TEVORA™

VMware®

Whitepaper on Cybersecurity Maturity Model Certification (CMMC)

Kaitlyn Bestenheider

September 28th, 2020

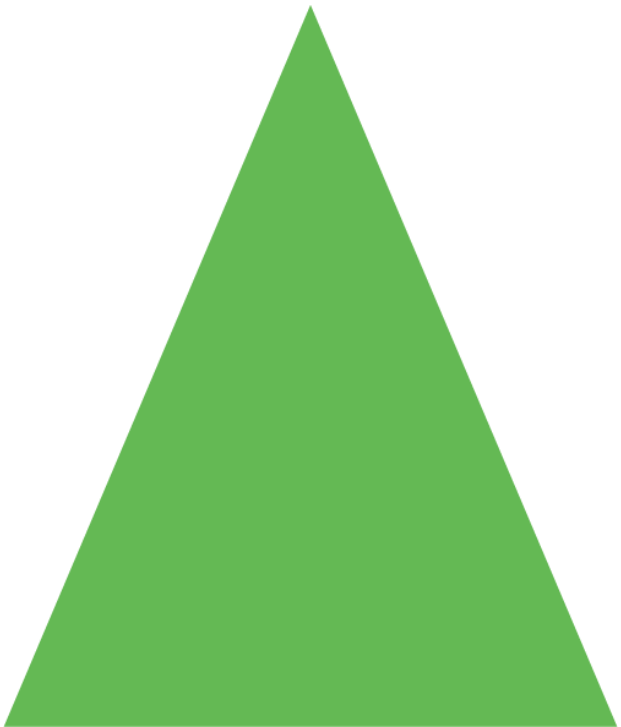

Table of Contents

Design Subject Matter Experts

The following people provided key input on this whitepaper.

Name	Role / Comments	Contact
Kaitlyn Bestenheider	Co-Author	kbestenheider@tevora.com
Jeremiah Sahlberg	Managing Director – Federal, Tevora	jsahlberg@tevora.com
Carlos Phoenix	Global Cyber Strategist, VMware	cphoenix1@vmware.com

Trademarks & Intellectual Property Notices

Solution Area	Key Products
Software-Defined Compute	VMware ESXi™, VMware vCenter®, VMware Cloud Foundation™, VMware vSAN™, VMware vCloud Director®, VMware vCloud Director Extender, VMware vCloud ® Usage Meter
Software-Defined Networking	VMware NSX®, VMware NSXT®
Management and Automation	VMware vRealize® Network Insight™, VMware vRealize Automation™, VMware vRealize Orchestrator™, VMware vRealize Log Insight™, VMware vRealize Operations Manager™, VMware AppDefense™, VMware Identity Manager™
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 Cybersecurity Maturity Model Certification (CMMC) 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 Cybersecurity Maturity Model (CMMC) document will provide an initial evaluation of VMware products that make up and support a Software-Defined Data Center (SDDC), and how they may support the CMMC 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 an SDDC. The VMware Compliance Solutions team developed a framework that incorporates SDDC product capabilities aligned to CMMC controls. The product capabilities and framework of this document use NIST 800-171 as their foundational security framework to create a series of standards. These standards are then used to illustrate how VMware products and their capabilities apply to other industry frameworks such as NIST 800-53, PCI DSS, and CMMC.

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

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 document will navigate readers through the CMMC standard and highlight applicable VMware product capabilities.

VMware and CMMC

Today's infrastructure is complex. VMware products aim to simplify infrastructure and develop a more secure environment. VMware's approach to enabling customers to meet regulatory controls includes compliance kits, validation of product capabilities and VMWare products' ability to meet compliance requirements, and producing a framework focused on assembling products to support a holistic compliance solution.

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. This overlap between products and compliance requirements marries security and non-security product capabilities. It also supports operational innovation aligned to CMMC compliance requirements.

What is SDDC?

The Software-Defined Data Center (SDDC) architecture assembles storage, network, and compute layers into a unified environment. Capable of being highly automated and available, SDDC can support applications and their requisite system components. 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 across the cloud environment. Features of an SDDC can be deployed as a suite or can also work independently to allow for a controlled deployment over time.

What is the CMMC Framework?

