TEVORA™

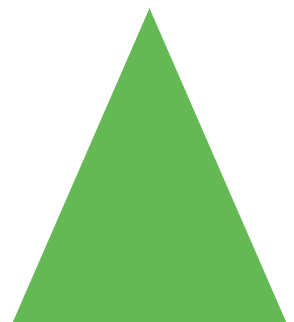## *VMware® Software-Defined Data Center (SDDC) Product Applicability Guide for NIST 800-171*

November 26, 2018

Table of Contents

Revision History

Date	Rev	Author	Comments	Reviewers
November 2018	1.0	Tevora	Initial Draft	VMware

Design Subject Matter Experts

The following people provided key input into this whitepaper.

Name	Email Address	Role/Comments
David Grazer	dgrazer@tevora.com	Co-Author
Christina Whiting	cwhiting@tevora.com	Co-Author
Carlos Phoenix	cphoenix1@vmware.com	Compliance and Cybersecurity SME, VMware
Jerry Breaud	jbreaud@vmware.com	Director, Product Management, Compliance Solutions, VMware

Trademarks and Other Intellectual Property Notices

The VMware products and solutions discussed in this document are protected by U.S. and international copyright and intellectual property laws. VMware products are covered by one or more patents listed at http://www.vmware.com/go/patents. VMware is a registered trademark or trademark of VMware, Inc. and its subsidiaries in the United States and other jurisdictions. All other marks and names mentioned herein may be trademarks of their respective companies.

Solution Area	Key Products
Software-Defined Compute	VMware ESXi™, VMware vCenter®, VMware Cloud Foundation™, VMware vSphere®, VMware vSAN™, VMware vCloud Director® Extender, VMware vCloud® Usage Meter
Network Virtualization and Security	VMware NSX®, VMware AppDefense™
Management and Automation	VMware vRealize® Network Insight™, VMware vRealize Automation™, VMware vRealize Orchestrator™, VMware vRealize Log Insight™, VMware vRealize Operations Manager™, VMware Mirage™, VMware vCloud Director
Disaster Recovery Automation	VMware Site Recovery Manager™, VMware vSphere Replication™, VMware vCloud Availability for vCloud Director®

Disclaimer (Tevora)

The opinions stated in this guide concerning the applicability of VMware® products to the NIST 800-171 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 Solution Exchange: Compliance and Cyber Risk Solutions. This whitepaper 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

Background

This Product Applicability Guide (PAG) provides an evaluation of VMware products that make up and support the Software-Defined Data Center (SDDC) and how they may support NIST 800-171 Rev. 1 (NIST 800-171) controls. These products virtualize and abstract the physical technology layers such as compute, storage, and network, the essence of an SDDC. The changing technology landscape that is modernizing the data center is also modernizing the virtual desktop environment and mobile device management while making inroads to consolidate and automate Information Technology (IT) resources. VMware prioritizes data protection and system security features within the SDDC. The VMware Compliance Solutions team developed a framework that incorporates SDDC product capabilities aligned to NIST 800-171 controls. The overarching PAG framework is built upon NIST 800-53 as a foundational risk framework and security control catalog. The framework maps VMware products to control requirements to weave together VMware product capabilities with compliance requirements and cybersecurity controls.

VMware engaged Tevora, an independent third-party IT audit firm, to conduct a review of the SDDC and VMware Cloud™ solution's alignment to NIST 800-171. This document is the culmination of Tevora's discussions with VMware product teams to perform a thorough evaluation of VMware product capabilities mapped to NIST 800-171 controls.

Tevora is a leading security consulting firm specializing in enterprise risk, compliance, information security solutions, and threat research. Tevora offers a comprehensive portfolio of information security solutions and services to clients in virtually all industries. This PAG will navigate readers through the NIST 800-171 standard and highlight applicable VMware product capabilities.

VMware SDDC and NIST 800-171

Today's infrastructures are heterogeneous in nature, built upon collaborations between internally constructed products and third-party sourced components, all guided by a customer's nuanced business and compliance requirements.

VMware approaches compliance with a view that understands the complex nature of technical environments and addresses those areas where virtualization can be leveraged to develop a more secure environment. This focused view on compliance is reflected in the VMware Compliance Solutions framework, which allows for a wide-ranging adoption of regulatory controls.

The phrase "security by design" identifies architectural decisions and default settings inside VMware products that are integrated into the product lifecycle. This approach reflects the process VMware follows to weave in security through all stages of the product lifecycle, and not as an afterthought. A compliance-capable design follows the philosophy that mapping SDDC product capabilities to NIST 800-171 security requirements can result in a solution that has been vetted as capable of meeting compliance standards if utilized appropriately. This overlap between products and compliance requirements establishes a new level marrying security and non-security product capabilities to also achieve operational innovation. Due to the breadth of the NIST compliance

frameworks, VMware selected NIST 800-53 as its foundation for all future PAGs including NIST 800-171 and alternative industry standards that have been derived from the larger NIST risk framework.

What is SDDC?

The Software-Defined Data Center architecture creates a completely automated, highly available environment for any application, and any hardware. SDDC can be used in any type of cloud model, and extends the existing concepts associated with the cloud such as abstraction, pooling, and virtualization to all aspects of the cloud environment. Features of the SDDC can be deployed as a suite or can also work independently to allow for a controlled deployment over time.

What is NIST?

The National Institute of Standards and Technology (NIST) was founded in 1901 and is now part of the U.S. Department of Commerce. NIST is one of the nation's oldest physical science laboratories. Today, NIST measurements support the smallest of technologies to the largest and most complex of human-made creations—from nanoscale devices so tiny that tens of thousands can fit on the end of a single human hair, up to earthquake-resistant skyscrapers and global communication networks. NIST also assists the federal government in issuing standards to meet the provisions and requirements such as the Federal Information Security Management Act (FISMA).

Introduction

What is NIST 800-171

NIST Special Publication (SP) 800-171 Rev. 1 has been developed by NIST to provide federal agencies with a standard of requirements for protecting the confidentiality of controlled unclassified information (CUI) in nonfederal systems and organizations. The standard assumes that these requirements shall be applied to entities supporting the delivery of federal services and business operations.

It is important to note that Defense Federal Acquisition Regulation supplement 252.204-7012 (DFARS) designates that government contractors handling CUI will need to implement NIST 800-171 as soon as practical but not later than December 31, 2017. This underscores the importance of this standard for contracting organizations.

How does NIST 800-171 work?

The NIST 800-171 standard requires organizations to comply with a robust set of criteria. The criteria are split into 14 control families (listed below) and provide ratings of impact to the business or organization. Organizations are afforded the opportunity to define their requirements and direct system controls.

- Access Control (AC)
- Awareness and Training (AT)
- Audit and Accountability (AU)
- Configuration Management (CM)
- Identification and Authentication (IA)
- Incident Response (IR)
- Maintenance (MA)
- Media Protection (MP)
- Personnel Security (PS)
- Physical Protection (PE)
- Risk Assessment (RA)
- Security Assessment (SA)
- System and Communications Protection (SC)
- System and Information Integrity (SI)

The basic and derived requirements are developed through a combination of FIPS Publication 200 and NIST 800-171 along the moderate baseline. The requirements are then tailored to exclude controls that are:

• Uniquely federal (i.e., primarily the responsibility of the federal government);
• Not directly related to protecting the confidentiality of CUI; or
• Expected to be routinely satisfied by nonfederal organizations without specification.

The aforementioned tailoring validated the removal of the Planning family. All control families may not be applicable to an organization. The relevancy is dependent on the size and scope of the business. It is incumbent upon the organization to identify those which may not apply.

Scope and Approach

The SDDC and VMware Cloud platform covers a wide number of products and architectures. The platforms and each of their component products contain features that could be mapped to some NIST 800-171 controls. Of the 14 total control families, 12 had mapping overlaps to VMware software capabilities. This guide expands to account for all products underneath the SDDC umbrella. The scope of this guide is limited to those requirements supported either technically or through direct API integration. Additional technologies required in addition to VMware products are not identified.

Our Approach

This Product Applicability Guide (PAG) is intended to provide information for all security and compliance practitioners on Tevora's recommended usage of the VMware technical stack to address regulatory compliance obligations and enhance the security of their services through the security and compliance framework of NIST 800-171. It is up to each organization to identify the applicable NIST 800-171 controls and requirements that are in scope and, in addition, to determine if their environment is aligned to either the basic or derived security requirements as stated. The PAG focuses on capabilities of the SDDC product and VMware Cloud at the control family level, as each organization will need to identify its control scope and to perform its own requirement level and selection of controls based on the organization's scope and the relevance to its objectives.

Appendix B outlines specific product capabilities for SDDC and VMware Cloud, and their alignment to NIST 800-171 control families.

In addition to the NIST 800-171 control families, we used eleven (11) security lenses that serve as a baseline to evaluate SDDC and VMware Cloud products. From the ground up, VMware strives to design, define, and deliver compliance solutions to customers. The compliance solution begins with a compliance context (e.g., requirements from the appropriate standards in question).

Next, the technical requirements applicable to the VMware products are mapped to in-scope compliance requirements.

Finally, an independent audit evaluation of the design is conducted. The output is a solution that has interwoven compliance requirements into the end solution available to customers. Below is an overview of this process.

Compliance Solutions
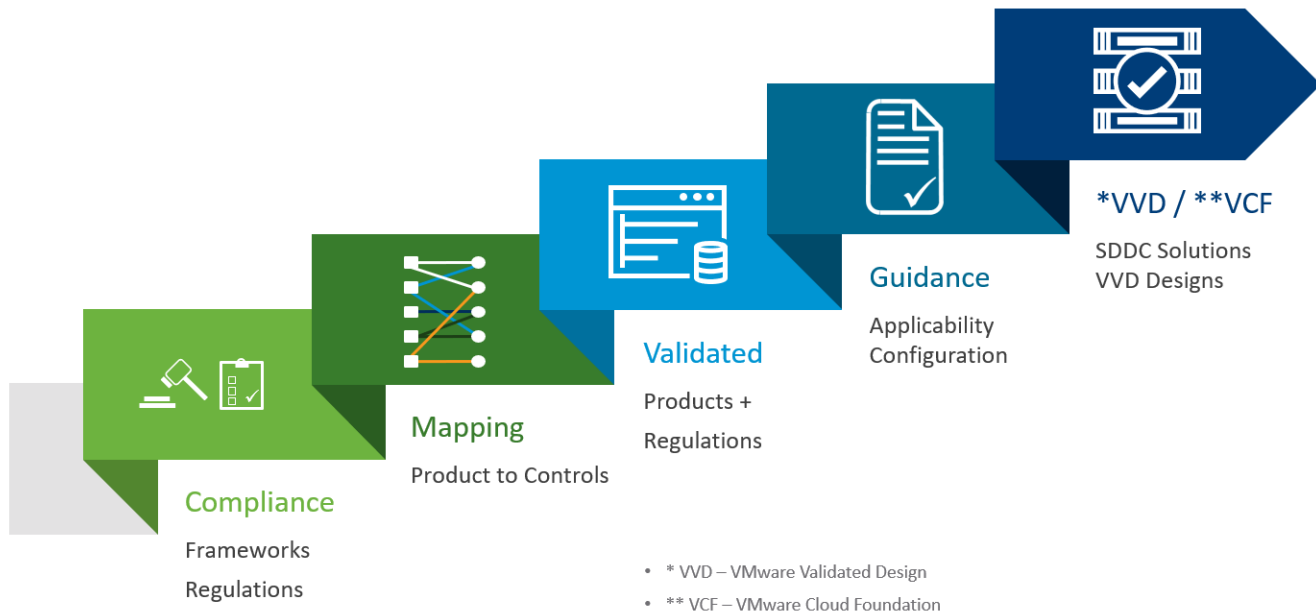
Regulatory Controls Mapping

Exhibit 1: VMware Compliance Solutions Regulatory Controls Mapping

Outside of the process described above, these eleven (11) areas are broad categories of controls that are implemented within today's security programs. They can be used to further understand the broader technology concepts used to build security architectures and to implement controls to mitigate risks.

The eleven (11) security lenses include:

- Automated Security
- System Hardening
- Compliance Validation
- System Access
- Data Segmentation
- System Monitoring
- Data Encryption and Protection
- Network Protection
- Endpoint Protection
- Trusted Execution/Secure Boot
- Software Development Lifecycle (SDLC)

Evaluating the SDDC and VMware Cloud through the additional layer of security lenses helps security and compliance practitioners understand how products deliver the features required not only to support compliance with the NIST 800-171 standard but also to comport with general security best practices.

Tevora reviewed the high-level product design, followed by a detailed examination of data flows, features, architectures, and capabilities across all in-scope products to identify applicable controls. The testing considered all potential configurations that allow SDDC products to support each requirement.

