TEVORA

VMware® Validated Design Compliance Kit for NIST 800-53 Rev. 4 Audit Guide

June 11, 2019

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
June 2019	1.0	Tevora	Initial Draft	Carlos Phoenix

Design Subject Matter Experts

The following people provided key input into this whitepaper.

Name	Email Address	Role/Comments
Christina Whiting	cwhiting@tevora.com	Co-Author
Zachary Curley	zcurley@tevora.com	Co-Author
Carlos Phoenix	cphoenix1@vmware.com	Compliance and Cybersecurity SME, VMware

Trademarks and Other Intellectual Property Notices

VMware Validated Design for the Software-Defined Data Center

The VMware Validated Design (VVD) architecture strives to balance security and innovation without sacrificing one for the other. Together, this by-design approach assures customers that when they implement a VMware Validated Design for the Software-Defined Data Center (SDDC), they are getting a comprehensive software stack that not only supports their legislative and security needs but also meets 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 Validated Design Compliance Kit for NIST 800-53.

VMware Validated Design: Software-Defined Data Center Layer	Key Products
Physical Infrastructure	VMware ESXi™, VMware vSAN™
Virtual Infrastructure	VMware ESXi, VMware vCenter Server® Appliance™, VMware NSX® Data Center for VMware vSphere®, VMware vSAN, VMware vSphere Update Manager™, VMware Update Manager Download Service, VMware Cloud Builder
Operations Infrastructure	VMware vRealize® Operations Manager™, VMware vRealize Operations Manager Content Pack, VMware vCenter Lifecycle Manager, VMware vRealize Log Insight™, VMware vRealize Log Insight Content Pack™,
Cloud Management	VMware vRealize Automation™, VMware vRealize Business™ for Cloud, VMware vRealize Orchestrator™
	VMware Site Recovery Manager™, VMware vSphere Replication™

Disclaimer (Tevora)

The opinions stated in this audit guide concerning the applicability of VMware products to the NIST 800-53 framework 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. 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 technology across data centers is altering the audit landscape. Information technology auditors encounter VMware products without substantial technical guidance from regulators and standards bodies. The pace of innovation has required auditors to develop their own best practices to assess virtualization technology. To address the need for technical guidance, VMware hired Tevora to compile this audit guide, which is divided into two areas—this document and technical procedures included as appendices within a separate file.

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 is publishing documentation as compliance kits to address both audiences. Each compliance kit is purpose built to a regulation, standard, or framework. The kit contains a configuration guide that supports the implementation of the VMware Validated Design, while the audit guide supports the auditing of the deployed solution.

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 Validated Design for the Software-Defined Data Center. The goal of this document is to ensure that all stakeholders feel confident that the configuration of their SDDC will align with the intent of NIST 800-53 R4.

A key detail for the reader 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 the security configurations and leverage VMware expertise to evaluate whether the SDDC is provisioned appropriately. Certifiable compliance is at the discretion of the organization and their designated parties.

How to Use This Audit Guide

The audit guide is constructed to be informative, comprehensive, and audit friendly. The authors not only are technologists but have also held positions responsible for IT compliance at various organizations. The guide assumes knowledge of the auditing process flow. Auditors can use this document to evaluate existing compliance requirements compared to the VMware Validated Design Compliance Kit for NIST 800-53, identify control requirements necessary to meet compliance, and test security configurations.

The audit guide appendices outline how the SDDC can address NIST 800-53 requirements across the high-impact level. Readers of the audit guide can gain an important tool to address regulatory needs and can apply the knowledge in gathering documentation to support security configurations often 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. Auditors should marry this approach and details to exhume product capabilities that provide evidence for use in formal audits. It is important to reiterate that although VMware Validated Design (VVD) for the Software-Defined Data Center provides some capabilities to meet NIST 800-53, it does not carry responsibility for certifying compliance.

By performing detailed reviews at multiple stages of your implementation process, you will find yourself well positioned to align your program with NIST 800-53. 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.