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

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

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

Introduction

CMMC Applicability

CMMC will be required for Department of Defense (DoD) contractors who access, store, or process federal contract information (FCI) or controlled unclassified information (CUI) on behalf on the DoD. For each contract, the government is required to stipulate the CMMC Level of protection based on the sensitivity of the information and the potential threat. Organizations must select and maintain a CMMC Level that can be accomplished efficiently and cost effectively.

At minimum, contracts that involve FCI data will require CMMC Maturity Level 1 compliance and contracts that involve CUI will require CMMC Maturity Level 3 or higher. CUI is data that is created or processed by, or on behalf of, the federal government. The National Archives CUI Registry (https://www.archives.gov/cui/registry/category-list) organizes CUI data into the following 20 data categories:

- Critical Infrastructure
- Defense
- Export Control
- Financial
- Immigration
- Intelligence
- International Agreements
- Law Enforcement
- Legal
- Natural and Cultural Resources
- North Atlantic Treaty Organization (NATO)
- Nuclear
- Patent
- Privacy
- Procurement and Acquisition
- Proprietary Business Information
- Provisional
- Statistical
- Tax
- Transportation

How does CMMC work?

The CMMC recognizes that not all contractors will store, process, or transmit equally sensitive data. Therefore, the CMMC model is based on a multi-tiered approach to allow a more cost-effective opportunity for smaller businesses to support contracts at a lower CMMC Level for contractors that handle data with lower sensitivity.

The CMMC model has 17 domains. Each domain outlines specific processes, capabilities, and practices. See Figure 1 below describing the relationship between these key terminologies.

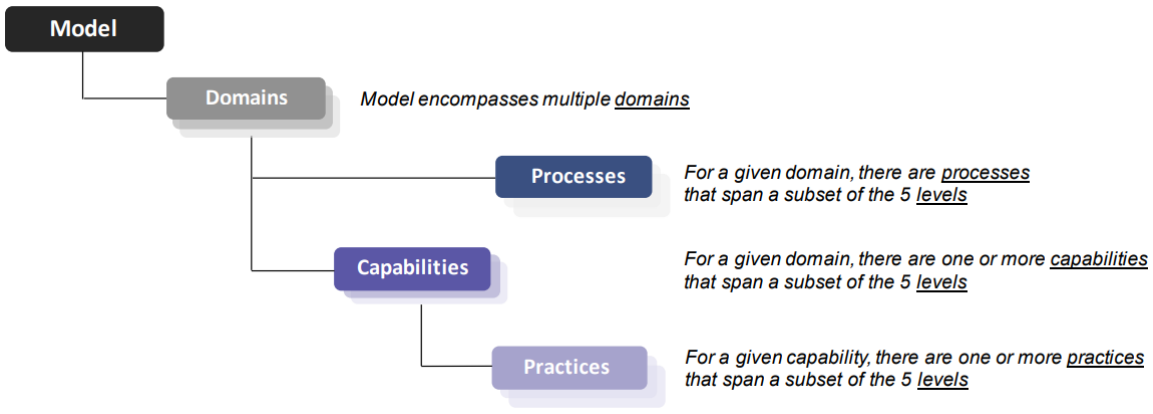

Figure 1 – CMMC Model Framework (Simplified Hierarchical View)

Capabilities are core system or program requirements that must be possible within the system. There are 43 CMMC capabilities across the 17 domains of the CMMC model. Below is an excerpt of the capabilities for three domains.

Domain	Capability
Access Control (AC)	▪ Establish system access requirements. ▪ Control internal system access. ▪ Control remote system access. ▪ Limit data access to authorized users and processes.
Asset Management (AM)	▪ Identify and document assets. ▪ Manage asset inventory.
Audit and Accountability (AU)	▪ Define audit requirements. ▪ Perform auditing. ▪ Identify and protect audit information. ▪ Review and manage audit logs.

Table 1 - Sample of Capabilities within Domains

Capabilities can be considered high level policy statements that address the initial requirements at the highest level. Practices are the 171 requirements spread across all five CMMC Levels and are the more detailed requirements or procedures that must be implemented.

Processes are the measurement of how ingrained the practices are within a system. The table below shows how the Maturity Level relates to the processes.

Maturity Level	Maturity Level Description	Processes
Level 1	Performed	*There are not maturity processes assessed at Maturity Level 1.* *An organization performs Level 1 practices but does not have process institutionalization requirements.*
Level 2	Documented	Establish a policy that includes [DOMAIN NAME]. Document the CMMC practices to implement the [DOMAIN NAME] policy.
Level 3	Managed	Establish, maintain, and resource a plan that includes [DOMAIN NAME].
Level 4	Reviewed	Review and measure [DOMAIN NAME] activities for effectiveness.
Level 5	Optimizing	Standardize and optimize a documented approach for [DOMAIN NAME] across all applicable organization units.