The evaluation produced this guide to provide executives, technology experts, and security and compliance practitioners with insight to enhance security and compliance postures using VMware products. The SDDC's flexibility in feature deployment allows for connection with preexisting systems to further fortify security, privacy, and compliance. Understanding this flexibility is key to then understanding how VMware products can be deployed with continuous compliance in mind.

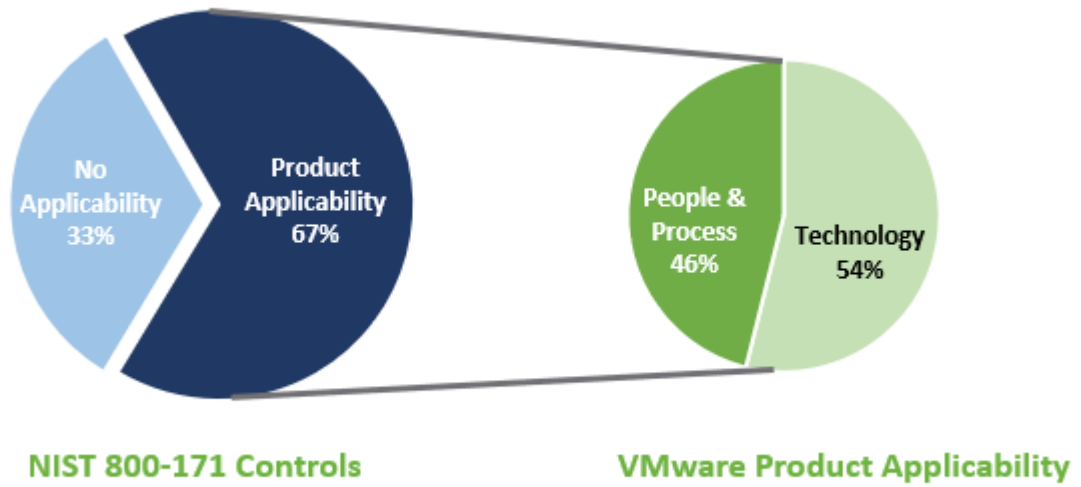**NIST 800-171 Controls**

No Applicability 33%

Product Applicability 67%

VMware Product Applicability

People & Process 46%

Technology 54%

Exhibit 2: Percentage of SDDC Products that are capable of meeting the NIST 800-171 control objectives.

In-Scope VMware Product List

Software-Defined Data Center (SDDC)

VMware vSphere® – vSphere, 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 ESXi™ – ESXi is a purpose-built bare-metal hypervisor that installs directly onto a physical server. With direct access to and control of underlying resources, ESXi is more efficient than hosted architectures and can effectively partition hardware to increase consolidation ratios and cut costs for our customers.

VMware vCenter® – 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™ – **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 Cloud Foundation™

VMware Cloud Foundation and SDDC Manager – Cloud Foundation is the integrated cloud infrastructure platform for the hybrid cloud. It provides dynamic software-defined infrastructure (compute, storage, networking, and security) to run enterprise applications in both private and public environments.

VMware Cloud Provider Platform

VMware vCloud Director® –vCloud Director is the VMware flagship Cloud Management Platform for Cloud Providers. vCloud Director enables Cloud Providers to deliver differentiated cloud services on their VMware cloud infrastructure and provides enterprises with self-service cloud capabilities.

VMware vCloud Director Extender – vCloud Director Extender enables Cloud Providers to connect vCenter environments on-premises to a cloud based on vCloud Director to securely migrate virtual machines, and extend virtual networks to the cloud. vCloud Director Extender provides seamless hybridity between on-prem and cloud environments based on vSphere.

VMware vCloud Usage Meter – vCloud Usage Meter helps Cloud Providers access VMware resources on a consumption-based monthly subscription, including vCloud Usage Insight, an SaaS tool that provides automated usage reporting, simple onboarding, secure data transfer and aggregation of usage across all contracts and sites.

VMware vCloud Availability for vCloud Director® – vCloud Availability Cloud to Cloud DR enables Cloud Providers to perform vSphere native replication of workloads for Disaster Recovery or migration purposes between vCloud Director Organization Virtual Data Centers. The solution is compatible to the vCloud Director self-service user interface or standalone and features symmetric source or destination execution of replication, migration, failover and failback of workload virtual machines and VMware vSphere vApps™ within vCloud Director.

VMware Cloud Provider Pod – Cloud Provider Pod automates and documents the deployment of a Cloud Provider Platform solution stack that adheres to VMware Validated Design for Cloud Provider principles and is thoroughly tested for interoperability and performance. The Cloud Provider Platform technologies deployed by Cloud Provider

Pod enables providers to deliver self-service tenant capabilities such as data center extension, cloud management, cloud migration, metering and chargeback in an inherently multi-tenant infrastructure. Cloud Provider Pod helps Cloud Providers achieve the fastest path to VMware based cloud services delivery.

Virtualized Networking

VMware NSX® Data Center – NSX is the network virtualization and security platform for the Software-Defined Data Center (SDDC), delivering networking and security entirely in software, abstracted from the underlying physical infrastructure. NSX provides network micro-segmentation functions including switching, routing, and firewalling that are embedded in the hypervisor and distributed across the environment.

VMware vRealize® Suite

VMware vRealize Operations Manager™ – vRealize Operations Manager is designed to automate and simplify the performance, troubleshooting, capacity, cost planning, and configuration management of applications and infrastructure across physical, virtual, and cloud environments.

VMware vRealize Log Insight™ – vRealize Log Insight delivers heterogeneous and highly scalable central log management with intuitive, actionable dashboards; sophisticated analytics; and broad, third-party extensibility, providing deep operational visibility and faster troubleshooting.

VMware vRealize Network Insight™ – vRealize Network Insight delivers intelligent operations for network virtualization and security. It helps customers build an optimized, highly available, and secure network infrastructure across multi-cloud environments. It accelerates micro-segmentation planning and deployment, enables visibility across virtual and physical networks, and provides operational views to manage and scale NSX deployments.

VMware vRealize Orchestrator™ – vRealize Orchestrator is a powerful automation tool designed for system administrators and IT operations staff who must streamline tasks and remediation actions and integrate these functions with third-party IT operations software.

VMware vRealize Automation™ – vRealize Automation empowers IT to accelerate the provisioning and delivery of IT services across infrastructure, containers, applications, and custom services. Leveraging the extensible framework provided by vRealize Automation, you can streamline and automate the lifecycle management of IT resources from initial service model design through Day One provisioning and Day Two operations.

Business Continuity

VMware Site Recovery Manager™ – Site Recovery Manager is the industry-leading solution to enable application availability and mobility across sites in private cloud environments. It is an automation software that integrates with an underlying replication technology to provide policy-based management, non-disruptive testing, and automated orchestration of recovery plans. This provides simple and reliable recovery and mobility of virtual machines between sites, with minimal or no downtime.

VMware vSphere Replication™ – vSphere Replication is an extension to VMware vCenter Server® that provides hypervisor-based virtual machine replication and recovery.

Desktop and Application Virtualization

VMware Mirage™ – **Mirage** provides next-generation image management for physical desktops and POS (point-of-sale or point-of-service) devices. Dynamic layering and full system recovery ensure that IT can quickly and cost-effectively deliver, manage, and protect updates to operating systems and applications on endpoints at scale.

VMware AppDefense™

VMware AppDefense – **AppDefense** is a data center endpoint security product that protects applications running in virtualized and cloud environments. AppDefense understands an application's intended state and behavior, then monitors for changes to that intended state that indicate a threat. When a threat is detected, AppDefense automatically responds.

Appendix B in this guide showcases the capabilities of all products in alignment with NIST 800-171 intents.

Overview of VMware and NIST 800-171 Best Practices and Requirement Mapping

Best Practice Area (Lens)	NIST 800-171	Capability Description	VMware Product Applicability
Automated Security	CP, RA	Automated Deployment, Automated Remediation	Site Recovery Manager vSphere Replication vRealize Operations vCloud Director vCloud Availability for vCloud Director
Data Segmentation	SA, SC, SI	Network and Host Firewall, Information Flow	NSX Cloud Foundation vRealize Network Insight vRealize Operations vRealize Log Insight AppDefense vCloud Usage Meter vCloud Director vCloud Director Extender vCloud Availability for vCloud Director
System Hardening	CM, MP, PS, SA, SC, SI	Configuration Management, Patch Management, Vulnerability Management	vRealize Network Insight vRealize Operations vRealize Log Insight VMware vSphere Update Manager™ NSX ESXi 6.5 AppDefense vCloud Usage Meter vCloud Director vCloud Director Extender vCloud Availability for vCloud Director
Compliance Validation	CM	Configuration Management	vRealize Network Insight vRealize Operations vRealize Log Insight NSX AppDefense vCloud Director
System Access	AC, AT, AU, IA, IR, PE, , PS, SC	Two-Factor Authentication, Identity and Access Management	vCenter NSX vRealize Network Insight vRealize Log Insight vRealize Operations ESXi 6.5 AppDefense vCloud Usage Meter vCloud Director vCloud Director Extender vCloud Availability for vCloud Director
System Monitoring	AT, AU, CA, CM, CP, IR, MA, PE, PS, RA, SC, SI	Security Information Event Monitoring (SIEM), Database Monitoring	vRealize Log Insight vRealize Network Insight vRealize Operations Site Recovery Manager vSphere Replication vCenter vSphere Update Manager AppDefense

			vCloud Usage Meter vCloud Director vCloud Director Extender vCloud Availability for vCloud Director
Data Encryption and Protection	CA, IA, MA, SA, SC, SI	Data at Rest Encryption, Data in Motion Encryption, System Backup and Restore	vSphere 6.5 VM Encryption feature vSAN 6.6 vSAN Encryption feature VMware vSphere vMotion® encryption NSX vRealize Operations vRealize Network Insight vRealize Log Insight vSphere Cloud Foundation vSphere Update Manager AppDefense vCloud Usage Meter vCloud Director vCloud Director Extender vCloud Availability for vCloud Director
Network Protection	AT, CA, CP, IR, PE, RA, SC	Intrusion Prevention System, Web Application Firewall	Site Recovery Manager vSphere Replication NSX vRealize Operations vRealize Network Insight vRealize Log Insight AppDefense vCloud Director vCloud Director Extender vCloud Availability for vCloud Director
Endpoint Protection	AC, CM	Endpoint A/V and Malware Prevention, File Integrity Monitoring, Data Leakage Protection, Mobile Device Management	NSX ESXi 6.5 vRealize Operations vRealize Network Insight vRealize Log Insight AppDefense vCloud Director vCloud Director Extender vCloud Availability for vCloud Director
Trusted Execution/Secure Boot	SC, SI	Execution Integrity	ESXi 6.5 NSX vRealize Log Insight vRealize Operations vRealize Network Insight vSphere Update Manager AppDefense vCloud Director vCloud Director Extender vCloud Availability for vCloud Director
Software Development Lifecycle (SDLC)	SA	Configuration Integrity	Cloud Foundation

Exhibit 3 represents a high-level view of how VMware technology capabilities match up to best practices areas as well as NIST 800-171 requirement topics.

VMware Control Capabilities Detail

VMware Validated Design and Software Development Process

VMware has developed the VMware Validated Design (VVD) to allow organizations to implement the full SDDC platform using a design that is validated and provides the detail required to confidently deploy SDDC. The VVD is available to anyone and is published on the VMware website.

The VMware Software Development Lifecycle (SDLC) designs security into all phases of SDDC and VMware Cloud products (Exhibit 3). This principled approach to designing security, overseen by VMware Product Security from the start, is important to NIST 800-171 compliance, as the products utilized are required to have security interwoven through their underlying substructures, to be supported by administrative policy.

With compliance and security woven into the SDLC, VMware improves the quality of its products and solution platforms that can support organizations using the NIST 800-171 risk-and-control framework.

As further reference to the primary purposes of a control family, each detail segment provides the applicable security lens defined within the VMware approach. These lenses are hallmarks of a mature security program addressing common areas of vulnerabilities.
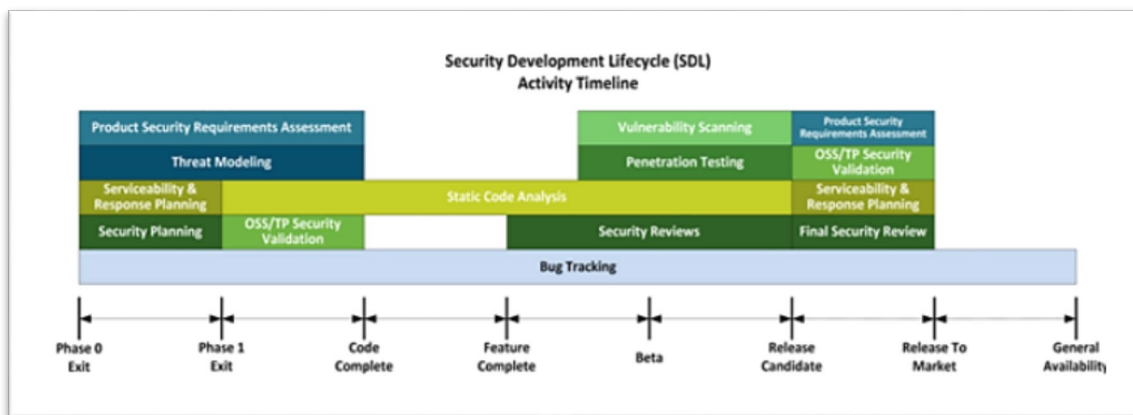
Exhibit 4: VMware SDL Activity Timeline

Core and Administrative Control Categories

To streamline the delivery of this PAG 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. Further details on these categories and the aligned control families can be found in the following sections.