Anyone using this audit guide should ensure that they conduct regular internal reviews and understand internal requirements outlined by your organization and the requirements of outside auditors. They should also be aware of any specific details relating to their software deployments and their regulatory compliance needs. This guide should be leveraged throughout your implementation and then again post deployment to foster alignment to all in-scope NIST controls.

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

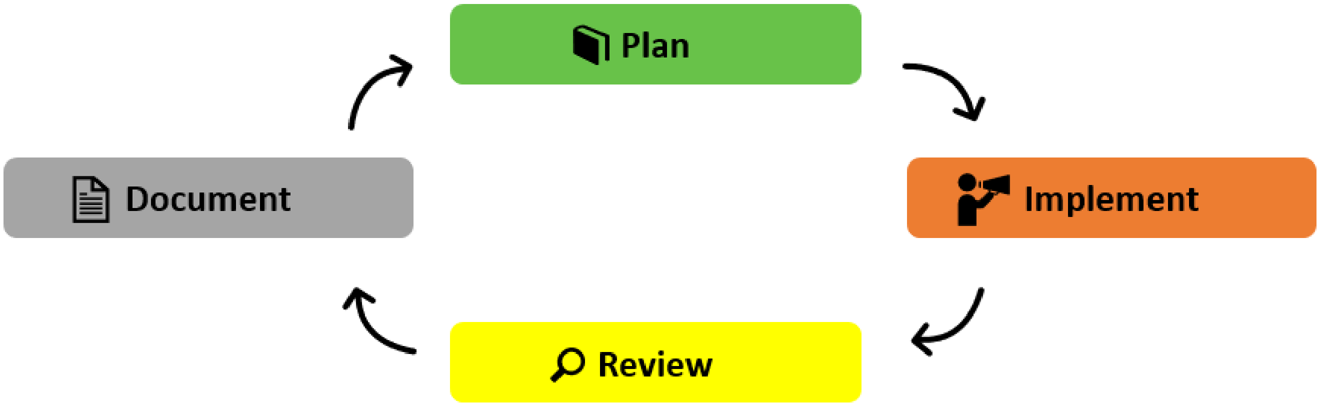

Figure 1: Internal Review Process

Tips for Auditing an SDDC

To complete an audit evaluation of the SDDC, it is imperative that you understand the architecture used to develop the VMware Validated Design Compliance Kit for NIST 800-53. The kit uses a verifiable blueprint and model of security that supports NIST 800-53. 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 a Virtual Environment

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

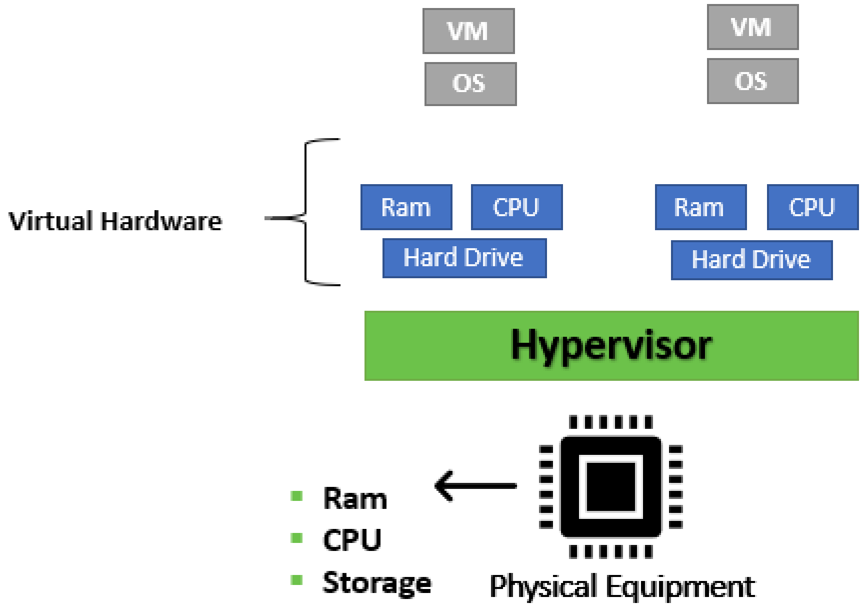

Figure 2: Breakdown of a Virtual Environment

At the core 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 leverages the physical hardware, either directly or 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 virtual device is assigned virtual resources, which are segments of the overall physical equipment, which allow for specific OS, applications, or other tools to operate. Functionality is determined by the cloud provider, whether that is a private cloud hosted internally or services provided by AWS or Azure, but the basic operations are similar.