Table 2 - CMMC Maturity Levels

Cumulative Compliance

Each CMMC Level comprises its own practices and those practices of the levels below it. For example, Level 3 requires all practices from Levels 1 and 2, plus an additional 58 practices required for Level 3 itself. Level 5 is cumulative and requires all 156 practices found in Levels 1 through 4, plus an additional 15 practices.

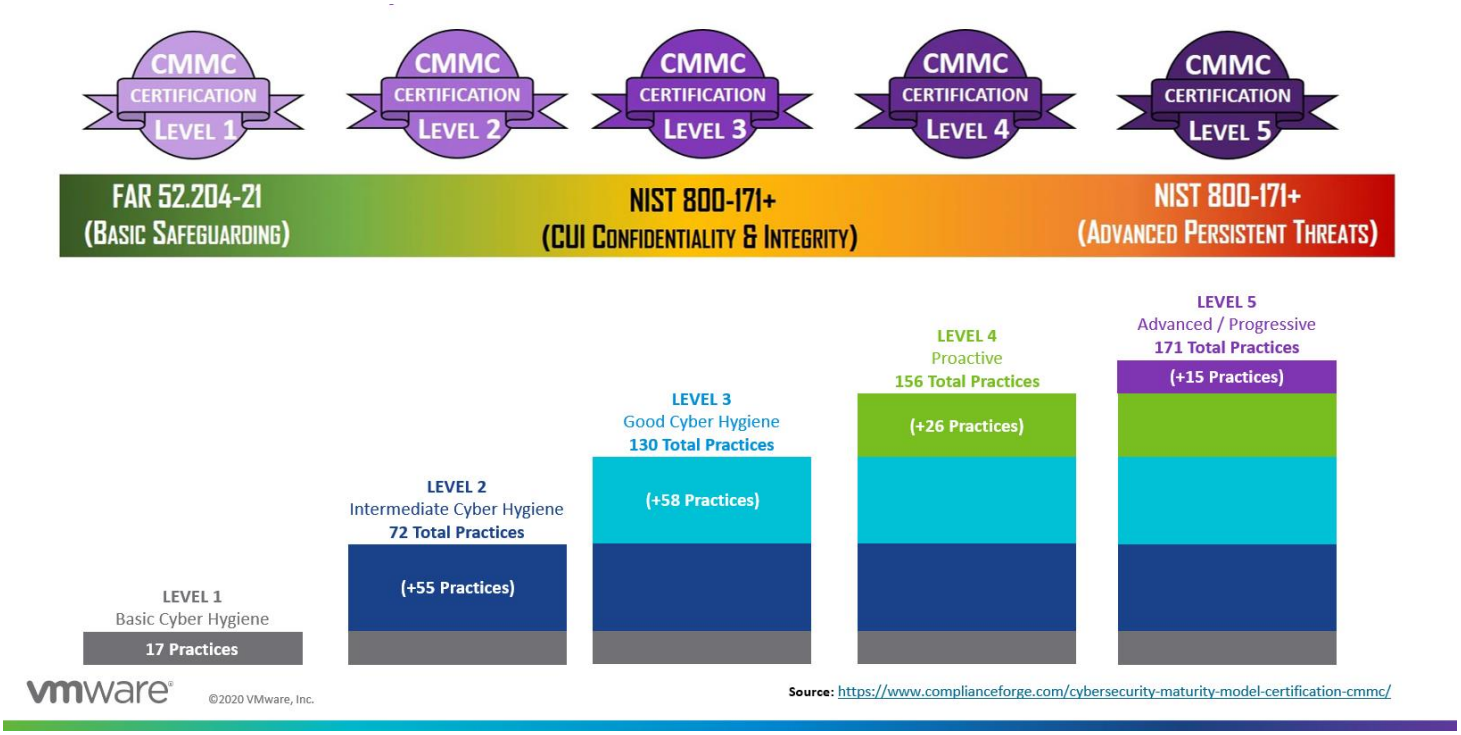

Figure 2 - CMMC Practices Per Level

CMMC unique identifiers use the naming convention of [DOMAIN].[LEVEL].[PRACTICE NUMBER] where:

- DOMAIN is the two-letter domain abbreviation
- LEVEL is the level number (1-5)
- PRACTICE NUMBER is the numerical identifier assigned to that practice

For example, the first Level 2 control of Access Control is referenced by AC.2.005.