VMware Administrative Support for NIST Control Families

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

This is a common thread throughout the capabilities discussed below. An organization will be able to deploy VMware products, apply the NIST 800-171 controls, and monitor them through the compliance-capable platform. In this way, implementing policy or operating procedures assists in maintaining a secure and compliant information architecture.

Another key aspect of NIST 800-171 includes derived controls in addition to the basic requirements. As a framework, NIST 800-171 provides organizations with an opportunity to enhance controls using additional, complementary controls beyond the baseline of controls associated with each control family.

An example of an administrative control family is Awareness and Training (AT). This control family may require a documented security training program or detailed data usage policies. Using VMware products such as NSX, vRealize Network Insight, or vRealize Log Insight to strengthen and accelerate discoveries and corrective actions can yield data via their monitoring, troubleshooting, and remediation capabilities that can be utilized to create more effective programs or better refine existing policies. However, this control family is more focused on the people and process. Thus, this guide will treat the control family as an administrative support control family instead of a core control family because VMware product capabilities support the administration of the control family rather than a core technology control.

The following Control Families fall within Administrative:

- Awareness and Training
- Incident Response
- Maintenance
- Media Protection

- Physical Protection
- Maintenance
- Personnel Security
- Risk Assessment

VMware Core Support for NIST Control Families

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 800-171 that best highlight how each product provides capabilities to strengthen the security and support a compliance-capable platform.

The details below showcase the SDDC and VMware Cloud components that support or apply to each NIST control family and their respective High-Impact controls. Each area defines the intention of the NIST family, aligning security lenses as described in the "**Our Approach**" section (above), and the specifics of the product and their native features that meet control standards. Exhibit 2 (above) illustrates this information.

This guide provides organizations with the opportunity to harness the capability of modern virtualization technology to enhance their security program and processes. Organizations can be confident in their decision to elevate the sophistication of techniques needed to meet complex requirements and secure modern technology infrastructure.

The following Control Families fall within Core:

- Access Control

- Audit and Accountability

- Security Assessment
- System and Communications Protection
- Configuration Management
- Identification and Authentication

- System and Information Integrity

VMware Core Controls

Access Control (AC)

NIST Controls 3.1.1 – 3.1.22

The Access Control family focuses on the ability of any user, at all permission levels, to reach key elements of the environment. It looks at coverage across subjects such as remote access, the protection of access and authentication, as well as the integrity of the entire authentication process.

Applicable Security Lens:

- System Access
- Endpoint Protection

Applicable VMware Product(s):

- VMware NSX for vSphere
- vSphere
- SDDC Manager
- Cloud Foundation
- vRealize Automation
- vRealize Log Insight
- vRealize Network Insight
- vRealize Orchestrator
- vRealize Operations

- Mirage
- Site Recovery Manager
- vSAN 6.6
- AppDefense
- vCloud Usage Meter
- vCloud Director Extender
- vCloud Director
- vCloud Availability for vCloud Director

VMware Product Capabilities

For all products within the SDDC platform, Access Control can be implemented at a granular level. This is presented through Role-Based Access Control (RBAC) mechanisms natively available. User management interfaces are provided to control password complexity and user profiles and to access review tasks. Products, for instance vCenter, enable complementary products with RBAC capabilities. This is particularly the case for Site Recovery Manager used in conjunction with vCenter.

As an elevated protection, VMware has built third-party integration capabilities to allow organizations to integrate single-sign-on (SSO) tools to strengthen authentication needs and restrict access into many of their core offerings. Organizations can integrate their Active Directory (AD)/Lightweight Directory Access Protocol (LDAP) instance through use of VMware published Application Programmable Interfaces (API) to refine access at all levels of their virtual stack. vRealize Operations allows administrators to limit concurrent sessions and define account lockout parameters. vCloud Usage Meter provides additional LDAP configuration and has HTTPS enabled by default, with support for SSH. The vCloud Director provides the ability to administer user accounts via the Administration page, the provided API, and LDAP integration. Further, vCloud Director provides multi-tenancy, isolation of tenants, and logically isolated switches. vCloud Director can be combined with vCloud Director Extender and vCloud Availability for vCloud Director.

To ensure that only trusted IPs, subnets, or IP devices are allowed into the environment, vCenter and NSX provide access restriction to an organization's East–West traffic, or Virtual Machine (VM) to Virtual Machine

communications. Mirage allows for restricting elevated access to Domain accounts, limiting unauthorized movement throughout an environment.

NSX supports role based access control through the implementation of micro-segmentation via security policies. The NSX Identity Firewall feature enhances the access control down to the virtual networking level, permitting only approved users with need to access specific virtual machines. The supported micro-segmentation can segment workload and platform components, including restricting remote access to approved communication standards and administration. These authentication mechanisms can be managed through security groups and policies configured within the VMware vSphere Web Client.

AppDefense integrates vSphere access controls, which include LDAP support to restrict access to the AppDefense Manager. AppDefense also provides the capability to log user activity for anyone with root access to the monitored applications to better track privileged access.

Within vCloud Director manage and monitor portals, various logging capabilities can be configured and reviewed. Additionally, servers can be configured into a log repository to hold logs from NSX components and hosts. The administration portal also offers the ability to configure account lockouts and to configure devices and accounts with access control permissions based on compliance requirements. The system administrator account permissions encompass all existing rights, in addition to those associated with administrator accounts, which are immutable.

Additional product capability details can be found at the VMware Compliance IDs listed in *Appendix B*.

Audit and Accountability (AU)

NIST Controls 3.3.1-3.3.9

The Audit and Accountability NIST control family discusses the implementation, governance, and operation of an audit program. As a function of the program, it calls for organizations to ensure the protection of any logs and additional information associated with audit procedures.

Applicable Security Lens:

- Systems Monitoring
- System Access

Applicable VMware Product(s):

- vCenter
- vRealize Log Insight
- Site Recovery Manager
- ESXi 6.5
- vRealize Operations
- vRealize Network Insight
- vSphere Replication
- vRealize Operations
- vRealize Automation

- NSX for vSphere
- vSAN
- AppDefense
- vCloud Usage Meter
- vCloud Director
- vCloud Director Extender
- vCloud Availability for vCloud Director

VMware Product Capabilities

The Audit and Accountability control family speaks to the need for a security program to conduct ongoing audits to maintain integrity and compliance. Implementing the SDDC through the VVD (VMware Validated Design) provides a reference architecture to identify security requirements throughout the virtual platform, from Hypervisor through to the User Interface that collects audit log data.

Across all products, rich logging features exist to allow administrators to ascertain who logged in, the origin, at what time (coordinated through NTP), and whether the attempt was a success or failure. Logs can be pointed to third-party management tools through API integration if desired. AppDefense delivers alerts for all changes made within the environment and has several logging features. This can be configured through the provided "Scopes" feature or through the vSphere Web Client. Any logs generated by AppDefense can be calibrated using both vSphere and the AppDefense Manager and access can be restricted to only an administrator. Additionally, vSphere supports capacity planning within configured environments and any location where AppDefense is installed.

Implementing vCloud Director can add additional benefits in the form of monitoring functionality, which produces audit logs on the environment and can be used to monitor all assets within the environment. Access to this functionality can be restricted, as administrators can restrict access to most of the vCloud Director instance. vCloud Director is also integrated into the vSphere environment, with the ability to be united with vCloud Availability for vCloud Director to guarantee functionality.

Further, vRealize Log Insight gives IT and IT Security Teams the ability to point all products in their stack (not only their VMware product stack) to vRealize Log Insight to help manage and correlate any incidents or perceived incidents through an audit dashboard and native log analysis. vCloud Usage Meter can store additional logs in the VMware vFabric® Postgres database of the appliance, which can be secured.

Monitoring is possible by using vRealize Network Insight, vRealize Log Insight, and vRealize Operations. vRealize Log Insight strengthens access security with forensic monitoring of the virtual/physical networking and flow. This also includes NSX stateful firewall and security group policies. Out of the box, vRealize Log Insight provides security dashboards that enable monitoring of associated VMware products.

To support non-repudiation, administrators are advised to design strong access control surrounding Administrator Passwords. All administrative actions should be logged and reviewed on a consistent basis.

vCenter can be configured for specific-day retention. Tamper proofing can also be configured if leveraging vRealize Log Insight. vRealize Log Insight retains data based on defined storage capacity. vRealize Operations assists by monitoring the datastore's health and capacity, prompting the Administrator to determine how to proceed with further log archival if need be.

vRealize Network Insight contains the ability to adjust forensic data retention. Database storage can be adjusted to a specified limit up to 13 months. ESXi 6.5 affords administrators the ability to adjust the richness and frequency of audit logs.

For advancing an organizational audit process, it is recommended that a Security Incident Event Management (SIEM) platform be coordinated through vRealize Log Insight to ingest logs. This can all be set through the REST API and will enable organizations to garner meaningful evidence to take real-time action.

Additional product capability details can be found at the VMware Compliance IDs listed in *Appendix B*.

Configuration Management (CM)

NIST Controls 3.4.1-3.4.9

This control family establishes management of information systems and software configurations within the environment and how those configurations and baselines are secured. Attention is given to identifying baseline configurations and how any changes to the configurations are managed with the security program.

Applicable Security Lens:

- System Hardening
- Compliance Validation
- System Monitoring
- Endpoint Protection

Applicable VMware Product(s):

- NSX for vSphere
- vRealize Orchestration
- vRealize Operations
- vCenter
- ESXi 6.5
- vSphere Replication
- vSphere Update Manager

- vSphere 6.5 VM Encryption feature
- AppDefense
- vCloud Director
- VMware Cloud platform
- vCloud Usage Meter

VMware Product Capabilities

The VVD architecture contains specified requirements for each component's configuration. This provides a "gold standard" for deployment across the entire suite of products. This standard is developed with security requirements through the SDLC.

To further protect any adjustments to information systems configuration, micro-segmentation can be defined through NSX for vSphere. Routing specifications can be set and protected by tamperproof logging. Active Directory can be integrated to enforce least privilege functionality, based on requirements across the user base. Devices can be isolated to eliminate rogue device infiltration. All configuration and isolation activities can utilize REST API to deliver at scale and in real time. This is an advised strategy on environments deploying VMware vRealize Configuration Manager™. Endpoints should be configured to collect data and point information into vRealize Configuration Manager.

Endpoints can be further protected with AppDefense, which can comprehend the state of an environment and actively monitor changes in any applications, configurations, or system behavior. AppDefense can also be configured to block individual ports or protocols. Engaging vCloud Director can provide the ability to manage traffic between virtual machines within an organization via distributed firewall rules, along with edge gateway firewall capabilities.

Knowing that the protection of or adherence to standards is difficult without knowing what resides in the network, vSphere and vRealize Automation have features to provide a database of virtual machines, which can be updated automatically. In conjunction, vRealize Operations provides organizations with the option to deploy agents to unearth deep, network-layer intel and monitor host configurations.

Additional product capability details can be found at the VMware Compliance IDs listed in *Appendix B*.

Identification and Authentication (IA)

NIST Controls 3.5.1-3.5.11

This control family establishes how an organization should address and protect authentication. The family delves into re-authentication requirements and cryptographic-enabled security. Overall, the intent of the family is to ensure that appropriate measures are employed for the operations and management of Identification and Authentication within an environment.

Applicable Security Lens:

- Data Encryption and Protection
- System Access

Applicable VMware Product(s):

- Mirage
- NSX for vSphere
- SDDC Manager
- vRealize Log Insight
- vRealize Operations
- vSphere
- ESXi 6.5
- Site Recovery Manager

- vSAN 6.6
- vCenter
- AppDefense
- vCloud Usage Meter
- vCloud Director
- vCloud Director Extender
- vCloud Availability for vCloud Director

VMware Product Capabilities

SDDC requires the use of AES256 cryptographic protocols. To assist with user authentication, Active Directory can be integrated for central management of credentials. To guarantee that no sessions remain unlocked, time-outs and re-authentication can be set across all SDDC products by following the standard VVD requirement. Both the vSphere 6.5 VM Encryption feature and the vSAN Encryption feature in vSAN 6.6 certify that all data stored within a customer's SDDC environment is encrypted to industry standards.

