizations that handle branded credit cards from the major credit card brands. The standard was created to increase security around cardholder data and protect consumers. This standard applies to any organization that stores, processes, or handles cardholder data.

Cardholder data can consist of several items, including:

- Primary Account Number (PAN)
- Name of the cardholder
- The Card’s expiration date
- The Card’s service code

An individual business interaction with cardholder data will vary depending on their defined operations. This underscores that there is no one-size fits all recommendation to secure a cardholder data environment (CDE). The responsibility resides with the individual business to ensure they appropriately assess what requirements fit their environment to adequately protect cardholder data along PCI DSS standards.

Validation of compliance should be performed annually, either by an external Qualified Security Assessor (QSA) that creates a Report on Compliance (ROC) for organizations handling large volumes of transactions, or by Self-Assessment Questionnaire (SAQ) for companies handling smaller volumes.

As with many security standards, PCI DSS takes a variety of its intentions from NIST 800-53 as guidance for defense in depth security within the cardholder environment. The PCI DSS standard requires organizations to comply with a robust set of requirements. The criteria are broken down into 6 objective areas and 12 requirements (listed below). Each requirement has a set of controls, the necessary testing procedures to ensure that they are implemented appropriately with expert guidance.

- Build and Maintain a Secure Network and Systems
    - Requirement 1: Install and maintain a firewall configuration to protect cardholder data
    - Requirement 2: Do not use vendor-supplied defaults for system passwords and other security parameters
- Protect Cardholder Data
    - Requirement 3: Protect stored cardholder data
    - Requirement 4: Encrypt transmission of cardholder data across open, public networks
- Maintain a Vulnerability Management Program
    - Requirement 5: Protect all systems against malware and regularly update anti-virus software or programs
    - Requirement 6: Develop and maintain secure systems and applications
- Implement Strong Access Control Measures
    - Requirement 7: Restrict access to cardholder data by business need to know
    - Requirement 8: Identify and authenticate access to system components
    - Requirement 9: Restrict physical access to cardholder data
- Regularly Monitor and Test Networks
    - Requirement 10: Track and monitor all access to network resources and cardholder data
    - Requirement 11: Regularly test security systems and processes.
- Maintain an Information Security Policy
    - Requirement 12: Maintain a policy that addresses information security for all personnel.

The scope of the PCI environment varies from organization to organization. VMware products help enforce controls configured by each client based on their individual environment. Organizations need to define the scope of their cardholder environment and controls.

SOC 2

The Service Organization Control (SOC) 2 is a set of compliance requirements and auditing processes, specifically for third-party service providers, that aims at data security and client privacy. SOC 2 reports are tailored specifically to an organization's environment; however, SOC 2 defines criteria for managing client data based on five "trust service principles" including security, availability, processing integrity, confidentiality, and privacy. In total, there are 43 controls included within the framework.

FedRAMP

The Federal Risk and Authorization Management Program (FedRAMP) is a U.S. government program which aims to provide a standardized framework for security assessment protocols, authorization management processes, and continuous monitoring strategies for cloud products and services utilized by the federal government.

The governing bodies of FedRAMP include the Office of Management and Budget (OMB), US General Services Administration (GSA), US Department of Homeland Security (DHS), US Department of Defense (DoD), National Institutes of Standards & Technology (NIST), and the Federal Chief Information Officers (CIO) Council. The Office of Management and Budget requires any cloud service operators which hold or process federal data to be fully compliant with FedRAMP security standards.
FedRAMP is divided into 17 distinct control areas which vary in stringency based on the characteristics of the information system in question. These control areas are:

1. Access Control
2. Audit and Accountability
3. Awareness and Training
4. Configuration Management
5. Contingency Planning
6. Identification and Authentication
7. Incident Response
8. Maintenance
9. Media Protection
10. Personnel Security
11. Physical and Environmental Protection
12. Planning
13. Risk Assessment
14. Security Assessment and Authorization
15. System and Communications Protection
16. System and Information Integrity
17. System and Services Acquisition

HIPAA

The Health Insurance Portability and Accountability Act of 1996 (HIPAA) is a U.S. federal law which focuses on establishing national standards for the protection of patient health information from being disclosed without consent or knowledge of the patient. HIPAA features two recognized sub-standards issued by the U.S. Department of Health and Human Services (HHS) known as the Privacy Rule and the Security Rule.