With enough physical resources, namely RAM and disk space, there is no limit to what you can host with a single server. Today, all critical components of IT infrastructure have some level of 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 every scenario, virtual counterparts are both cheaper and easier to deploy, although not necessarily to configure, than physical alternatives. The following is a breakdown of key differences between a few common technological components and their virtual counterparts:

Virtual Machines and Servers

Unlike 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 incredibly simple. Securing these machines is easier as well because after a secure template is developed, you can leverage it across every other deployment of similar system down the line.

For all intents and purposes, a virtual server is a VM assigned to a specific task. It might run specialized software, akin to physical servers, or might simply be leveraged to manage a database or other dedicated service. These will likely have more resources allocated to them, but there is no checkbox that transforms a regular VM into a server or vice versa.

Virtual Networking

There are virtual technologies that can replicate switches, firewalls, and network segmentation as a whole. These components, along with other tools, allow for a data center to direct and reconfigure traffic flows to best suit their compliance and operational needs. We have provided a brief outline of the different options and some additional features provided by virtual networking technology in the following sections.

Firewalls

Virtual firewalls are a type of software that can be placed at various areas within the virtual network, such as between VLANs or individual VMs. The virtual firewall can prevent the transmission/transfer of data, or files, by either unauthorized users or malicious insiders. Virtual firewalls are significantly cheaper than their physical counterparts, although they handle less network throughput. These firewalls can also be centrally managed and can have standardized configurations applied immediately without need for direct user interaction.

Switches

Along with the standard features such as packet forwarding, virtual switches can provide significant additional benefits not present within a physical switch. The biggest difference is that virtual switches can ensure the security and configuration standards of VMs as they move between physical hosts, eliminating a key risk facet associated with virtual systems.

VLANs

Virtual technology allows for strict segmentation that is strict enough to comply with all relevant legislation or industry requirements outlined in frameworks such as PCI DSS and ISO without requiring separate physical sets of networking equipment. Segmenting entire departments, or individual workstations, is easy and effective with virtualization and allows for both greater security and additional network control. This can all be accomplished without requiring several different sets of physical equipment, cables, and overall maintenance.

Additional Benefits and Risks

While virtual environments provide numerous benefits and cost savings, this does not mean that they are any less risky than a physical setup would be. If a public cloud provider, such as Amazon, is being used, some areas such as physical security and hardware maintenance diminish as concerns, while other areas such as operating system selection or patch management become even more critical. Auditing virtual environments also brings new challenges, because direct access to the infrastructure in use by public cloud providers is not permitted.

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 grows exponentially because many physical limitations are not present. A single server can host dozens or hundreds of workstations, services, or other critical infrastructure components that can all be communicating with each other. Processes such as VM migration greatly increase the amount of communication that exists within an SDDC, as VMs are moved between physical hardware components within the provider’s environment. Accordingly, the opportunity for attackers or outsiders to obtain sensitive data is increased as well.

If the SDDC is operating within a public cloud environment, the differences are even more significant, as these providers operate on a co-tenant model. In a co-tenant model, physical equipment that is shared by VMs, communication infrastructure, routers, or any other virtual technology would then also be further segmented by individual tenants. This can create issues in managing specific devices and in patch management; however, these will be specific to each provider and each contract.

Virtual technology also produces a few specific technical risks that are unique to themselves. 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. This means that even if your system is secure and hardened, attackers can still access critical information.

The feature set within the SDDC allows you to configure by default or as otherwise stated, to ensure that these risks are either greatly reduced or never active within their environment. Some other common risks that persist across any type of virtual environment, regardless of scope and location, are outlined in the following sections.

Configuration Risk

Given that the VMware SDDC is entirely software based, the primary risk to this environment is from either software-specific vulnerabilities or from misconfigurations. Misconfigurations are one of the greatest threats associated with any environment, but they take greater precedence in a digital environment.