How does CMMC relate to other frameworks?

The CMMC model addresses the following 17 security domains, 14 of which are derived from the Federal Information Processing Standards (FIPS) Publication 200 and NIST 800-171, and 3 additional domains.

- Access Control (AC)
- Asset Management (AM)*
- Audit and Accountability (AU)
- Awareness and Training (AT)
- Configuration Management (CM)
- Identification and Authentication (IA)
- Incident Response (IR)
- Maintenance (MA)
- Media Protection (MP)
- Personnel Security (PS)
- Physical Protection (PE)
- Recovery (RE)*
- Risk Management (RM)
- Security Assessment (CA)
- Situational Awareness (SA)*
- System Communication Protection (SC)
- System and Information Integrity (SI)

**denotes a new control family for CMMC.*

These control families are based largely on the existing NIST SP 800-171 framework but add an additional three control families which include Asset Management (AM), Recovery (RE), and Situational Awareness (SA). At Level 3, the CMMC model encompasses all 110 security requirements defined in NIST SP 800-171 and 20 additional controls.

For these additional controls and for the controls found in Levels 4 and 5, CMMC incorporated key additional practices and processes from other standards and references such as NIST SP 800-53, Aerospace Industries Association (AIA) National Aerospace Standard (NAS) 9933 "Critical Security Controls for Effective Capability in Cyber Defense", and Computer Emergency Response Team (CERT) Resilience Management Model (RMM) v1.2.

The following table shows the primary source frameworks for all CMMC controls by level.

CMMC Level	Total Requirements	NIST 800-171 Requirements	Draft NIST SP 800-171B	Additional Requirements
Level 1	17	17	-	-
Level 2	72	65	-	7
Level 3	130	110	-	20
Level 4	156	110	11	35
Level 5	171	110	15	46

Table 3 - Source for CMMC Practices Per Level

Scope and Approach

VMware's SDDC includes multiple products and architectures. Each product component contains features that can be mapped to CMMC requirements. Of the 17 security domains, 12 had mapping overlaps to VMware software capabilities. This document expands to account for all products underneath an SDDC umbrella. The scope of this guide is limited to technical requirements. People and process controls are out of scope.

What is the System Boundary?

The System Boundary is the key area in question within CMMC. The System Boundary can be described as any computer system or network that either processes, stores, or transmits FCI, CUI, or other sensitive information. The System Boundary extends to include any device that maintains a direct connection to the device(s) meeting description of the environment as outlined above.

The System Boundary can include but is not limited to any of the following:

- Firewalls
- Switches
- Routers
- Access Points
- Servers (including Webservers, application servers, or database servers)
- Any application that accepts payments
- Any associated virtual components (including virtual machines (VMs) and virtual networking devices)
- Third-party support staff or systems

Certification Pathway

Organizations interested in CMMC certification for the first time, or who are considering pursuing a higher level should begin by evaluating all polices, standards, procedures, and technical configurations against NIST-800-171 and CMMC controls. All security controls should be required by policy and be supported by clearly designed procedures. Additionally, the organization should perform their own internal assessment to ensure that relevant controls are enforced by system configuration settings and applied consistently on all in-scope systems.

After this thorough review is completed, organizations should document and maintain an up-to-date System Security Plan (SSP). A comprehensive SSP should include at least the following:

- Information System
    - Information System Name and Title
    - System Function
    - System Environment of Operation
    - Network Architecture
    - System Boundary
    - System Interconnections
- Subjective CMMC Level

- Organization Contacts
    - Information System Owner
    - Other Designated Contacts
- Leveraged Practices and Processes
- Practices
- Processes
- POA&M

For each of the applicable practices and processes, organizations should document the implementation status (implemented, partially implemented, alternative implementation, not applicable, or inherited) and the applicable implementation details.

For more information on composing an SSP, see the Tevora Whitepaper, *FedRAMP Authorization Guide: Addendum A: FedRAMP System Security Plan*.