- The Privacy Rule (Standards for Privacy of Individually Identifiable Health Information) establishes national standards for the protection of specific health information.
- The Security Rule (Security Standards for the Protection of Electronic Protected Health Information) establishes a national set of security standards for protecting certain health information that is held or transferred in electronic form.

FBI CJIS

The Federal Bureau of Investigation Criminal Justice Information Services (FBI CJIS) is a sub-division of the U.S. FBI that focuses on data privacy and regulation as it relates to law enforcement and criminal justice. The FBI CJIS Security Policy defines controls to protect the lifecycle of Criminal Justice Information (CJI) and guidance on the creation, viewing, modification, transmission, dissemination, storage, and destruction of CJI. The Security Policy outlines roles and responsibilities for involved parties, sets requirements on CJI and Personally Identifiable Information (PII), and contains thirteen policy areas. The policy also contains a series of appendices, one of which contains 8 best practices including virtualization. The policy areas are defined as follows:

1. Information Exchange
2. Security Awareness Training
3. Incident Response
4. Auditing and Accountability
5. Access Control
6. Identification and Authentication
7. Configuration Management
8. Media Protection
9. Physical Protection
10. System and Communications Protection and Information Integrity
11. Formal Audits
12. Personnel Security
13. Mobile Devices

DISA STIG

The Defense Information Systems Agency Security Technical Implementation Guide (DISA STIG) is a technical testing and hardening framework released by the U.S. Department of Defense (DoD). The DoD releases a variety of STIGs to address different devices, operating systems, and software. To-date, the

DoD has published more than thirty STIGs for VMware products including six STIGs for vSphere. Each DISA STIG includes individual product components that make up the technology.

NERC CIP

The North American Electric Reliability Corporation (NERC) Critical Infrastructure Protection (CIP) is a set of requirements designed to secure the assets required for operating North America's bulk electric system. The intent of the standards is to require utilities to establish a baseline set of security measures. NERC developed the standards using a results-based approach, focusing on performance, risk management, and entity capabilities. The current standards that are subject to enforcement are as follows:

- CIP-002-5.1a: Cyber Security – BES Cyber System Categorization
- CIP-003-8: Cyber Security – Security Management Controls
- CIP-004-6: Cyber Security – Personnel & Training
- CIP-005-6: Cyber Security – Electronic Security Perimeter(s)
- CIP-006-6: Cyber Security – Physical Security of BES Cyber Systems
- CIP-007-6: Cyber Security – System Security Management
- CIP-008-5: Cyber Security – Incident Reporting and Response Planning
- CIP-009-6: Cyber Security – Recovery Plans for BES Cyber Systems
- CIP-010-3: Cyber Security – Configuration Change Management and Vulnerability Assessments
- CIP-011-2: Cyber Security – Information Protection
- CIP-013-1: Cyber Security - Supply Chain Risk Management
- CIP-014-2: Physical Security

NIST 800-171

The National Institute of Standards and Technology Special Publication 800-171 Revision 2 (NIST SP 800-171 Rev. 2) is a framework for "Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations". NIST 800-171 works in conjunction with NIST SP 800-53 and is designed in a similar format. The requirements apply to all components of nonfederal systems and organizations that process, store, and/or transmit CUI, or that provide protection for such components. The security requirements are intended for use by federal agencies in contractual vehicles or other agreements established between those agencies and nonfederal organizations. NIST SP 800-171 is broken down into 11 control families as follows:

- Access Control
- Audit and Accountability
- Awareness and Training
- Configuration Management
- Identification and Authentication
- Maintenance
- Media Protection

- Personnel Security
- Physical and Environmental Protection
- System and Communications Protection
- System and Information Integrity

CMMC

The Cybersecurity Maturity Model Certification (CMMC) is a new cybersecurity framework with five maturity levels that range from "Basic Cybersecurity Hygiene" to "Advanced/Progressive." CMMC was designed to reduce data and intellectual property theft due to the loss of Federal contract information (FCI) or controlled unclassified information (CUI). This regulation creates a process to verify that DoD contractors have sufficient controls to safeguard sensitive data. Created by the Office of the Under Secretary of Defense for Acquisition and Sustainment (OUSD(A&S)), CMMC requires contractors and subcontractors to hire an independent third-party organization (C3PAO) to conduct an assessment and report on compliance rather than producing a self-attestation. All new DoD contract requests for proposal (RFPs) and requests for information (RFIs) will include the appropriate CMMC Level requirement. Companies that are not CMMC compliant will be automatically disqualified from new contract opportunities.