The VVD was developed with software versions that are implemented in accordance with select best practices that help achieve the stated design objectives. This solution is tested for interoperability and scalability. A key goal with this approach is to minimize misconfigurations—thus, the need for such a detailed blueprint. The VVD includes known issues, installation guidelines, software component lifecycles, as well as many other relevant implementation insights. If you operate in a highly regulated industry or are processing personal information (i.e., subject to PCI DSS or CCPA), this risk can have major significance.

Software-Vulnerability Risk

VMware takes extensive steps to ensure that their offerings are free from security flaws or exploits. Internal security programs and best practices operate “by design” to evolve methodologies of protection against new threats as they are discovered. This approach is followed throughout the development process. Products are also subject to intensive vulnerability scans and penetration tests prior to any full release or version update.

Architectural Risk

To help balance the threat posed by architectural misconfiguration or poor implementation, VMware created the Validated Design Compliance Kit for NIST 800-53. The VVD helps you implement a well-architected environment, decrease the risk of configuration errors, and provide procedures to audit your security configurations. Using the VVD as a foundational architecture component, the approach outlined in the configuration guide can enhance the deployment of virtual architecture components.

To address architectural risk, use the procedures included in the audit guide appendices. The processes crafted by VMware act as constant reverification of the configuration and implementation details necessary to secure an SDDC instance, while also meeting compliance needs for customers. Both built-in functionality and enhanced configurations are outlined in the appendices.

Components of the VVD for the SDDC

There are four key objectives of the VVD:

- Accelerate time to market
- Increase efficiency
- Improve IT agility
- De-risk deployments and operations

With key areas of virtualization designed to enhance efficiency and reduce risk at the software and architectural levels, the consistency provided in the VVD stands as the backbone for virtualization best practices in a digital marketplace.

VMware Validated Design provides a detailed overview of several foundational software components related to launching and operating an SDDC. The VVD also provides various use cases that can be used as templates to create an SDDC that addresses specific business concerns or compliance requirements.