Following the creation of a comprehensive SSP, Tevora recommends that organizations use an independent third-party assessment organization (C3PAO) to conduct a gap assessment to review the SSP and supporting documentation to ensure that the controls are fully met as documented and that these measures provide sufficient security to meet all DFARS controls. The 3PAO's findings should be shared with all relevant business or system owners.

All identified risks and vulnerabilities from internal and external assessments should be rated based on impact and likelihood of occurrence. This risk rating and remediation efforts should be tracked and monitored with a Plan of Actions and Milestones (POA&M).

After the initial gap assessment results, organizations should remediate known compliance gaps and critical vulnerabilities in accordance with the methodology defined within the POA&M. The process, status, and results of remediation efforts should also be updated and maintained within the POA&M.

Once all known gaps and critical vulnerabilities have been remediated, an organization will partner with a CMMC C3PAO to perform a full assessment against the CMMC controls applicable to the selected CMMC Level for accreditation.

System Boundary Management with VMware

From a security perspective, it is an industry best practice to proactively manage data from the initial introduction into a system and throughout the data lifecycle including processing, storage, and the eventual disposal of data. To successfully manage data, it is best to logically control all access and data transmission within a predefined system or system boundary. This can be accomplished by strict access control lists and boundary protection. Boundary protection methodologies can include deny all, permit by exception firewall rules, least privilege, and encrypted data transmission. It is critical that CUI data is not permitted on systems that do not have a specific business requirement to access the data. By reducing the number of systems that can access, store, or process data, an organization can drastically reduce the attack surface or number of systems that could be potentially vulnerable to malicious activity.

From a security audit and compliance perspective, it is best to reduce the number of systems that would be in scope for assessment. With fewer systems that access, process, or store FCI or CUI, compliance assessments will be more efficient and cost effective.

VMWare products allow administrators to create a system where all access, storage and transmission can occur within a pre-defined virtual environment. The three main purposes of an SDDC (Compute, Store, and Network) allow for strict control of data throughout the entire data lifecycle.

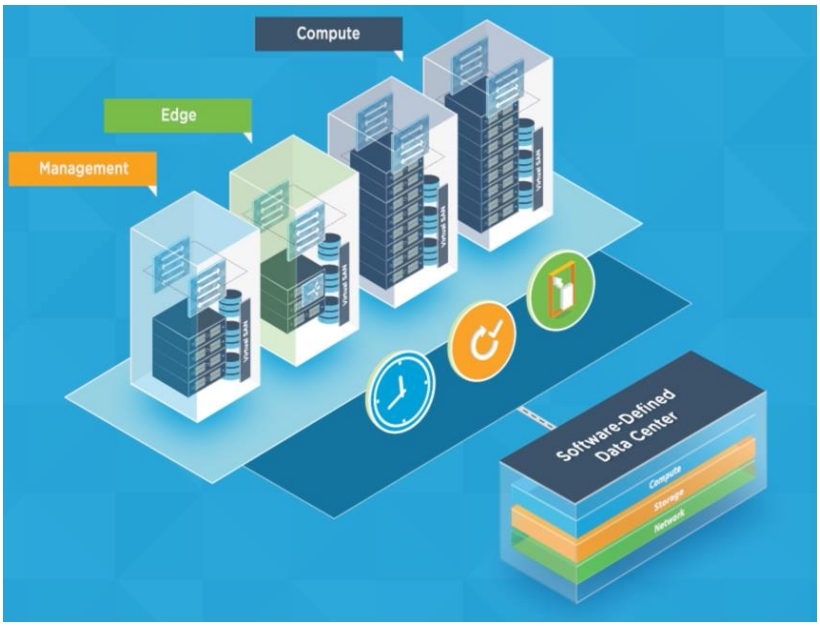

Figure 3 - VMWare SDDC

In-Scope VMware Product List

Software-Defined Data Center (SDDC)

- **VMware vSphere®**
  - **VMware ESXi™6.0, 6.5, 6.7, 6.7 update 2 – 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 its use can effectively partition hardware to increase consolidation ratios and cut costs for customers.
  - **VMware vCenter® 6.0, 6.5, 6.7, 6.7 update 2 – vCenter** provides centralized management of vSphere virtual infrastructure. IT administrators can prioritize security and availability, simplify day-to-day tasks, and reduce the complexity of managing virtual infrastructure.
- **VMware NSX-T** – NSX-T is a network virtualization program which creates, deletes, and restores software-based virtual networks. With network virtualization, the functional equivalent of a network hypervisor reproduces the complete set of Layer 2 through Layer 7 networking services (for example, switching, routing, access control, firewalling, QoS) in software.
- **VMware vSAN™ 6.2, 6.5, 6.6, 6.7 update 3** – **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 vRealize® Suite