The current policy, DFARS Clause 252.204-7012, requires the contractor or subcontractor to:

- Provide adequate security to safeguard covered defense information that resides on or is transiting through a contractor's internal information system or network.
- Report cyber incidents that affect a covered contractor information system or the covered defense information residing therein, or that affect the contractor's ability to perform requirements designated as operationally critical support.
- Submit malicious software discovered and isolated in connection with a reported cyber-incident to the DoD Cyber Crime Center
- Submit media/information as requested to support damage assessment activities.
- Flow down the clause in subcontracts for operationally critical support, or for which subcontract performance will involve covered defense information.

GDPR

The General Data Protection Regulation 2016/697 is a regulation in EU law on data protection and privacy in the European Union and the European Economic Area. It also addresses the transfer of personal data outside the EU and EEA areas. GDPR, which contains eleven chapters, aims at standardizing data privacy laws across Europe. The chapters are as follows:

- Chapter 1 (Art. 1–4) General provisions
- Chapter 2 (Art. 5–11) Principles
- Chapter 3 (Art. 12–23) Rights of the data subject
- Chapter 4 (Art. 24–43) Controller and processor

- Chapter 5 (Art. 44–50) Transfers of personal data to third countries or international organizations
- Chapter 6 (Art. 51–59) Independent supervisory authorities
- Chapter 7 (Art. 60–76) Cooperation and consistency
- Chapter 8 (Art. 77–84) Remedies, liability, and penalties
- Chapter 9 (Art. 85–91) Provisions relating to specific processing situations
- Chapter 10 (Art. 92–93) Delegated acts and implementing acts
- Chapter 11 (Art. 94–99) Final provisions

ISO 27001:2013

The ISO/IEC 27001:2013 standard, published by the International Organization for Standardization, is a framework that details specifications for an information security management system (ISMS). The standard is split into two primary portions: Clauses and Controls. The 10 clauses are as follows:

1. Scope of the standard
2. How the document is referenced
3. Reuse of the terms and definitions in ISO/IEC 27000
4. Organizational context and stakeholders
5. Information security leadership and high-level support for policy
6. Planning an information security management system; risk assessment; risk treatment
7. Supporting an information security management system
8. Making an information security management system operational
9. Reviewing the system's performance
10. Corrective action

Annex A outlines a list of controls and any related objectives. There are 114 controls in 14 groups and 35 control categories in the 2013 version of the standard. The controls are as follows:

- A.5: Information security policies (2 controls)
- A.6: Organization of information security (7 controls)
- A.7: Human resource security - 6 controls that are applied before, during, or after employment
- A.8: Asset management (10 controls)
- A.9: Access control (14 controls)
- A.10: Cryptography (2 controls)
- A.11: Physical and environmental security (15 controls)
- A.12: Operations security (14 controls)
- A.13: Communications security (7 controls)
- A.14: System acquisition, development and maintenance (13 controls)
- A.15: Supplier relationships (5 controls)
- A.16: Information security incident management (7 controls)
- A.17: Information security aspects of business continuity management (4 controls)

- A.18: Compliance; with internal requirements, such as policies, and with external requirements, such as laws (8 controls)

Approach to Auditing the SDDC

Understanding the SDDC Architecture

To complete an audit evaluation of the SDDC, it is imperative that you understand the architecture used to develop VMware Cloud Foundation and the Compliance Kit for the top ten compliance frameworks. The kit uses a verifiable blueprint and model of security that supports these compliance frameworks. The SDDC is software based, which benefits from a level of abstraction that can be configured with granularity and precision without sacrificing operational efficiency.