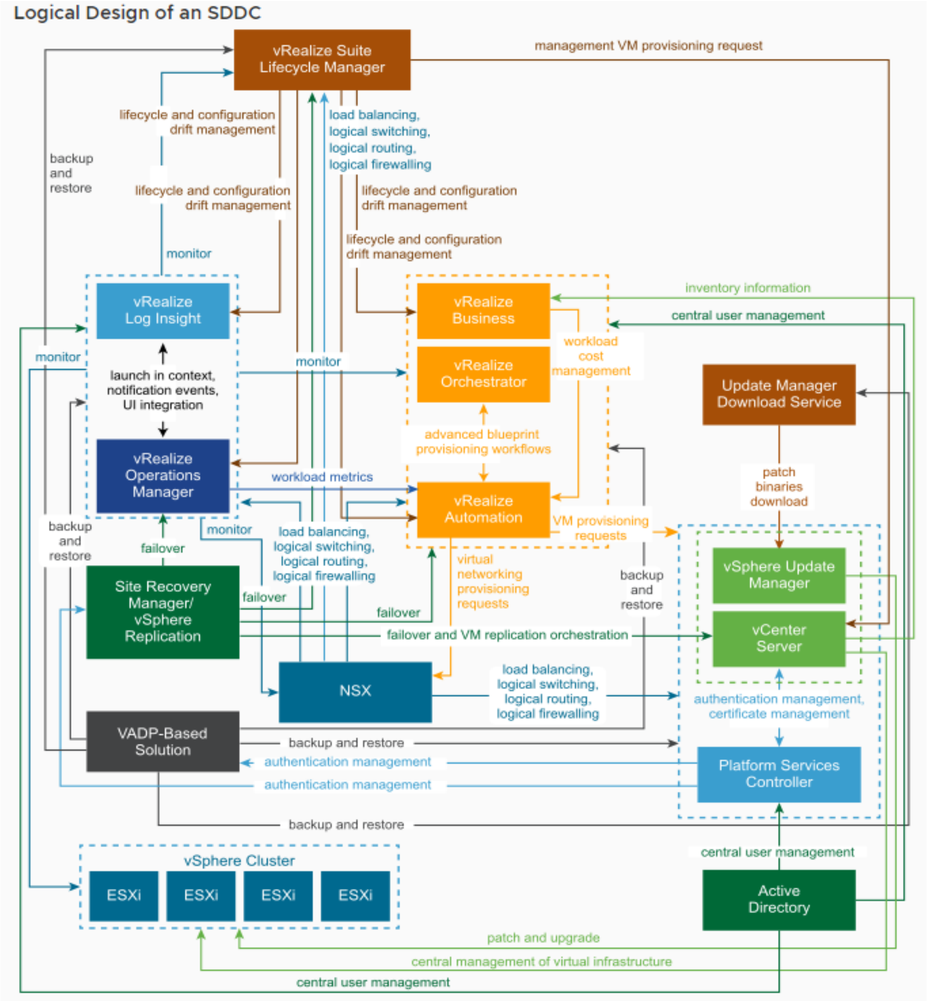
Logical Design of an SDDC
vRealize Suite Lifecycle Manager
management VM provisioning request
lifecycle and configuration drift management
load balancing, logical switching, logical routing, logical firewalling
backup and restore
lifecycle and configuration drift management
lifecycle and configuration drift management
lifecycle and configuration drift management
monitor
vRealize Log Insight
monitor
launch in context, notification events, UI integration
monitor
vRealize Operations Manager
workload metrics
vRealize Business
vRealize Orchestrator
workload cost management
advanced blueprint provisioning workflows
vRealize Automation
VM provisioning requests
inventory information
central user management
Update Manager Download Service
patch binaries download
backup and restore
failover
monitor
load balancing, logical switching, logical routing, logical firewalling
Site Recovery Manager/ vSphere Replication
failover
failover
virtual networking provisioning requests
backup and restore
vSphere Update Manager
vCenter Server
failover and VM replication orchestration
NSX
load balancing, logical switching, logical routing, logical firewalling
authentication management, certificate management
VADP-Based Solution
backup and restore
authentication management
authentication management
Platform Services Controller
backup and restore
vSphere Cluster
ESXi
ESXi
ESXi
ESXi
central user management
Active Directory
patch and upgrade
central management of virtual infrastructure
central user management

Figure 3: VVD Depiction of SDDC Deployment

SDDC – People, Process, and Technology

VMware Validated Design Compliance Kit for NIST 800-53 provides a technology solution to customers rather than the implementation of a NIST 800-53 compliance program. Thus, people and process components of this standard are not a major component of the kit. Features within the SDDC that enable organizations to enhance or craft a process based on compliance requirements can be classified as people or process controls.

As outlined in the NIST 800-53 Product Applicability Guide (PAG), not all technology controls defined by NIST are directly addressed by VMware technology. Some capabilities in the VVD might support people and process controls, which are identified as "administrative" in nature because they relate to internal operational practices and not to specific technology capabilities. Further details on these categories and the aligned NIST control families can be found in the PAG at **https://www.tevora.com/wp-content/uploads/2018/08/VMware-SDDC-and-EUC-Product-Applicability-Guide-for-NIST-800-53-Rev.4.pdf**.

SDDC – Scope Based on Core and Administrative Controls

The NIST 800-53 authority document historically established "Security Control Class Designation" in the form of management, operational, and technical references. To streamline the delivery of this audit guide and the intent of each control family, those categories were tailored into "core" and "administrative." Core control families are those that address the main structure of a NIST program through technical features and capabilities. Administrative control families support multiple control areas through policy development and general program, people, and process management tasks.

Administrative Controls

Many NIST control families establish policies and procedure requirements in the form of documentation, which might cite VMware products or rely on VMware technology capabilities. Other NIST controls might identify people or process requirements that are not specific to VMware products, but these too might rely on underlying VMware product capabilities. While VMware products do not map neatly to these controls, they support their fulfillment through alerts, scripting, monitoring, or other operations.