- **VMware vRealize Operations Manager™ 6.6, 7.5** – **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™ 4.5, 4.6, 4.7, 4.8** – **vRealize Log Insight** delivers heterogeneous and highly scalable log management with intuitive, actionable dashboards; sophisticated analytics; and broad, third-party extensibility, providing deep operational visibility and faster troubleshooting.
- **VMware vRealize Network Insight™ 3.4, 4.0, 4.1, 4.2, 5.0** – **vRealize Network Insight** delivers intelligent operations for software-defined networking 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™ 7.3, 7.4, 7.5, 7.6** – **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™7.3** – **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 allows for streamlining and automating 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™ 6.5, 8.2** – **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™ 6.5, 8.1, 8.2** – **vSphere Replication** is an extension to VMware vCenter Server® that provides hypervisor-based virtual machine replication and recovery.

Overview of VMware and CMMC Best Practices and Requirement Mapping

CMMC Level 1

- 17 Practices
- VMware has 50% applicability with capabilities across VMware products aligning with 8 requirements
- Level 1 focuses on performing Basic Cyber Hygiene process maturity

VMWare Product	Applicability
Software Defined Data Center:	
VMware vCenter	AC.1.001, AC.1.002, AC.1.003, AC.1.004, SI.1.210
VMware ESXi	AC.1.001, AC.1.002, AC.1.003, AC.1.004, SI.1.210
VMware NSX-T	AC.1.001, AC.1.002, SC.1.175, SC.1.176, SI.1.211,
VMware vSAN	AC.1.001, AC.1.002

VMWare Product	Applicability
VMware Realize Suite	
VMware vRealize Operations Manager	AC.1.001, AC.1.002, AC.1.003, AC.1.004
VMware vRealize Log Insight	AC.1.001, AC.1.002, AC.1.003, AC.1.004, PE.1.131
VMware vRealize Network Insight	AC.1.001, AC.1.002, AC.1.003, AC.1.004, PE.1.131
VMware vRealize Orchestrator	AC.1.001, AC.1.002, AC.1.003, AC.1.004
VMware vRealize Automation	AC.1.001, AC.1.002, AC.1.003, AC.1.004, PE.1.131

VMWare Product	Applicability
Business Continuity	
VMware Site Recovery Manager	AC.1.001, AC.1.002, AC.1.003, AC.1.004
VMware vSphere Replication	-

CMMC Level 2

- 82 Practices
- VMware has 64% applicability with capabilities across VMware products aligning with 54 requirements.
- Level 2 focuses on performing Intermediate Cyber Hygiene process maturity.

VMWare Product	Applicability
Software Defined Data Center:	
VMware vCenter	AC.2.007, AC.2.009, AC.2.016, AT.2.056, AU.2.044, CM.2.065, IA.2.080, MA.2.113, SC.2.179, SI.2.214, SI.2.216
VMware ESXi	AC.2.007, AC.2.009, AC.2.016, AT.2.056, AU.2.044, CM.2.063, CM.2.065, IA.2.080, MA.2.113, SC.2.179
VMware NSX-T	AC.2.007, AC.2.008, AC.2.009, AC.2.010, AC.2.016, AU.2.041, AU.2.042, AU.2.043, CM.2.061, CM.2.062, CM.2.064, IA.2.078, IA.2.080, IA.2.081, IA.2.082, MA.2.113, RE.2.137, SC.2.179, SI.2.214, SI.2.216, SI.2.217
VMware vSAN	AC.2.007, AC.2.008, AC.2.010, AU.2.043, AU.2.044, CM.2.065, IA.2.078

VMWare Product	Applicability
VMware Realize Suite	
VMware vRealize Operations Manager	AC.2.007, AC.2.016, AU.2.044, CM.2.065, IA.2.080
VMware vRealize Log Insight	AC.2.007, AC.2.016, AU.2.041, AU.2.042, AU.2.044, IA.2.080, IR.2.092, SI.2.214, SI.2.216
VMware vRealize Network Insight	AC.2.007, AC.2.016, AU.2.044, SI.2.214, SI.2.216
VMware vRealize Orchestrator	AC.2.007, AC.2.016, AU.2.044, CM.2.061, CM.2.065, IA.2.080
VMware vRealize Automation	AC.2.007, AC.2.016, AU.2.044, CM.2.061

VMWare Product	Applicability
Business Continuity	
VMware Site Recovery Manager	AC.2.007, AC.2.016, AU.2.044, IA.2.080
VMware vSphere Replication	-

CMMC Level 3

- 130 Practices
- VMware has 64% applicability with capabilities across VMware products aligning with 88 requirements.
- Level 3 focuses on performing Good Cyber Hygiene process maturity.