Key Characteristics of Virtualized Environments

To better understand how to audit an SDDC, it is important to know how virtualized environments differ from a traditional environment. Technical cornerstones such as servers, firewalls, and even storage arrays, while possessing features analogous to their traditional counterparts, have several differences within the virtualized environment. Before diving into specific differences, understanding the fundamental architecture of a virtualized environment is important:

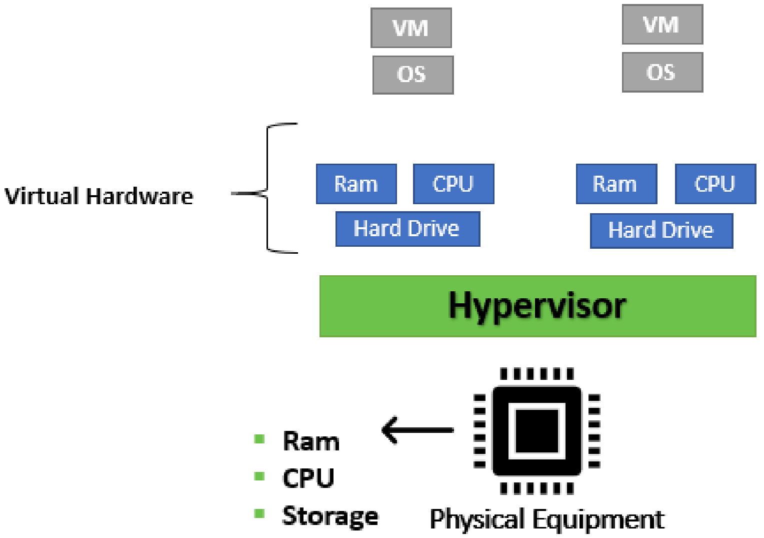

Figure 2: Breakdown of a Virtual Environment

Virtualization was a technological breakthrough that allowed more flexible allocation of physical computational resources, removing constraints on the number of systems and functions a piece of physical hardware may support. At the building block of any virtual environment, there is a physical server that is operating what is known as a “hypervisor.” A hypervisor is simply the software that interacts with the physical hardware, either directly as firmware or indirectly via a standard operating system (OS), to create and manage virtual machines (VMs). These machines can be workstations, servers, backup devices, or anything else you might require. Each VM is assigned memory and storage partitioned from hardware resources, which allow for specific OS, applications, or other tools to operate. Hypervisors are designed to isolate computing resources by default so that VMs on the same hypervisor are unable to share resources, such as memory or storage, unless explicitly configured otherwise.

Cloud infrastructure providers use virtualization to allow flexible and on-demand allocation of computing resources, with all customer systems hosted as VMs within the cloud environment. Regardless of the typic of cloud offering, from privately hosted enterprise cloud environments, to Amazon Web Services and Azure public cloud offerings, or whether the cloud offering is IaaS, PaaS, or SaaS, these fundamental building blocks of virtualization remain ubiquitous in cloud computing.

With enough physical resources, namely RAM and disk space, there is effectively no limit to what you can host with a single physical server. Today, all critical components of IT infrastructure have available some degree of a virtual counterpart. From firewalls to switches to long-term storage devices, there is very little that can be achieved with a physical infrastructure that cannot be emulated by a virtual environment.

In practically every scenario, virtual counterparts are both cheaper and easier to deploy than physical alternatives. The following is a breakdown of key differences between a few common technological components and their virtual counterparts:

Inventory of Systems

The hypervisor and lifecycle management tools allow for automation and close monitoring of system components (Virtual Machines, Virtual Appliances, Management Components, et cetera). Additional integration into management components across the SDDC Manager can help in collapsing the compute, network, and storage layers.

Easily tracking all components which are interacting within a system enables increased efficiency, security, and ease-of-use throughout inventory management processes. Without the simple inventory solutions provided by these virtualized systems, a vast inventory of components must be manually managed using systems that can be costly and inefficient.

Virtual Machine Instances

With virtualization, the number of operating systems is no longer restrained to the 1:1 ratio between system and central processing unit (CPU). On a hypervisor, many VMs instances, such as servers or virtual appliances, may be hosted and simultaneously running on a single physical CPU. This consequently increases the efficiency of managing such programs, removing the requirement for physical interaction when deploying or decommissioning program instances.

VMs may not only be used to host standard operating system instances but may also run specialized software akin to physical appliances. These VMs may include dedicated systems such as firewalls, intrusion detection systems, security incident and event management systems, and virtual hardware security modules.

In contrast to traditional physical machines, you can easily provision or deprovision VMs with any type of operating system you need, usually within minutes. This applies to additional storage or raw compute power as well, making tasks such as long-term data storage or load balancing simple. Secure configuration management of these machines is also simplified because after a securely configured virtual image is developed, processes for building systems based on this image can be automatic.