By default, all session time-outs require user re-authentication. Typically set to 15 to 20 minutes, session time-out thresholds can be configured within the product and adjusted to meet control intents. Products can again harness Active Directory integration to maintain vigilance over authentications to products. AppDefense can manage and configure unique user identifiers within the Operational Console for any user logged into the AppDefense Console. vCloud Usage Meter can utilize LDAP for user authentication. These instances are then logged within vSphere.

Natively, organizations can harness micro-segmentation to reduce the risk profile of their environment. For this control family, micro-segmentation is particularly important and can be implemented using NSX. Virtual machines (VMs) can be configured to only speak to other VMs in specified situations, based upon security policies.

Across all products, default passwords can be reset. vRealize Operations can be configured to force root users to reset their passwords during their initial login. All products in accordance with the VVD and SDLC are required to have minimum password standards that are stored in an encrypted fashion, never maintained in clear text format.

SDDC and VMware Cloud products across the suite allow for seamless 2FA deployment through third-party integrations.

Administrators viewing all passwords through the graphic user interface (GUI) will have passwords for all credentials obscured or masked with asterisks.

To note, some controls only have partial matches but are supported across all products within the SDDC. These controls relate to authentication against a certificate authority (CA). The organization will need to identify the CA that will then be assessed against during each user session.

Additional product capability details can be found at the VMware Compliance IDs listed in *Appendix B*.

Incident Response (IR)

NIST Controls 3.6.1-3.6.3

The Incident Response control family is driven by the creation of organizational policies that address how evolving disaster or security events will be addressed. SDDC components can assist in the research, auditing, and curtailing of those events attributed to technical elements through integration into IDS/IPS appliances or a SIEM.

In other respects, the breadth of the family is focused on developed administrative policy.

Applicable Security Lens:

- System Access
- System Monitoring
- Network Protection

Applicable VMware Product(s):

- ESXi 6.5
- vSphere Replication
- vCenter
- AppDefense
- vCloud Director

- vRealize Log Insight
- NSX
- Site Recovery Manager
- VMware Cloud platform

VMware Product Capabilities

AppDefense provides continuous detection at the hypervisor level of vSphere, allowing it to block, suspend, or shutdown malicious behavior. It can also block or whitelist other activity within the environment based on its 'Learning Mode,' which assists with identifying the desired functionality of applications to determine when malicious activity is present. This, combined with the ESXi Secure Boot feature, promotes automated response orchestration at launch and during operation. vCloud Director supports integration of AppDefense into the vSphere environment, which extends AppDefense intrusion detection and prevention capabilities to various cloud environments, enhancing an organization's ability to respond to evolving incidents.

Site Recovery Manager can be included in simulated events to assist with recovery or continuity planning tests or training. These events can be triggered manually at the administrator's discretion, if individual tests need to be conducted. Site Recovery Manager also supports system prioritization.

vRealize Log Insight provides the ability for alerts to be generated when agents become unresponsive or are offline for a defined period of time.

Physical Protection (PP)

NIST Controls 3.10.1-3.10.6

The Physical Protection control family establishes criteria for the physical security of data, technology, and people. This control family certifies that the physical controls are addressed within policies, procedures, or technical applications and are enforced appropriately through the environment's scope.

VMware products can support the controls of this family through organizationally developed policy when properly used. All SDDC platform components provide backup and recovery capabilities, which will aid the employment of the policy for requirements such as data protection and handling of physical security measures.

Applicable Security Lens:

- System Access
- System Monitoring
- Network Protection

Applicable VMware Product(s):

- vSphere Replication

VMware Product Capabilities

vSphere Replication provides additional data security by providing robust, easy-to-use replication solutions reducing the data's susceptibility to physical risks such as equipment theft, disasters, or connectivity outages.

Security Assessment (SA)

NIST Controls 3.12.1-3.12.4

The Security Assessment control family establishes criteria and controls to ensure that only authorized connections are enabled throughout an organization's environment. At its core, the Security Assessment and Authorization control family aims to certify that all systems support security in depth. The interconnections of systems, appropriate authorizations, and the processes that support them are key. The applicable VMware products create an ease of configuration natively to support this intent.

Beyond product applicability, organizations are advised to perform proactive penetration tests to meet the full extent of the control area.

Applicable Security Lens:

- System Monitoring
- Data Encryption and Protection
- Network Protection

Applicable VMware Product(s):

- vCenter
- vRealize Operations

VMware Product Capabilities

vCenter provides the capability to support existing Business Continuity Plans by providing workload management during host disruptions. Additionally, vRealize Operations generates metrics and system performance reports, which can be utilized alongside organizational standards, or other benchmarks, to support capacity planning and general system operations.

Additional product capability details can be found at the VMware Compliance IDs listed in *Appendix B*.

System and Communications Protection (SC)

NIST Controls 3.13.1-3.13.16

The System and Communications control family addresses the need for protecting information throughout its lifecycle within the environment. It assesses how traffic travels from outside to inside an organization's network and the layers in between.

Applicable Security Lens:

- Data Segmentation
- System Hardening
- System Access
- System Monitoring

- Network Protection
- Data Encryption and Protection
- Trusted Execution/Secure Boot

Applicable VMware Product(s):

- NSX for vSphere
- VMware vSphere NSX-T Data Center
- vRealize Automation
- vRealize Network Insight
- vRealize Orchestrator
- vRealize Operations
- vCenter
- Site Recovery Manager
- ESXi 6.5

- vSphere Replication
- vSAN 6.6
- Mirage
- Cloud Foundation
- SDDC Manager
- vCloud Usage Meter
- vCloud Director
- vCloud Availability for vCloud Director
- vCloud Director Extender

VMware Product Capabilities

One main objective within this control set is minimizing the development of covert channels. VMware conducts peer reviews during each development cycle to plug all potential back doors. VVD requirements force security requirements to maintain adequate levels of encryption, logging specifically through separating vRealize Log Insight from vRealize Network Insight and pushing security groups through NSX.

All pieces of VMware software include digital signatures and 256 MAC hashing.

Micro-segmentation allows logical domain segmentation at a granular isolation level. For DDoS attacks, NSX builds in capabilities to perform malware analysis. These attributes supplement vulnerability scanning capabilities that exist within the SDLC. NSX and other SDDC products grant administrator functionality to restrict remote access to defined protocols, i.e., SSH and RDP. For instance, Mirage utilizes Remote Desktop Protocol (RDP) solely. vCloud Usage Meter has TLS enabled by default for all communications and conducts checksum verification for generated reports.

Beyond protocol restriction, vRealize Automation contains multiple default roles that segment information based on roles at scale. Coupled with vRealize Log Insight, this enables authentication to be authorized granularly across a designed environment without third-party integration. Similar to vRealize Automation, vRealize Operations

permits the creation of groups utilizing RBAC to define segregation of certain areas or devices within an environment.

VMware NSX Edge™ gateways give boundary protection and network isolation to user environments. Through its Dynamic Host Configuration Protocol (DHCP) service, NSX Edge gateways set a static binding. By doing so, unique identifiers are set prior to any execution, fortifying an information system against malicious activity and defining a virtual boundary for organizations utilizing multi-tenant cloud environments.

For enhanced visibility, organizations can leverage vRealize Network Insight to provide context on information flow within the environment. vRealize Network Insight uses platform and proxy use certificates to restrict flow within an infrastructure. NSX and its micro-segmentation can then enforce defined information flow guidelines. VMware NSX Manager™ can sync with RBAC to restrict access based on specified group names. The information contained within these data flows is then secured at rest with the vSAN Encryption feature in vSAN 6.6 and with the vSphere 6.5 VM Encryption feature. ESXi 6.5 further segments processes within resource pools. vCloud Director supports native integration into NSX Distributed Firewall to provide application isolation. vCloud Usage Meter provides further protection by allowing users to be segmented into three groups: root Unix user, non-root Unix user, and UI user, who has no system access.

VMware security programs and practices establish requirements "by design" to evolve methodologies of protection against new "in-the-wild threats." This takes effect throughout the development process and is developed into products. Products are tested by first-class vulnerability scans and penetration tests prior to any full release or version update.

For further information, please visit:
https://www.vmware.com/content/dam/digitalmarketing/vmware/en/pdf/VMware-Product-Security.pdf.

Additional product capability details can be found at the VMware Compliance IDs listed in *Appendix B*.

System and Information Integrity (SI)

NIST Controls 3.14.1-3.14.7

Maintaining integrity within the system and information it provides is paramount. This control family requires that organizations implement protections concentrated on three key areas: System Monitoring; Software, Firmware, and Information Integrity; and Flaw Remediation.

Applicable Security Lens:

- Data Segmentation
- System Monitoring
- System Hardening

- Data Encryption
- Trusted Execution/Secure Boot

Applicable VMware Product(s)

- ESXi 6.5
- vSphere Replication
- vSAN 6.6
- vRealize Log Insight
- NSX for vSphere
- vRealize Automation

- vRealize Network Insight
- Cloud Foundation
- vSphere Update Manager
- vCenter
- AppDefense
- Mirage
- VMware Cloud platform

VMware Product Capabilities

Through the lens of the VVD "secure by default" directive and the guidance of the security criteria held within the SDLC, VMware SDDC and VMware Cloud platform components consistently prioritize system integrity and the information it holds.

To highlight, ESXi 6.5 maintains a secure boot protocol utilizing vSphere Installation Bundles (VIBs). Harnessing the Unified Extensible Firmware Interface (UEFI), the hypervisor refrains from loading unless the signature database (containing the whitelisted and blacklisted signatures) validates. vCenter supports alerts to prevent unauthorized execution within the environment, and AppDefense can detect unauthorized code execution, send alerts, and address anomalies directly.

If signatures are not validated, the hypervisor fails to activate. ESXi 6.5 does not report system intelligence back on the failure to the session's origin. This is crucial as it protects the integrity of an organization's virtual servers from adversaries targeting intelligence to exploit. NSX natively includes defined guest introspection framework that allows administrators to conduct analysis on the data plane level from North–South traffic flows.

Adding strength to the secure boot protocol are vRealize Log Insight and vRealize Network Insight features that can be configured to notify the security team in the event a root account is being accessed, brute force attack, or

attempt to attack an ESXi host. All alerts can be sent via email, allowing security personnel to intercept incidents at their earliest stages.

To widen appliance coordination, vRealize Log Insight, vRealize Network Insight, and vRealize Orchestration can be combined to define an event occurrence–level alert. This capability will enable organizations to calibrate alerts so that critical alerts are noticed through visual dashboards and defined distribution lists. vSphere Update Manager can be configured to automate remediation on identified vulnerabilities. Third-party solutions can be inserted to combine both on-premises and cloud-based synchronization of updates.

AppDefense can, on its own, isolate threats as they appear and suspend the affected section of the environment. AppDefense actively monitors the environment from the hypervisor layer and can detect anomalies in application behavior or network traffic, as well as changes made to network configuration. Actions can be addressed automatically when alerts are triggered. It can also be integrated with the vSphere environment, which if used in conjunction with vCloud Director can be used to establish and maintain intrusion detection and management.

Finally, all VMs can be configured for destruction upon end of life, defined by the administrator.

Additional product capability details can be found at the VMware Compliance IDs listed in *Appendix B*.

VMware Administrative Controls

Awareness and Training (AT)

NIST Controls 3.2.1-3.2.3

This control family is managed through Administrative action on the client side and is not applicable to VMware natively. VMware provides documentation that may support security awareness and training efforts.

Applicable Security Lens:

- System Monitoring
- System Access
- Network Protection

Applicable VMware Product(s):

- vRealize Log Insight
- vRealize Network Insight
- vRealize Operations
- ESXi
- vSphere Replication

- vCenter
- vCloud Director Extender

Maintenance (MA)

NIST Controls 3.7.1-3.7.6

Most controls listed underneath this control family are performed in accordance with organizational policy. vSphere Update Manager and vRealize Operations allow for maintaining up-to-date patching. When configured accordingly, products such as vCenter assist in the updates and patching for complementary VMware products, e.g., ESXi 6.5.

Moreover, all products are pre-inspected prior to ingestion/deployment and are hashed to elevate security protocols at the deepest levels of the virtual stack.

Lastly, proof of maintenance within NIST is required to ensure that all procedures are being followed as stated in governing policies. All products can generate logs that highlight when maintenance did occur on the component.

Applicable Security Lens:

- System Monitoring
- Data Encryption and Protection

Applicable VMware Product(s):

- NSX for vSphere
- vRealize Configuration Manager
- vRealize Operations

- ESXi 6.5
- vCenter
- vCloud Availability for vCloud Director

Media Protection (MP)

NIST Controls 3.8.1-3.8.9

VMware products can support the controls of this family through organizationally developed policy when properly used. Products within the SDDC do not natively provide features that directly apply to the family's intent. Natively, the vSAN Encryption feature provides two media functions within its datastore for cache and capacity to protect media if this feature is activated.