Your organization will be able to deploy VMware products, apply the configurations required to enable NIST 800-53 compliance requirements, and monitor them through VMware and other technology capabilities. In this way, implementing policy or operating procedures assists in maintaining a secure and compliant information architecture.

Core Controls

For those NIST control families where a technology will partially or fully satisfy a control requirement, VMware capabilities are identified as core to the NIST control family. These are the areas within NIST 800-53 that best highlight how each product provides capabilities to strengthen the security and support VMware and other technology capabilities.

Auditing a Virtualized Versus Traditional Environment

VMware Validated Design Compliance Kit for NIST 800-53 uses a Software-Defined Data Center, which is a virtual environment rather than a traditional physical environment for infrastructure. Auditing a virtual environment introduces some limitations to conduct an audit and raises the need for new methods. This section will highlight some of these methods and provide guidance on incorporating these methods into your existing Governance, Risk, and Compliance (GRC) strategy.

Audits focused on a virtual environment are conducted by conforming controls and software settings using command-line interface (CLI) or a graphic user interface (GUI). To facilitate this, the audit guide appendices outline procedures to test the configurations. These commands are needed for you to conduct an audit of both built-in and enhanced configurations related to deployed software components. The virtual nature of the evaluation provides the assessor with the opportunity to conduct many tests on the components, in most cases using commands that are outlined in the appendix.

The audit guide exists to assist with audits of virtual environments. This guide helps you confirm that your environments are configured to the specifications outlined in the compliance kit. The guide does not cover physical equipment, physical security, or hardware functionality. Take care that due diligence is shown when selecting or auditing these additional aspects, as any failure of physical security or hardware can impact your compliance with NIST requirements.

VMware integrates security throughout the phases of their product development and solution design. Responsibility also rests on customers to ensure that proper installation, configuration, and ongoing operations are performed. Access controls, physical or otherwise, are the sole responsibility of the customers, as are software-specific settings and configuration management. Addressing these last two items can be done either by applying provided software documentation and auditing guidelines or by engaging a third party.

In virtualized environments, risks posed by software errors and misconfigurations can pose a higher risk than in more standard environments. Configuration management is a top priority for any organization or audit, as this is where customers' responsibilities begin. Given the ease with which virtual environments can be created and copied, configuration drift is a serious risk that you must carefully manage.

Additional differentiation can be seen in the layout of a virtual network versus a physical network. With the VMware SDDC, the entire network infrastructure has been virtualized, from servers to firewalls to internal communication pathways. Auditors must take care to review every aspect of the environment and understand what the scope of the virtualized environment is for the organization they are auditing, to ensure that all areas receive appropriate reviews and tests.

In-Scope VMware Product List

Software-Defined Data Center (SDDC)

VMware vSphere®
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® provides centralized management of vSphere virtual infrastructure. IT administrators can ensure 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.

Virtualized Networking

VMware NSX® is the network virtualization and security platform for the Software-Defined Data Center, delivering the operational model of a virtual machine for entire networks. With NSX, network functions including switching, routing, and firewalling are embedded in the hypervisor and distributed across the environment.

About VMware

VMware, a global leader in cloud infrastructure and business mobility, accelerates our customers' digital transformation journey by enabling enterprises to master a software-defined approach to business and IT.

With the VMware Cross-Cloud Architecture™ and digital workspace solutions, organizations are creating exceptional experiences by mobilizing everything; differentiating and responding faster to opportunities with modern apps hosted across hybrid clouds; and safeguarding brand and customer trust with a defense-in-depth approach to security.

The VMware Cross-Cloud Architecture extends the company's hybrid cloud strategy with new public and private cloud capabilities that enable enterprises to run, manage, connect, and secure their applications across clouds and devices in a common operating environment. As the world's most complete and capable hybrid cloud architecture, the VMware Cross-Cloud Architecture enables consistent deployment models, security policies, visibility, and governance for all applications, running on premises and off, regardless of the underlying cloud or hypervisor.

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 a Qualified Security Assessor (QSA) and Payment Application Qualified Security Assessor (PA-QSA) in good standing with the PCI Security Standards Council. 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 – Data Privacy – Security Solutions – Threat Management