Virtual Networking

Traditional data center environments deploy physical network appliances to manage connectivity of systems and services across the environment. As organizations transition towards virtualization, the initial stage of this transition typically manifests itself as a hybrid deployment comprised of virtual servers with connectivity managed via traditional firewall, router, and switch appliances. Fully fledged SDDC environments adopt virtual technologies that replicate firewalls, switches, and in some cases routers, that may be managed through a single integrated solution, such as VMware NSX-T Data Center, which supports cloud-native applications, bare metal workloads, multi-hypervisor environments, public clouds, and multiple clouds.

Components of the VMware Cloud Foundation for the SDDC

VMware Cloud Foundation is a comprehensive software-defined data center stack, which consists of eight key components:

- VMware SDDC Manager
- VMware Cloud Foundation
- VMware Cloud Builder (initial SDDC deployment tool only)
- VMware vSphere
- VMware vSAN
- VMware Tanzu
- VMware NSX-T Data Center
- VMware vRealize Suite

With multiple key areas of virtualization conglomerated into a singular stack, efficiency can be greatly improved, and risk can be decreased. The VMware Cloud Foundation provides a unified automation suite of products for the SDDC that help to address agility, reliability, and efficiency in public and private cloud environments. This ubiquitous hybrid cloud platform provides extensive functionality to meet all security and compliance needs of an organization. At the software and architectural levels, the consistency provided in VMware Cloud Foundation stands as the backbone for virtualization best practices in a digital marketplace.

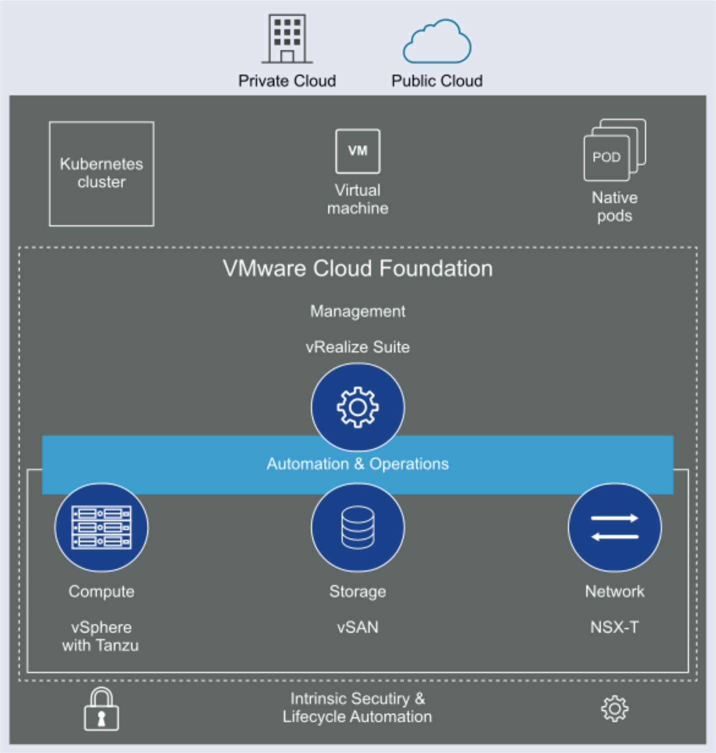

Figure 3: VMware Depiction of VMware Cloud Foundation Deployment

The VMware Cloud Foundation stack is brought up by and relies heavily on SDDC Manager. SDDC Manager creates and manages workload domains and performs lifecycle management so that software components remain up-to date. It also monitors the logical and physical resources of VMware Cloud Foundation systems, enabling administrators to easily modify their resources via a singular interface and system. Additionally, SDDC Manager tracks VMware Cloud Foundation systems to identify points-of-failure within their processes, providing precise information which helps to streamline the restoration and remediation of system processes. SDDC Manager includes security functionality for Access Control, rotation of passwords across core products, and assist in key management.

Understanding Inherent Risks Commonly Affecting the SDDC

Transformation of Risk Landscape

While virtual environments provide numerous benefits and cost savings, this does not mean that they are overall less risky than a traditional environment. Instead, the inherent risks simply shift due to the changes in threat and vulnerability surface. For instance, if a public cloud provider such as Amazon Web Services is being used, some areas such as physical security and hardware maintenance become less of concerns, while other areas such as access management and information disclosure become more critical. Predominantly, virtualization will impact how users and administrators interact with the machines they use. Auditing virtual environments brings new challenges because visibility into the infrastructure is covered with additional layers of abstraction and new ways to interact with systems, consequently requiring additional understanding of and trust in particular vendor solutions.