Applicable Security Lens:

- System Hardening

Applicable VMware Product(s):

- ESXi 6.5
- vSAN Encryption feature of vSAN 6.6
- vSphere Replication
- vCloud Director Extender

Personnel Security (PS)

NIST Controls 3.9.1-3.9.2

VMware products can support the controls of this family through organizationally developed policy when properly used. Products within the SDDC natively provide features that support the family's intent. These features include general user review reports and log intelligence capabilities.

Applicable Security Lens:

- System Access
- System Hardening
- System Monitoring

Applicable VMware Product(s):

- vRealize Configuration Manager

Risk Assessment (RA)

NIST Controls 3.11.1-3.11.3

VMware products can support the controls of this family through organizationally developed policy when properly used. All SDDC platform components do provide backup and recovery capabilities, which will thus aid the employment of a policy's requirements such as data protection and being able to meet recovery time objectives (RTO) and recovery point objectives (RPO). Site Recovery Manager and vSphere Replication can support the assurance of meeting RTO and RPO criteria. vRealize Network Insight assists risk assessments through visibility into network traffic throughout the environment.

Applicable Security Lens:

- System Monitoring
- Network Protection
- Automated Security

Applicable VMware Product(s):

- vRealize Network Insight
- Site Recovery Manager
- vSphere Replication
- vCenter
- AppDefense
- vCloud Director

Conclusion

To meet evolving regulatory needs, security programs now must define applicable controls at early stages. From ideation to design and through to the end of the product lifecycle, VMware has focused on developing methodologies that set this tone, regardless of the framework in question.

Through the eleven (11) security lenses and in accompaniment of the VMware Validated Design, the SDDC platform components and VMware Cloud provide users with a virtualization stack that adheres to the comprehensive requirements of NIST 800-171 for protecting CUI at both basic and derived control levels.

Organizations can seamlessly piece together full SDDC and VMware Cloud environments, or a subset made up of individual components, and be confident in the security and privacy measures employed in the products.

The considerations that VMware brings to bear on continuous compliance for clients come from its development culture, which constructs requirements that balance functionality and security for all deployable products. These policies provide customers with the confidence to include the SDDC product suite within their architecture and NIST 800-171 security program.

Bibliography

1. Holmes, Wade. VMware NSX Micro-segmentation Day 1. VMware Press, 2017.
   "Secure Boot for ESXi 6.5 – Hypervisor Assurance."

2. Foley, Mike. May 4, 2017. Accessed July 20, 2017.
   https://blogs.vmware.com/vsphere/2017/05/secure-boot-esxi-6-5-hypervisor-assurance.html

3. "NIST Special Publication (SP) 800-171 Revision 1."
   National Institute of Standards and Technology. December 2016. Accessed October 8, 2018.
   https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-171r1.pdf

4. "NIST Special Publication (SP) 800-53 Revision 4."
   National Institute of Standards and Technology. April 2013. Accessed July 26, 2017.
   https://doi.org/10.6028/NIST.SP.800-53r4.

5. "VMware Product Security: An Overview of VMware's Security Programs and Practices."
   VMware. Accessed July 26, 2017.
   https://www.vmware.com/content/dam/digitalmarketing/vmware/en/pdf/whitepaper/vmware-product-security-white-paper.pdf

Appendix A: NIST 800-171 Control Mapping

VMware Product	NIST 800-171 Control Families Supported
VMware NSX	AC, AU, CM, IA, IR, MA, SC, SI,
VMware vRealize Log Insight	AC, AU, CM, IA, IR, SI
VMware vRealize Network Insight	AC, AU, SC, SI
VMware vRealize Orchestration	AC, AU, CM, SC
VMware vRealize Operations	AC, AU, CM, IA, MA, SC
VMware vSAN	AC, AU, CM, IA, IR, MP, SC, SI
VMware vSphere VMware vCenter VMware ESXi VMware vSphere Replication VMware vSphere Update Manager VMware vSphere VM Encryption feature	AC, AU, CM, IA, IR, MA, MP, SC, SI
VMware Site Recovery Manager	AC, AU, IA, IR, SC
VMware Cloud Foundation	AC, AU, SC
VMware Mirage	AC, CM, IA, SC, SI
VMware AppDefense	AC, AU, CM, IA, IR, SC, SI
VMware vCloud Usage Meter	AC, AU, IA, SC,
VMware Cloud platform	AC, AU, CM, IA, IR, MA, MP, SC, SI

Appendix B: SDDC Product Capability Relationship with NIST 800-171

Product	Capability ID	Product Capability	NIST Control Family
ESXi	ESXI_001	Login attempts can be limited.	AC – Access Control
	ESXI_002	Concurrent sessions can be limited on web clients and virtual machine consoles.	AC – Access Control
	ESXI_003	ESXi can be integrated with Active Directory, or LDAP, to employ unique user identifiers, instead of using the root account.	AC – Access Control IA – Identification and Authorization
	ESXI_004	A proof of maintenance log is available to report on archived maintenance activity.	AU – Audit and Accountability
	ESXI_005	Remote access to ESXi via SSH, or the vSphere Web Client or API over HTTPS, can be configured as the secure communication protocol. Session identifiers are invalidated after session termination.	AC – Access Control
	ESXI_006	ESXi supports integration with external authentication solutions, such as Active Directory. Users that are members of a group that has been granted access to ESXi can sign in using single sign-on and will be able to log in using their user ID with elevated permissions.	AC – Access Control IA – Identification and Authorization
	ESXI_007	ESXi will perform the encryption on virtual machines that have been configured by vCenter to support VM Encryption. A third-party key manager solution is required to manage encryption keys. ESXi supports virtual machine encryption but requires a third-party integration.	MP – Media Protection
	ESXI_008	ESXi can push logs to be stored in an external log repository that supports syslog, including vRealize Log Insight. In the event vRealize Log Insight is used, it can then apply tamper protection of logging that can be used during after-the-fact investigations without altering the event logs.	AC – Access Control AU – Audit and Accountability
	ESXI_009	ESXi supports the Secure Boot feature to monitor firmware to validate version control and authorization. If the violation is detected during boot, the system will not boot up. If the violation is detected during run-time, the command will be rejected and not boot.	CM – Configuration Management IR – Incident Response
	ESXI_010	ESXi has inherent capabilities to log events and specify frequency. The richness of logging can be adjusted, and the log retention based on disk space can be enhanced, through use of a separate logging repository via syslog or vRealize Log Insight.	AC – Access Control AU – Audit and Accountability
	ESXI_011	If ESXi has Secure Boot enabled, any attempt to execute unsigned binaries will result in an alert that will be sent to the vCenter instance.	AU – Audit and Accountability IR – Incident Response
	ESXI_012	ESXi can be configured to display a login banner before granting access to the system.	AC – Access Control

	ESXI_013	ESXi provides memory safeguards to protect it from executing unauthorized code.	CM – Configuration Management SC – System and Communications SI – System and Information Integrity
	ESXI_014	ESXi limits the use of resources through resource pools, which can be constrained or prioritized based on priority.	MA – Maintenance
	ESXI_015	ESXi has the capabilities to establish firewalls using VLAN, to deny traffic by default, and to allow only explicitly designated traffic.	SC – System and Communications Protection
	ESXI_016	ESXi patching is performed via vCenter using vSphere Update Manager.	CM – Configuration Management SI – System and Information Integrity
	ESXI_017	*vSphere Hardening Guide* provides support for ESXi and vCenter hardening procedures.	CM – Configuration Management
Mirage	MIRAGE_001	Remote access to Mirage is managed via Remote Desktop Protocol (RDP) and session identifiers are terminated upon session termination.	AC – Access Control IA – Identification and Authorization
	MIRAGE_002	Session lockouts are enforceable and require users to re-authenticate after a session time-out.	AC – Access Control
	MIRAGE_003	Mirage can restrict elevated system access to a domain account, which will have access to sensitive information such as storage files, SQL database, and other sensitive information. Additional users can be created to operate the system without access to sensitive information.	AC – Access Control SC – System and Communications Protection
	MIRAGE_004	The Mirage client can be installed on devices to facilitate device management. A report of the devices and most recent remote login is available to support managing the access control List.	AC – Access Control
AppDefense	AD_001	AppDefense monitors all application endpoints within an environment utilizing its Intended State Engine (ISE), which is located in the virtualization layer. Since AppDefense is installed in the vSphere hypervisor, it is completely isolated, ensuring secure communication throughout the environment. AppDefense actively monitors endpoints within the environment for any changes to their intended state and correlates the changes via a snapshot of the endpoint to discern If the changes are permitted.	AC – Access Control CM – Configuration Management SI – System and Information Integrity
	AD_002	Access rights corresponding to AppDefense can be established through vSphere, which has the ability to prevent users from accessing AppDefense Manager due to separation from other areas.	AC – Access Control
	AD_003	The AppDefense Manager is capable of logging activity from users with root privileges via applications monitored by AppDefense. A user can configure	AC – Access Control AU – Audit and Accountability

		multiple logging methods through the AppDefense Manager.	
	AD_004	Logs and records generated through AppDefense are reliant upon functionality provided by vSphere. Event capturing can be extensively configured utilizing both the vSphere Web Client and the AppDefense Manager.	AU – Audit and Accountability CM – Configuration Management
	AD_005	Substantial storage space can be configured via vSphere and applied through the AppDefense Manager. vSphere will notify the user if storage is reaching maximum capacity and includes those environments where AppDefense is configured in.	AU – Audit and Accountability CM – Configuration Management
	AD_006	AppDefense alerts to any and all changes within the environment including auditable event failure and can be configured through its "Scopes" feature. Additional configuration can be accomplished through the vSphere Web Client.	AU – Audit and Accountability
	AD_007	AppDefense compiles event logs through its "Alarms" tab and can be reviewed at any time.	AU – Audit and Accountability CM – Configuration Management
	AD_008	AppDefense affords the user the ability to view all previous event logs at any time via the AppDefense Manager. This allows for the analysis of any questionable event.	CM – Configuration Management SI – System and Information Integrity
	AD_009	Access to AppDefense logs can be configured to only be accessible via an admin account and can be further secured by utilizing configuration setting through vSphere.	AU – Audit and Accountability CM – Configuration Management
	AD_010	AppDefense is integrated within the vSphere environment, which includes a full view of the ports and protocols in use. AppDefense includes a full list of applications and services that are currently in use. AppDefense is capable of learning the intended state of the environment and can whitelist processes accordingly through its "Learning Mode." When malicious activity is suspected within the environment, AppDefense can suspend, or completely shut down, any application and device.	CM – Configuration Management SI – System and Information Integrity
	AD_011	User identifier management is possible within the vSphere Web Client, on which AppDefense heavily relies.	AC – Access Control IA – Identification and Authorization MA – Maintenance
	AD_012	AppDefense employs the use of a continuous detection system that is capable of responsive measures when malicious actions appear to be present. AppDefense responds by suspending, shutting down, and taking a snapshot of the environment. AppDefense also utilizes a "Learning Mode" to identify the desired functionality of applications within the environment.	IR – Incident Response

	AD_013	The separation of various domains is accomplished via vSphere, with which AppDefense is integrated. User privileges are applied to each separate domain.	AC – Access Control
	AD_014	During the course of a debilitating event, AppDefense responds by isolating the threat and suspending that section of the environment. Fail-safe procedures take the form of snapshots of the environment, which can be utilized to restore functionality to compromised applications.	SC – System and Communications
	AD_015	AppDefense lies within the hypervisor of vSphere, affording it the ability to isolate various elements of applications.	CM – Configuration Management SC – System and Communications
	AD_016	Unauthorized code execution can be mitigated via AppDefense detection capabilities. If anomalies are detected within the environment, such as unauthorized code execution, AppDefense will alert and respond. AppDefense can block untrusted network protocols, resulting in a secure environment.	SI – System and Information Integrity
	AD_017	AppDefense is installed within the hypervisor of vSphere (the virtualization layer) and monitors various endpoints in the environment. These endpoints are the desirable attack vector, making this the effective area to monitor.	SI – System and Information Integrity
	AD_018	AppDefense detects any changes within the network. Any changes, such as configuration changes and suspicious anomalies, will trigger alerts that can be viewed in the AppDefense Manager.	SI – System and Information Integrity
	AD_019	Suspension of the endpoint environment can occur if AppDefense detects the use of unauthorized, executable code.	SI – System and Information Integrity
	AD_020	AppDefense can be fully automated and can issue automated responses when various anomalies are detected, such as leveraging virtualization processes like suspending and shutting down the environment.	SI – System and Information Integrity
NSX for vSphere	NSX_V_001	Information protection can be implemented using policies that restrict access information flow based on network micro-segmentation.	AC – Access Control
	NSX_V_002	Within the data plane, the guest introspection framework (host based) or Network Extensibility (redirect network flow to third-party appliances/tools) is supported by NSX, which can be accessed by third-party tools to support intrusion detection system (IDS).	SI – System and Information Integrity
	NSX_V_003	The NSX Identity Firewall feature supports Role Based Access Controls (RBAC) to limit permissions that restrict viewing virtual machines. Also, micro-segmentation can be used to manage access to specific areas of the network using RBAC and minimize attack surface.	AC – Access Control SC – System and Communications Protection
	NSX_V_004	A proof of maintenance log is available to report on archived maintenance activity. These logs are captured at key components: NSX Manager (Management Plane) and vCenter (Data Plane). For a consolidated	AU – Audit and Accountability MA – Maintenance

		view, logs can be pushed to a syslog server or vRealize Log Insight.	
	NSX_V_006	Session lockouts are enforceable and require users to re-authenticate after a session time-out.	AC – Access Control
	NSX_V_007	Account lockout threshold can be altered.	AC – Access Control
	NSX_V_008	NSX can push logs to be stored in syslog audit repositories, including vRealize Log Insight. NSX supports multiple log repository servers to enhance tamper protection of logging that can be used during after-the-fact investigations without altering the event logs.	AC – Access Control AU – Audit and Accountability
	NSX_V_009	NSX can be used to monitor the network using logging of firewalls and other traffic. This can be used to support monitoring the system for inappropriate usage and other security violations. Use of the NSX Application Rule Manager tool can monitor enforcement of access rules.	AC – Access Control AU – Audit and Accountability SI – System and Information Integrity
	NSX_V_010	NSX provides monitoring of the system, using event logs and other security logs to identify abnormal activity. The NSX NetX feature can redirect network traffic flow to be redirected to third-party intrusion detection system (IDS) solution on a per security policy.	AC – Access Control AU – Audit and Accountability
	NSX_V_011	NSX can deny access to rogue devices that have not been approved, using SpoofGuard. Also, a default deny with a list of approved devices can be established to further prevent rogue devices, including various mobile devices.	AC – Access Control CM – Configuration Management
	NSX_V_012	NSX can isolate any devices that are out of compliance and restrict their access to the network, if the device is tagged as rogue and a policy defined to isolate devices that have this tag. NSX can quarantine any devices identified as rogue devices, using the Guest Introspection framework.	AC – Access Control CM – Configuration Management
	NSX_V_013	NSX can use micro-segmentation to establish processing domains based on access rights and user privileges. Granularity around trust can be defined as a virtual NIC, or more broadly as a region, for both static infrastructure and dynamic logical objects.	AC – Access Control
	NSX_V_014	NSX can restrict network traffic based on system security classification, which can be defined using static objects and dynamic objects. Access control for objects can be restricted based on security rules and tags.	AC – Access Control
	NSX_V_015	Network access controls can be managed using NSX, which can also be integrated with third-party tools to support managing network access.	AC – Access Control
	NSX_V_016	Using NetX API, NSX can support integration with third-party intrusion detection systems (IDS) to support responses in network locations or granular to VM/workflow between VMs. In addition, NSX can use Guest Introspection to further enhance IDS responses.	AC – Access Control IR – Incident Response SI – System and Information Integrity
	NSX_V_017	NSX can manage all internal network connections and provides documentation to describe the networking components available for deployment.	AC – Access Control SI – System and Information Integrity

	NSX_V_018	NSX can manage external network connections through the NSX Edge gateway, firewall, VPN, or SSL through Load Balancer. This includes establishing a boundary defense.	AC – Access Control SC – System and Communications Protection SI – System and Information Integrity
	NSX_V_019	Using the NSX Edge firewall, distributed firewall, Guest Introspection (within the VM), and third-party NetX API (network enforcement), NSX can prohibit systems from connecting directly to external networks.	AC – Access Control SI – System and Information Integrity
	NSX_V_020	NSX can be implemented with a fault-tolerant architecture; documentation supporting this design is available.	SC – System and Communications Protection
	NSX_V_021	NSX can restrict inbound Internet traffic inside the DMZ using ESG FW, distributed firewall, and the principles of DMZ Anywhere.	SC – System and Communications Protection
	NSX_V_022	All capabilities of NSX can be programmatically created by Rest API to segregate applications and databases that can restrict information in an internal network zone.	AC – Access Control SC – System and Communications Protection
	NSX_V_023	NSX can apply configuration standards and remove unnecessary functionality using Rest API, Guest Introspection, and distributed firewall specifically to protocols, ports, applications, and services in the firewall and router configuration standard.	AC – Access Control
	NSX_V_024	NSX can be used to configure traffic including firewall deny all traffic by default, explicit exceptions for designated traffic, restricting outbound traffic, protecting devices from outbound connections, protecting devices to deny inbound connections, managing IP addresses in DHCP, assigning or reserving static IP addresses in DHCP.	AC – Access Control SC – System and Communications Protection -
	NSX_V_025	NSX can leverage a Root Certification Authority to support Public Key Infrastructure within the virtualized network platform.	SC – System and Communications Protection
	NSX_V_026	NSX can support analytics to be used with third-party solutions to identify behavior and characterize malicious code, which would be supported via Guest Introspection.	MA – Maintenance SI – System and Information Integrity
	NSX_V_027	In the event of fail-safe procedures, NSX can move around machines to other recovery networks via automated quarantine actions.	IR – Incident Response
	NSX_V_028	NSX provides a dashboard to monitor the platform's health, which can inform users around maintenance information of the platform itself.	IR – Incident Response
	NSX_V_029	NSX can be configured to protect against unauthorized data mining of the NSX vFabric Postgres database.	AC – Access Control
	NSX_V_030	NSX includes some Denial of Service (DoS) attack prevention mechanisms, which may support detection processes but will not monitor and detect DoS before the attack occurs.	SC – System and Communications Protection

	NSX_V_031	NSX provides stateful firewall capabilities that can support adding devices requiring access control based on an access control List.	AC – Access Control SC – System and Communications Protection
	NSX_V_032	NSX supports least privilege around workloads and provides four different roles within NSX to support the principle of least privilege (enterprise administrator, NSX administrator, security administrator, and auditor/read only).	AC – Access Control
	NSX_V_033	NSX can be architected to place firewalls between security domains, DMZ, and other network zones.	SC – System and Communications
	NSX_V_035	The NSX appliance provides access via SSH, which can also be disabled. Access control to the NSX appliances can enforce password parameters, including length, requiring password change upon first login, and account lockout duration.	IA – Identification and Authorization
	NSX_V_036	NSX provides and maintains a system hardening guide.	CM – Configuration Management
SDDC Manager Cloud Foundation	SDDCMANAGE RVCF_001	A proof of maintenance log is available to report on archived maintenance activity related to ESXi, vCenter, vSAN, and NSX products within the Cloud Foundation suite. Access pertaining to these records can be limited to only authorized individuals.	AU – Audit and Accountability
	SDDCMANAGE RVCF_002	SDDC Manager supports two types of users: Read Only and Cloud Admin. User accounts can be managed within SDDC Manager and external user authentication services such as Active Directory.	AC – Access Control SC – System and Communications Protection
	SDDCMANAGE RVCF_003	Session lockouts are enforceable and require users to re-authenticate after a session time-out.	AC– Access Control
	SDDCMANAGE RVCF_004	SDDC Manager enables security architecture design through the separation of the Management Domain and the Workload Domain. Designing a separation of architecture can support segregation of duties and keep environments separate based on function.	AC – Access Control SC – System and Communications Protection
	SDDCMANAGER VCF_005	SDDC Manager includes configuration guidance for top-of-rack switches to ensure that communication within the environments is properly established. Hosts of VM clusters and communication across network traffic between the data center (internally and externally) can be impacted by this design.	AC – Access Control CM – Configuration Management
Site Recovery Manager	SRM_001	Recovery can be included in simulated events as part of the larger continuity plan training. The simulated failover can be triggered manually. In addition, tier systems can be prioritized or omitted through the use of consistency groups (high impact versus low impact).	IR – Incident Response
	SRM_002	Site Recovery Manager can push logs to be stored in vRealize Log Insight. A content pack is provided to facilitate Site Recovery Manager logging and dashboard visualization of logging.	AU – Audit and Accountability
	SRM_003	Results of test run can be included in documentation to evidence results of continuity planning exercises. Recovery mode can be run within the test plan and	AU – Audit and Accountability IR – Incident Response

		export the results to showcase the outcome of every test run inside test mode.	
	SRM_004	Site Recovery Manager can execute fail-safe procedures if initiated manually or via an API call. Additionally, if the source site is unavailable, then automatic fail-over will occur.	SC – System and Communications Protection
	SRM_005	Site Recovery Manager is an application that runs in Windows and relies on events and standard maintenance logs provided by Windows. Proof of maintenance and archival of reports depends on configuration of Windows event logging.	AU – Audit and Accountability
	SRM_007	Remote access is possible via Remote Desktop Protocol (RDP) to the Site Recovery Manager system. This can be managed through external authentication solutions. Use of Site Recovery Manager does not require RDP access mechanism and RDP is usually allocated for administrative access only.	AC – Access Control
	SRM_008	Site Recovery Manager relies on vCenter to manage assigned user access and manage user accounts, including assignment of roles to restrict functionality.	AC – Access Control SC – System and Communications Protection
	SRM_009	Site Recovery Manager can be configured to use Active Directory or vSphere domain accounts that adhere to organizational password standards, including forcing users to change their password upon first login.	IA – Identification and Authorization
vCloud Usage Meter	UM_001	Proxy configuration is available during the initial setup of vCloud Usage Meter and also features full LDAP configuration.	AC – Access Control
	UM_002	vCloud Usage Meter retains a list of connections that are the subject of monitoring and usage collection. vCloud Usage Meter is installed within the vSphere environment, which is capable of full LDAP integration where user accounts can be controlled even further.	AC – Access Control
	UM_003	vSphere logs user activity and can be maintained for a set period of time. These logs can be secured via various methods, such as user account permissions.	AU – Audit and Accountability
	UM_004	Users can be uniquely identified through different aspects via the vSphere Web Client, as well as various methods derived from LDAP integration and configuration.	AC – Access Control IA – Identification and Authorization
	UM_005	vCloud Usage Meter can be configured to utilize proxy services, in addition to leveraging LDAP integration to manage user IDs and passwords within a secure environment. This includes configuring the minimum and maximum password ages that can be applied to user accounts.	IA – Identification and Authorization
	UM_006	Any and all maintenance tools are controlled and monitored through the vSphere Web Client, with which vCloud Usage Meter is integrated.	SC – System and Communications Protection
	UM_007	LDAP and various parameters derived from the vSphere Web Client can be employed to maintain separation between user functionality and system management.	AC – Access Control SC – System and Communications Protection

	UM_008	Data transmissions can be secured through proxy configurations and are employed during the initial setup of vCloud Usage Meter.	SC – System and Communications Protection
vCloud Director	vCD_001	vCloud Director has the ability to administrate user accounts, in addition to assigning those accounts various permissions, through the Administration Home Page and LDAP integration. Account management can also be accomplished through the vCloud API.	AC – Access Control
	vCD_002	Permissions pertaining to non-privileged users can be configured in such a manner as to prevent the execution of various functions.	AC – Access Control AU – Audit and Accountability
	vCD_003	Session lock capabilities can be employed, such as configuring the number of invalid logins before lockout occurs, through the vCloud Director Administration portal and also within the General System Settings.	AC – Access Control
	vCD_004	Configuring devices and accounts that have access control permissions can be accomplished through the vCloud Director Administration portal, as well as through the NSX Manager.	AC – Access Control IA – Identification and Authorization
	vCD_005	System Administrator account permissions cannot be altered and encompass all existing rights, in addition to rights only associated with an Administrator role.	AC – Access Control
	vCD_006	An administrator account associated with vCloud Director has the capability of managing the access authorization list and is the only account that can do so.	AC – Access Control
	vCD_007	vCloud Director includes monitoring functionality, which can produce audit logs to provide insight regarding the overall statistics of the environment.	AU – Audit and Accountability
	vCD_008	The administrator account associated with vCloud Director can fully manage user accounts, including properly updating accounts and their access rights.	AC – Access Control
	vCD_009	The vCloud Director environment provides vCloud Director multi-tenancy capabilities, isolation of tenants and sub-tenants, and logically isolated switches. These features enforce logical separation between information flows.	AC – Access Control AU – Audit and Accountability
	vCD_010	vCloud Director has the ability to monitor all assets within its environment, as well as produce reports that can later be utilized during forensic analysis. Logging capabilities are configured, and observed, through the vCloud Director manage and monitor portals.	AU – Audit and Accountability
	vCD_011	Authentication measures are handled through the vSphere environment, of which vCloud Director is a part.	AC – Access Control IA – Identification and Authorization
	vCD_012	vCloud Director can be coupled with vCloud Director Availability to ensure proper contingency functionality within the vCloud Director environment, as well as other facets of the vSphere environment.	SC – System and Communications Protection
	vCD_013	AppDefense can be integrated into the vSphere environment, on which vCloud Director relies, to establish and maintain intrusion detection functionality.	IR – Incident Response