If the SDDC is operating within a public cloud environment, the differences are even more significant, as these providers usually operate on a multi-tenant model. In a multi-tenant model, physical equipment that is shared by VMs, communication infrastructure, routers, or any other virtual technology must then also be further segmented by individual tenants. This increases the requirement for coordination and dependency between organizations by which a shared responsibility model must be negotiated. Multitenancy also increases many other risk variables, such as overall assets potentially compromised and increased incentive for adversarial hackers to target the shared infrastructure.

The following are risks commonly affecting SDDC environments and considering these risks will support your ability to accurately evaluate the effectiveness of SDDC technical controls.

Configuration Risk

SDDC products provide an additional layer of abstraction, which reduces the extent to which control aspects require interaction with physical hardware. With this improved capability to control the environment purely through remote management interfaces comes the consequence of greater exposure to misconfigurations. For instance, with simply one or two clicks an administrator may be able to expose a customer database to the internet, an action that would previously require coordination between interdepartmental administrators in many traditional environments. If you operate in a highly regulated industry or are processing personal information (i.e., subject to GDPR or CCPA), this risk can have major significance. The likelihood of such misconfigurations is determined by both the administrators' knowledge of secure configuration parameters and user interface design decisions made by the SDDC product vendor to minimize insecure configuration.

The VMware Cloud Foundation Compliance Kit was developed in accordance with select best practices and designed to achieve both IT agility and risk mitigation. The VMware Cloud Foundation, Compliance Kit includes known issues, installation guidelines, software component lifecycles, as well as many other relevant implementation insights that will help minimize risks related to misconfigurations.

Software-Vulnerability Risk

Virtualization, as with any new technology, has also introduced new, exploitable vulnerabilities specific to the software adopted. Many of these vulnerabilities relate to flaws in the hypervisor's enforcement of isolation between VMs. For example, we have seen a rise in so-called "side-channel" attacks in recent years, which have taken on many forms. A common side-channel attack leverages the shared cache memory between VMs to obtain sensitive data such as encryption keys without compromising the host system. Just as with any common device or systems within traditional physical environments, patch management processes appropriate to the technology must be established.

VMware takes extensive steps to protect its offerings from security flaws and other vulnerability risks. Internal security programs and best practices operate "secure by design" to evolve methodologies of protection against new threats as they are discovered. This approach is followed throughout the development process. VMware products are subject to intensive vulnerability assessments and penetration tests prior to any full release or version update.

Architectural Risk

Within virtual environments, east–west traffic describes the traffic within a data center such as server-to-server traffic. North–south traffic describes the traffic between a client and a server, which is the traffic between the data center and the network outside of the data center. In an SDDC, east–west traffic may grow exponentially because many traditional constraints are not present. A single server can host dozens to hundreds of VMs that can all be communicating with each other. Further, systems and services are built and decommissioned at unprecedented speeds due to the management convenience virtualization provides.

Security architectural best-practices in traditional environments require a shift in form when applying the same principles to an SDDC environment. Patterns of connectivity become much more dynamic and increasingly difficult to track and control when provided powerful tools designed for IT agility and scalability. Approaches for architectural design must now follow a much more systematic and algorithmic approach to accommodate rapid scalability and automation.

VMware has created the VMware Cloud Foundation, Compliance Kit to provide an architectural blueprint that incorporates fundamental security architecture principles into practices appropriate for the VMware SDDC products. Leveraging VMware Cloud Foundation helps you implement a well-architected environment, decrease the risk of configuration errors, and provide mechanisms for continuous auditing of the environment.

Designing Control Testing Methods in an SDDC

In comparison with a traditional physical environment, auditing a virtualized environment introduces both visibility constraints and management interfaces that must be considered, consequently resulting in the need for new methods. This section will highlight some key considerations and provide guidance on how to approach designing your technical control testing methods.

People, Process, and Technology Controls

VMware Cloud Foundation, Compliance Kit for the top 10 regulatory standards provides a technology solution to customers that, though it may support key people, process, and technology controls, does not provide guidance on process or people elements around IT security and operational management of the system. The VMware Cloud Foundation, Compliance Kit primarily provides a methodology from which to assess an environment in relation to the technology controls within the top 10 regulatory standards.

Identify Control Dependencies on SDDC

An organization’s security and compliance requirements should carefully identify scope, define the boundaries, to prepare with their preferred regulatory standard(s). Based on the defined statement of scope, the systems and business processes that are reliant upon SDDC infrastructure and solutions can be determined.

You should identify both the SDDC elements supporting the underlying infrastructure and the tools which are used to fulfill each security control requirement. Identification of these components helps to provide a fundamental understanding the architecture being assessed and helps the process of designing an appropriate plan for technical control testing. For instance, the assessor must understand whether traditional network appliances are used, if an integrated software-defined networking solution, e.g., VMware NSX-T is employed, or if a combination of both must be assessed.

An overview of VMware SDDC products available to support the top 10 regulatory frameworks and their control objectives can be found in the “In-Scope VMware Product List” section of this guide.

Management Planes

Management planes which are used to manage the SDDC products that are in scope must be identified. In comparison to a traditional environment, an SDDC may have a distinct combination of both additions and removals to different management planes.

For instance, an SDDC may maintain server access via RDP and SSH, while adding a hypervisor management interface such as vSphere. Another SDDC environment may restrict RDP and limit SSH access from servers, and purely rely on management planes controlling hypervisors and deployment pipelines, or only allowing these communication protocols for specific times when administration of the system is performed.

Understanding the management planes available and exploring the functionality available on each management plane is necessary to differentiate what security parameters are configurable versus the security mechanisms that are hard coded into the product.

Configurable Security Parameters

Understanding what functionality and parameters are configurable by the end-user is necessary to identify what security controls the SDDC user is responsible for maintaining. Because interfaces and functionality will be unique to each vendor product, documentation maintained by both the vendor and the assessed entity must be relied upon to determine what is configurable, and what the respective security best-practice recommendations are. Only through this can you evaluate whether SDDC systems are configured with appropriate levels of security commensurate to the organization’s security policies.

VMware provides the Cloud Foundation, Compliance Kit, which includes this document and many other supplementary documents that detail guidance for implementing security best-practices into the VMware’s SDDC products.

In-Scope VMware Product List

This section lists VMware SDDC products that may be used to support compliance with the top 10 regulatory standards. This list represents the authors' evaluation of product applicability and may not be collectively exhaustive.

VMware vSphere is a server virtualization platform and product suite that delivers essential services for the modern hybrid cloud.

VMware ESXi™, the industry-leading virtualization platform, provides a powerful, flexible, and secure foundation for business agility that accelerates the digital transformation to cloud computing and success in the digital economy.

VMware vCenter® Server provides centralized management of vSphere virtual infrastructure. IT administrators can provide security and availability, simplify day-to-day tasks, and reduce the complexity of managing virtual infrastructure.

VMware vSAN™ is a core building block for the Software-Defined Data Center, delivering enterprise-class, flash-optimized, and secure storage for all of a user's critical vSphere workloads.

VMware vSphere Replication is a hypervisor-based, asynchronous replication solution for vSphere virtual machines. It is fully integrated with VMware vCenter Server and the vSphere Web Client. vSphere Replication delivers flexible, reliable and cost-efficient replication to enable data protection and disaster recovery for all virtual machines in your environment.

VMware NSX-T Data Center provides an agile software-defined infrastructure to build cloud-native application environments and is focused on providing networking, security, automation, and operational simplicity for emerging application frameworks and architectures that have heterogeneous endpoint environments and technology stacks.

Out-of-Scope VMware Product List

While the products below may not be directly referenced within the VMware Cloud Foundation Compliance Kit, their security guidance and security figures may be relevant to the objectives referenced within this Compliance Kit. At this time, the following products are not integrated within the VMware Cloud Foundation Compliance Kit.

VMware vRealize Operations delivers self-driving IT operations management from apps to infrastructure to optimize, plan and scale SDDC and VMware Cloud deployments with visibility into multiple public clouds.

VMware vRealize Orchestrator is a drag-and-drop workflow software that simplifies the automation of complex IT tasks and integrates with vRealize Suite and vCloud Suite to further improve service delivery efficiency, operational management and IT agility.