	vCD_014	AppDefense can be integrated into the vSphere environment, on which vCloud Director relies, to implement and maintain incident management functionality.	IR – Incident Response
	vCD_015	Intrusion detection procedures can be implemented within the vSphere environment, with which vCloud Director is integrated, through the addition of AppDefense.	IR – Incident Response
	vCD_016	vCloud Director is responsible for tethering various cloud environments together, one of which can provide customer service business functionalities.	IR – Incident Response
	vCD_017	An Incident Response program can be established within one of the cloud environments that vCloud Director is responsible for managing. Users are able to review and update the incident response procedures following the closure of such an event while utilizing features afforded through AppDefense to vSphere, which encompasses vCloud Director.	IR – Incident Response
	vCD_018	While utilizing AppDefense within the vSphere environment, which contains vCloud Director, a user is afforded the ability of establishing and maintaining various incident response procedures.	IR – Incident Response
vCloud Availability for vCloud Director	VCA_001	vCloud Availability for vCloud Director is integrated with vCloud Director, which is installed in the vSphere environment. In turn, users that are currently using vCloud Availability for vCloud Director services are subject to the termination of their session if idle for too long.	AC – Access Control SC – System and Communications
	VCA_002	It is possible to limit superuser accounts to designated system administrators, if using LDAP through vSphere.	AC – Access Control CM – Configuration Management SC – System and Communications
	VCA_003	Account lockout procedures can be configured by the use of LDAP services, which can be indirectly used in conjunction with vCloud Availability for vCloud Director. The procedures that can be configured are account lockout threshold and duration, in addition to the set number of consecutive login attempts before such procedures are triggered.	AC – Access Control
	VCA_004	vSphere has its own internal log management processes that can be utilized via any user, with applicable permissions, of vCloud Director Availability. Logging mechanisms within the vSphere environment can be configured and can be used for later analysis. Actions derived from a user can be traced back to them within the vSphere environment.	AC – Access Control CM – Configuration Management SC – System and Communications
	VCA_005	The policy engine allows monitoring and event generation to react to changing conditions in the vRealize Orchestrator or plugged-in technology.	AU – Audit and Accountability

	VCA_006	Event logs stemming from the vSphere environment, of which vCloud Director Availability is a part, can be stored securely and protected from unauthorized access.	IA – Identification and Authentication
	VCA_007	A complete network overview can be reviewed via vSphere. This includes any ports, protocols, and services that are currently active within the environment.	AU – Audit and Accountability
	VCA_008	When utilizing LDAP integration within the vSphere environment, uniquely identifying properties can be employed to user accounts. This includes those who have access to vCloud Director Availability through vSphere.	IA – Identification and Authentication
	VCA_009	Proxy measures can be implemented within the vSphere environment, in turn affecting vCloud Director Availability, and can be configured to only allow access to properly identified and authenticated connections.	AC – Access Control IA – Identification and Authentication SC – System and Communications
	VCA_010	The "Enable Password History" feature can be enabled via the vSphere Web Client, or through LDAP integration, and affects vCloud Director Availability services due to access being derived through vSphere.	IA – Identification and Authentication
	VCA_011	Various password settings can be configured through LDAP, which indirectly affects vCloud Director Availability services.	AC – Access Control
	VCA_012	System management is accomplished through the vSphere Web Client, which is completely separate from vCloud Director. vCloud Director governs services such as that of vCloud Director Availability.	AC – Access Control MA – Maintenance SC – System and Communications Protection
	VCA_013	Fall-back procedures and services are provided via vCloud Director Availability in the event of catastrophic failure of an environment through the use of various virtual machine replications.	SC – System and Communications Protection
	VCA_014	User privileges are dictated through configurations stemming from either vSphere or LDAP integration, all of which affect vCloud Director Availability due to being deeply entangled with vSphere through vCloud Director.	AC – Access Control SC – System and Communications Protection
vCloud Director Extender	vCDX_001	vCloud Director Extender is a plug-in for vCloud Director, which is inherently integrated within the vSphere environment. vSphere is capable of establishing various access rights to the user through the vSphere Web Client.	AC – Access Control
	vCDX_002	Various roles and accounts can be configured through the vCloud Director Web Client, which can be passed through to vCloud Director Extender.	AC – Access Control
	vCDX_003	The capturing of logs can be accomplished through the vCloud Director portal, as well as the vSphere Web Client. Actions taken by a user with root privileges can be detailed within the vSphere Web Client.	AU – Audit and Accountability

	vCDX_004	Account lockout procedures can be configured via LDAP integration with vCloud Director, which passes through to vCloud Director Extender.	AC – Access Control
	vCDX_005	vCloud Director Extender retains information regarding all previously performed virtual machine migrations performed by vCloud Director Extender.	AU – Audit and Accountability
	vCDX_006	The preservation of logs can be accomplished through log4j configuration.	AU – Audit and Accountability
	vCDX_007	A list detailing the network configuration can be viewed within the vSphere Web Client, in which vCloud Director Extender resides.	CM – Configuration Management
	vCDX_008	vCloud Director Extender is innately a part of the vSphere environment, which has the ability to enforce uniquely identifying properties to various users.	SC – System and Communications Protection
	vCDX_009	The enforcement of password history requirements can be accomplished through LDAP integration, which can be successfully accomplished within the environment.	IA – Identification and Authentication
	vCDX_010	vSphere can be successfully integrated with LDAP, which enables the options of configuring minimum and maximum password age standards for its users. vCloud Director Extender will inherit these properties due to its deep integration with vSphere via vCloud Director.	IA – Identification and Authentication
	vCDX_011	vCloud Director Extender employs the use of the Replicator, which provides the data transfer and monitoring, to protect data with encrypted TCP traffic during a virtual machine migration.	MP– Media Protection SC – System and Communications Protection
vCenter	VCENTER_001	vCenter supports access control configuration including session time-out, login attempts, account lockout threshold, account lockout duration, minimum password age, and requiring re-authentication.	AC – Access Control IA – Identification and Authorization
	VCENTER_002	Concurrent sessions can be limited on web clients and virtual machine consoles.	AC – Access Control
	VCENTER_003	vCenter employs unique user identifiers through a Platform Services Controller instance, which manages integration with SSO. Unique user identifiers can be assigned using a Platform Services Controller instance.	AC – Access Control IA – Identification and Authorization
	VCENTER_004	Access is supported using Role Based Access Control (RBAC) through local operating system access control, or integration with Active Directory and federated services. vCenter access control is established through permissions, which are assigned by a combination of roles and privileges. Users are assigned to roles. Privileges are assigned to roles. Thus, access authorization is a combination of the role a user is assigned and the privilege a role is assigned.	AC – Access Control IA – Identification and Authorization
	VCENTER_005	Assignment of elevated privileges can be restricted to only those users that are approved as designated system administrators.	AC – Access Control
	VCENTER_006	vCenter can support an organization's continuity plan by providing workload management in the event of a	SA – Security Assessment

		host system disruption. However, this capability is not a robust continuity planning solution.	
	VCENTER_007	vCenter can list all the virtual machines and support creating an inventory of technology systems.	CM – Configuration Management
	VCENTER_008	Remote access to vCenter via SSH, or the vSphere Web Client or API over HTTPS, can be configured as the secure communication protocol. For the VMware vCenter Server Appliance™, it runs on Linux and can be restricted to accept only HTTPS. Session identifiers are invalidated after session termination.	SC – System and Communications Protection
	VCENTER_009	vCenter can be configured to log out inactive sessions. By default, inactivity is set to log out after 15 minutes.	AC – Access Control
	VCENTER_010	vCenter can configure encryption parameter designation on a VM-by-VM basis. ESXi performs the actual encryption on the VM. Third-party key manager solution is required for encryption key management.	SC – System and Communications Protection
	VCENTER_011	vCenter can push logs to be stored in an external log repository that supports syslog, including vRealize Log Insight. In the event vRealize Log Insight is used, it can then apply tamper protection of logging that can be used during after-the-fact investigations without altering the event logs.	AC – Access Control AU – Audit and Accountability
	VCENTER_012	vCenter supports monitoring a set of standardized settings to monitor, which may indicate inappropriate usage or security violations. Alarms and alerts can be configured to notify users via email when triggered.	CM – Configuration Management SI – System and Information Integrity
	VCENTER_013	vCenter has inherent capabilities to log events and specify frequency. The richness of logging can be adjusted and the log retention based on disk space can be enhanced through use of a separate logging repository via syslog, or vRealize Log Insight.	AC – Access Control AU – Audit and Accountability
	VCENTER_014	vCenter can be configured to display a login banner to users before granting access to the system.	AC – Access Control
	VCENTER_015	vCenter supports enhanced logging of audit level events to support third-party integration with tools such as Introduction Detection Systems (IDS).	AC – Access Control AU – Audit and Accountability SI – System and Information Integrity
	VCENTER_016	vCenter has granular access control permissions that can be applied to virtual machines, VM clusters, and hosts. An organization can define the roles that can access these systems, such as bifurcating access between developers and production environments.	AC – Access Control
	VCENTER_017	Resources can be limited based on priority using pools, VMware vSphere Storage I/O Control, VMware vSphere Network I/O Control, or VMware vSphere Distributed Resource Scheduler™ (vSphere DRS) reservation.	MA – Maintenance
	VCENTER_018	vCenter can be run on a Linux appliance that is configured to restrict network traffic through use of a software firewall, which is restricted to only necessary ports during the installation. However, if vCenter is run on a Windows appliance, the network traffic and firewall is inherited based on the user's configuration of the Windows appliance.	AC – Access Control SC – System and Communications Protection

	VCENTER_019	vCenter can manage the encryption of virtual machines (applying encryption or removing encryption) and matching keys using a third-party key management solution.	CM – Configuration Management SC – System and Communications Protection
	VCENTER_020	vCenter can push audit trail logs to be archived in an external log repository that supports syslog, including vRealize Log Insight.	AU – Audit and Accountability
	VCENTER_021	vCenter can patch ESXi hosts through vSphere Update Manager.	CM – Configuration Management SI – System and Information Integrity
	VCENTER_022	vCenter can facilitate installation of critical security updates for ESXi. vSphere Update Manager alerts vCenter of any firmware issues that affect ESXi and can be used to install patches and also automate installation of updates. vCenter has a manual feature to check to see if there are any updates available for vCenter without specifying the nature of the update (security or operational).	CM – Configuration Management SI – System and Information Integrity
	VCENTER_023	*vSphere Hardening Guide* provides support for ESXi and vCenter hardening procedures.	CM – Configuration Management
vRealize Configuration Manager	VCM_001	A proof of maintenance log is available to report on archived maintenance activity, where access limitations can also be configured.	MA – Maintenance
	VCM_002	vRealize Configuration Manager can be accessed remotely via a web browser, or it can be launched from a Windows machine that has it installed whereby a user can SSH directly into the machine and secure remote access in this manner. Session identifiers are invalidated upon session termination.	AC – Access Control
	VCM_003	Session lockouts are enforceable and require users to re-authenticate after a session time-out.	AC – Access Control
	VCM_004	vRealize Configuration Manager supports user management, including user names and user roles. These user accounts can be reviewed for access control management.	AC – Access Control PS – Personnel Security SC – System and Communications Protection
	VCM_005	vRealize Configuration Manager can restrict access to system information, data, and actions based on assigned user roles.	AC – Access Control
	VCM_006	vRealize Configuration Manager can install agents on to endpoints (Windows, Linux, and vSphere Managing Agents on Windows) to collect data from vSphere in support of configuration management. Compliance packs can be installed to produce reports to support a risk management program.	CM – Configuration Management
vRealize Automation	VRA_001	Security and protection software can be installed using NSX Rest API and Guest Introspection.	SI – System and Information Integrity
	VRA_002	A proof of maintenance log is available to report on archived maintenance activity.	AU – Audit and Accountability

	VRA_003	Remote access to products can be restricted to just SSH or other desired and secure communication protocols. Manually the configuration files can be altered in vSphere to further restrict access to vSphere. This includes controlling remote access through an existing access control and authentication solution and invalidating session identifiers upon session termination.	SC – System and Communications Protection
	VRA_004	Unnecessary system functionality can be configured by using vRealize Automation to disable unwanted Service Catalog template items by default.	CM – Configuration Management
	VRA_005	vRealize Automation can push logs to syslog-supported logging solutions or vRealize Log Insight. vRealize Log Insight can then apply tamper protection of logging that can be used during after-the-fact investigations without altering the event logs.	AU – Audit and Accountability
	VRA_006	vRealize Automation can provide configuration management input to an asset inventory database using third-party tools. This includes adding devices to the access control list, recording the owner for applicable assets, and maintaining an asset inventory database. vRealize Orchestrator can update a control management database updating assets but does not create the database itself.	CM – Configuration Management
	VRA_007	vRealize Automation can restrict settings and services for new infrastructure and virtual machines created through the portal, which could by default launch secure, pre-defined virtual instances.	CM – Configuration Management
	VRA_008	vRealize Automation supports multiple roles to separate user functionality from system management functionality, as well as the capability to support the principle of least privilege user access control.	AC – Access Control SC – System and Communications Protection
	VRA_009	vRealize Automation can automate log capturing and transmission to logging solutions.	AC – Access Control AU – Audit and Accountability
	VRLI_002	A proof of maintenance log is available to report on archived maintenance activity.	CM – Configuration Management
	VRLI_003	Session lockouts are enforceable and require users to re-authenticate after a session time-out.	AC – Access Control
	VRLI_004	Search queries can be configured to monitor the system for inappropriate usage, security violations, and other defined events. Monitoring tools include alerts and dashboards. Dashboards and Interactive Analytics are provided out of the box.	AC – Access Control AU – Audit and Accountability SI – System and Information Integrity
	VRLI_005	vRealize Log Insight supports standard syslog and secure syslog. In addition, when using an internal vRealize Log Insight agent, a secure, encrypted protocol is enforceable.	AU – Audit and Accountability
	VRLI_006	Audit Dashboard is provided to analyze log data and support after-the-fact investigations. In addition, vRealize Log Insight can provide tamper protection by deploying a log system architecture configured to	AC – Access Control AU – Audit and Accountability IR – Incident Response

		support multiple storage locations to minimize the risk of a capacity limitation.	
	VRLI_007	vRealize Log Insight can gather event logs across any device within the virtualized or physical environment. Log data is stored in a centralized database. The logging database can be used to correlate system-wide audit trails. Security-related queries, dashboards, and alerts use time stamps to support event log correlation.	AC – Access Control AU – Audit and Accountability
	VRLI_008	vRealize Log Insight has a dashboard export feature to help distribute logs. In addition, a read-only view is available for designated users to log in and view the reports.	AU – Audit and Accountability
	VRLI_009	Logging uses the First in First out (FIFO) mechanism to avoid overwriting logs. If system capacity is reached, users are prompted to archive older log data. Users can define the retention policy.	AU – Audit and Accountability
	VRLI_010	Backups of logs can be performed for all products using vRealize Log Insight. Remote archival of vRealize Log Insight logging data is supported.	AU – Audit and Accountability
	VRLI_011	Hosts can use a vRealize Log Insight agent or send logs via syslog to the centralized vRealize Log Insight log database to manage storage and retention and to protect logs from unauthorized activity.	AC – Access Control AU – Audit and Accountability
	VRLI_012	Remote access to vRealize Log Insight is by default set to HTTPS. Session identifiers are discarded upon session termination.	AC – Access Control SC – System and Communications
	VRLI_013	vRealize Log Insight allows access control settings to be configured to manage sessions, including the following parameters: account lockout threshold, account lockout duration, and password policies. vRealize Log Insight can integrate authentication with Platform Services Controller to enable enforcement of authentication parameters from Active Directory directly.	AC – Access Control IA – Identification and Authorization
	VRLI_014	vRealize Log Insight provides management of user accounts through the access control panel, including managing users configured locally, as well as accounts created through an external authentication solution.	AC – Access Control
	VRLI_015	vRealize Log Insight allows users to be assigned to roles. The roles can be assigned granular access based on the organization's assignment of least privilege or job responsibilities within the groups. VMware Identity Manager™ or an external authentication solution is required to administer.	AC – Access Control SC – System and Communications Protection
	VRLI_016	vRealize Log Insight can manage an access control List via agent and host listings to manage devices, as well as restricting the logs a device can access. Role-based access can limit access to specific log devices and log data.	AC – Access Control AU – Audit and Accountability
	VRLI_017	If local accounts are created in vRealize Log Insight, users can be required to change their password upon first login.	IA – Identification and Authorization
	VRLI_019	vRealize Log Insight collects logs in real time. Content packs to enhance dashboards and provide custom queries tailored to many VMware products.	AC – Access Control AU – Audit and Accountability

			IR – Incident Response
vRealize Network Insight	VRNI_001	vRealize Network Insight receives NetFlow from VMware vSphere Distributed Switch™ (VDS) instances, which connect virtual machines. This can be used to monitor information flows and network flows.	SC – System and Communications
	VRNI_002	A proof of maintenance log is available to report on archived maintenance activity.	AU – Audit and Accountability
	VRNI_003	Remote access to administrative features can be restricted to just SSH or to other desired and secure communication protocols. Manually, the configuration files can be altered in vRealize Network Insight to further restrict access to vSphere. This includes controlling remote access through an existing access control and authentication solution and invalidating session identifiers upon session termination.	AC – Access Control
	VRNI_004	Authorization regarding remotely executed, privileged commands, as well as access, can be configured per user.	AC – Access Control
	VRNI_005	vRealize Network Insight can push logs to syslog, or vRealize Network Insight. vRealize Network Insight can then apply tamper protection of logging that can be used during after-the-fact investigations without altering the event logs.	AC – Access Control AU – Audit and Accountability
	VRNI_006	vRealize Network Insight can be used to monitor data center traffic and provide visibility to support monitoring activities.	SI – System and Information Integrity
	VRNI_007	vRealize Network Insight can be used to review network paths and troubleshoot components that are not communicating properly such as a web server not reaching a database. This feature can also help in establishing distributed firewalls.	SC – System and Communications Protection SI – System and Information Integrity
	VRNI_009	vRealize Network Insight can provide visibility into the information flow, including information flow insight for managing policies of the system and between interconnected systems.	AU – Audit and Accountability
	VRNI_010	The vRealize Network Insight administrator can manage User Interface (UI) users. Users connect via a Web Portal UI. These user accounts can be reviewed, access control can be managed using roles (administrator or read-only member user), and password complexity can be configured.	AC – Access Control SC – System and Communications Protection
	VRNI_011	vRealize Network Insight traffic between the platform and proxy servers can be encrypted using certificates.	SC – System and Communications
vRealize Orchestrator	VRO_001	Remote access to products can be restricted to just SSH or to other desired and secure communication protocols. Manually, the configuration files can be altered in vSphere to further restrict access to vSphere. This includes controlling remote access through an existing access control and authentication solution and invalidating session identifiers upon session termination.	AC – Access Control
	VRO_002	vRealize Orchestrator can provide user information responsible for creating or modifying the virtual	AU – Audit and Accountability

		machine, virtual infrastructure asset information, or other information. This can be used to trace ownership, if the creation or modification is appropriate.	CM – Configuration Management
	VRO_003	A proof of maintenance log is available to report on archived maintenance activity.	AU – Audit and Accountability
	VRO_004	vRealize Orchestrator supports multiple roles to separate user functionality from system management functionality, as well as the capability to support the principle of least privilege user access control.	SC – System and Communications Protection
vRealize Operations	VROPS_001	A proof of maintenance log is available to report on archived maintenance activity.	MA – Maintenance
	VROPS_002	Remote access to vRealize Operations is restricted by default. vRealize Operations appliance remote access can only be enabled to use SSH via the vCenter VM Console. vRealize Operations user interface is only accessible via a secure URL. Upon session termination, session identifiers are invalidated.	AC – Access Control
	VROPS_003	Session lockouts are enforced by default and require users to re-authenticate after a session time-out.	AC – Access Control
	VROPS_004	Using a management pack specific to the compliance area (PCI and HIPAA only at this time), vRealize Operations can be used to support a configuration management program. The content pack relies on vSphere to evaluate technical configurations and settings based on the compliance pack's baseline.	CM – Configuration Management
	VROPS_005	vRealize Operations has a maximum of concurrent sessions (6); this setting cannot be altered.	AC – Access Control CM – Configuration Management
	VROPS_006	Using a management pack, vRealize Operations can store information that is collected by agents via the use of plug-ins to collect data from guest Operating Systems running in virtual machines.	CM – Configuration Management
	VROPS_007	vRealize Operations can perform capacity planning, forecasting, and reporting. An input into this planning process can include comparing capacity between production and backup sites.	SI – System and Information Integrity
	VROPS_008	Initial login with the root account requires users to change the password. New users logging in for the first time can also be required to change their password upon initial login.	IA – Identification and Authorization
	VROPS_009	vRealize Operations can monitor the storage of vSAN (or another database) and upon running low, it can provide an alert and recommendation to adjust the storage capacity. The storage capacity data and alerts can be archived to support retaining records in accordance with compliance requirements.	AU – Audit and Accountability,
	VROPS_010	vRealize Operations can be configured to support account lockout duration, number of failed attempts, and password length and complexity.	AC – Access Control IA – Identification and Authorization
	VROPS_011	vRealize Operations can push audit trail logs to be archived in an external log repository that supports syslog, including vRealize Log Insight.	AU – Audit and Accountability
	VROPS_012	vRealize Operations permits creating roles and groups using Role Based Access Control (RBAC). Granularity	AC – Access Control

		can be applied to view or edit objects, run reports, and other functionality.	SC – System and Communications Protection
	VROPS_013	vRealize Operations provides metrics and system performance reports that users can compare against organizational standards or industry benchmarks. The metrics include capacity planning, virtual machine sizing, and behavioral analysis.	CM – Configuration Management
vSAN	vSAN_001	Access to data storage in vSAN is managed by roles within vCenter. vSAN 6.5 introduced a new role to manage enabling/disabling encryption that can be further applied to restrict non-cryptographic user access to configuration of this feature.	AC – Access Control IA – Identification and Authorization SC – System and Communications Protection
	vSAN_002	Logging capabilities can be enabled and customized to capture event information.	AC – Access Control AU – Audit and Accountability
	vSAN_003	Logging can be synchronized to system clocks (NTP) and capture a date and time stamp.	AU – Audit and Accountability
	vSAN_004	vSAN can push logs to be stored in vRealize Log Insight. A default vSAN dashboard is available in vRealize Log Insight as a content pack.	AC – Access Control AU – Audit and Accountability
	vSAN_005	Session lockouts are enforceable and require users to re-authenticate after a session time-out, which are controlled by vCenter or ESXi.	AC – Access Control
	vSAN_006	Encryption at rest can be performed for objects residing on the vSAN datastore (both in cache and long-term capacity storage media). However, a third-party key manager will be required to store and rotate keys.	MP – Media Protection SC – System and Communications Protection
	vSAN_007	vSAN can be patched via the vSphere Update Manager patching capabilities of vCenter. In addition, vSAN 6.6 has the ability to patch firmware controller drivers for participating vendors.	CM – Configuration Management IR – Incident Response SI – System and Information Integrity
	vSAN_008	Maintenance activity is logged and can be accessed via reports, which can be archived for historical reference. The maintenance logging information is captured at each component vCenter, ESXi, and vSAN instance, which can be holistically analyzed via vRealize Log Insight or customized.	AU – Audit and Accountability CM – Configuration Management
	vSAN_009	Overall storage size can be adjusted to prevent exceeding capacity, including space allocated for logs. This can be adjusted by adding physical devices or adding vSphere hosts, without a limit to file or block storage size.	AU – Audit and Accountability CM – Configuration Management
	vSAN_010	Cryptographic management features supported include rotation of keys via User Interface or API integration, changing Key Manage System (KMS) providers, and broadly enabling or disabling encryption. These	SC – System and Communications Protection

		capabilities can be used to support cryptographic procedures.	
	vSAN_011	vSAN utilization of public key infrastructure can be controlled by the RBAC capability of vCenter. Granular control can be provided or removed through the use of specific role-based permissions.	CM – Configuration Management
vSphere Replication	VSPHEREREPLICATION_001	Replication of virtual machine object and its data can be used to support continuity planning and provide a virtualization technology alternative to off-site vSphere environment storage using electronic media.	MP – Media Protection
	VSPHEREREPLICATION_002	vSphere Replication supports geographical separation through use of vSphere replicated infrastructure to provide timely and effective recovery operations.	MP – Media Protection
	VSPHEREREPLICATION_003	vSphere Replication integrates with Site Recovery Manager to enable mitigation during an outage or disruption.	MP – Media Protection
	VSPHEREREPLICATION_004	Recovery policies can be set up to specified Recovery Point Objectives (RPO), which can be selected from a range of 15 minutes to 24 hours. vSphere Replication (6.5) can be reduced to a period as short as 5 minutes and up to 24 hours.	MP – Media Protection

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.

For more information on VMware security, visit security.vmware.com.

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