VMware vRealize Log Insight delivers highly scalable log management with intuitive, actionable dashboards, sophisticated analytics and broad third-party extensibility. It provides deep operational visibility and faster troubleshooting across physical, virtual and cloud environments.

VMware vRealize Network Insight helps you build an optimized, highly available and secure network infrastructure across hybrid and multi-cloud environments. It provides network visibility and analytics to accelerate micro-segmentation security, minimize risk during application migration, optimize network performance and confidently manage and scale NSX, SD-WAN Velocloud, and Kubernetes deployments.

VMware vRealize Automation is a modern infrastructure automation platform that enables self-service multicloud environments. With vRealize Automation, customers can increase agility, productivity and efficiency through self-service automation, by reducing the complexity of their IT environment, streamlining IT processes and delivering a DevOps-ready automation platform.

VMware Workspace ONE Access, (formerly VMware Identity Manager), provides multi-factor authentication, conditional access and single sign-on to SaaS, web and native mobile apps.

VMware Site Recovery Manager is an industry-leading disaster recovery (DR) software that delivers automated orchestration of failover and fail-back to minimize downtime.

VMware Cloud Director is a leading cloud service-delivery platform used to operate and manage cloud-service businesses to support the delivery of secure, efficient, and elastic cloud resources.

VMware Cloud Director Availability™ is a Disaster Recovery-as-a-Service (DRaaS) solution that provides asynchronous replications, failover, and migration for vApps and for virtual machines.

VMware vCloud Director Extender is a hybrid cloud solution that enables cloud providers and tenants to expand multi-tier applications and perform workload migrations between on-premises data centers and the cloud.

VMware vCloud Availability solution provides replication and failover capabilities for vCloud Director and vCenter Server workloads at both VM and vApp level.

VMware vCloud Usage Meter is a virtual appliance that is installed on a vCenter Server instance that collects product consumption data and generates reports for products that are part of VMware Cloud Provider Program.

VMware User Environment Manager is a solution that IT professionals can use to configure and deploy employees' desktop computer settings.

VMware Cloud Foundation is the hybrid cloud platform for managing VMs and orchestrating containers, built on full stack hyperconverged infrastructure (HCI) technology.

VMware Cloud Provider Platform is a tested, validated, and scalable combination of VMware vSphere® and VMware NSX, along with VMware vCloud Director® and vCloud Usage Meter, that enables providers to rapidly implement VMware clouds wrapped with their own differentiated services.

VMware vSphere Virtual Machine Encryption is a feature that allows encryption of virtual machines to protect data-at-rest.

VMware Mirage is a solution for managing physical or virtual desktops and laptops, and for BYO users, combining centralized management for IT and local execution for end users.

VMware Horizon is a modern platform for secure delivery of virtual desktops and apps across the hybrid cloud, from the market leader in software-defined data center and digital workspaces.

VMware AppDefense improves the security of applications from within the hypervisor that analyzes workloads to model intended application behavior, monitor for anomalous activity, and provide application control, reputation scoring, and security.

About Tevora

Tevora is a leading management consulting firm specializing in enterprise risk, compliance, information security solutions, and threat research. We offer a comprehensive portfolio of information security solutions and services to clients in virtually all industries and also serve institutional and government clients.

Tevora's leaders are professionals with years of experience and records of accomplishments in technology as well as business. This dual background means that we understand the importance of growth and profitability and our solutions are designed to enhance both.

As a consulting firm that has the ability to fully implement whatever it recommends, Tevora works with all of the industry's top vendors, yet is beholden to none. We are completely vendor-independent and select best-of-breed products tailored exclusively to our clients' needs. Security is our only business and our single-minded focus on anticipating and solving client problems has been described as "obsessive." We consider this a fair assessment.

Our hard work and dedication has established us as a reliable partner CTOs CIOs, and CISOs can depend on to help protect against threats, both internal and external. With Tevora as a partner, business leaders can devote their energies to enhancing the overall value of information technology to their enterprise.

Tevora is also a DVBE (Disabled Veteran Business Enterprise) certified by the California General Services Department (Cert REF# 32786).

For more information please visit www.tevora.com.

TEVORA™

Go forward. We've got your back.

Compliance - Enterprise Risk Management - Incident Response
Data Privacy - Security Solutions - Threat Management