VMWare Product	Applicability
Software Defined Data Center:	
VMware vCenter	IA.3.083, SC.3.193
VMware ESXi	AC.3.018, AC.3.021, AT.3.058, AU.3.049, AU.3.052, IA.3.083, MP.3.125, SC.3.183, SC.3.193, SI.3.218
VMware NSX-T	AC.3.017, AC.3.018, AC.3.021, AU.3.045, AU.3.046, AU.3.048, AU.3.049, AU.3.051, AU.3.052, CM.3.067, CM.3.068, CM.3.069, IA.3.083, IA.3.084, IA.3.086, RE.3.139, SC.3.181, SC.3.183, SC.3.184, SC.3.186, SC.3.187, SC.3.190
VMware vSAN	AC.3.017, AC.3.018, AU.3.045, AU.3.049, AU.3.052, IA.3.086, MP.3.125, SC.3.181

VMWare Product	Applicability
VMware Realize Suite	
VMware vRealize Operations Manager	AC.3.021, AU.3.049, AU.3.052, IR.3.098, SC.3.181, SC.3.193
VMware vRealize Log Insight	AC.3.018, AC.3.021, AU.3.046, AU.3.048, AU.3.049, AU.3.051, AU.3.052, IR.3.098, SC.3.181, SC.3.193
VMware vRealize Network Insight	AC.3.018, AC.3.021, AU.3.049, AU.3.052, SC.3.181, SC.3.193
VMware vRealize Orchestrator	AC.3.021, AU.3.049, AU.3.052, IR.3.098, SC.3.181, SC.3.193
VMware vRealize Automation	AC.3.018, AC.3.021, AU.3.049, AU.3.052, CM.3.068, SC.3.181, SC.3.193, SI.3.218

VMWare Product	Applicability
Business Continuity	
VMware Site Recovery Manager	AC.3.018, AC.3.021, AU.3.049, AU.3.052, SC.3.181, SC.3.193
VMware vSphere Replication	SC.3.177, SC.3.185

CMMC Level 4

- 156 Practices
- VMware has 58% applicability with capabilities across VMware products aligning with 95 requirements.
- Level 4 focuses on performing Proactive process maturity.

VMWare Product	Applicability
Software Defined Data Center:	
VMware vCenter	AC.4.023
VMware ESXi	AC.4.023
VMware NSX-T	AC.4.023, AC.4.025, AU.4.054, CM.4.073, SC.4.197, SC.4.202
VMware vSAN	AC.4.025

VMWare Product	Applicability
VMware Realize Suite	
VMware vRealize Operations Manager	AC.4.023
VMware vRealize Log Insight	AC.4.023, AU.4.054
VMware vRealize Network Insight	AC.4.023
VMware vRealize Orchestrator	AC.4.023
VMware vRealize Automation	AC.4.023

VMWare Product	Applicability
Business Continuity	
VMware Site Recovery Manager	AC.4.023
VMware vSphere Replication	-

CMMC Level 5

- 171 Practices
- VMware has 55% applicability with capabilities across VMware products aligning with 99 requirements.
- Level 5 focuses on performing Advanced / Progressive process maturity.

VMWare Product	Applicability
Software Defined Data Center:	
VMware vCenter	SI.5.222, SI.5.223
VMware ESXi	AU.5.055
VMware NSX-T	SI.5.222, SI.5.223
VMware vSAN	AU.5.055

VMWare Product	Applicability
VMware Realize Suite	
VMware vRealize Operations Manager	AU.5.055
VMware vRealize Log Insight	AU.5.055, SI.5.222, SI.5.223
VMware vRealize Network Insight	AU.5.055, SI.5.222, SI.5.223
VMware vRealize Orchestrator	AU.5.055
VMware vRealize Automation	AU.5.055

VMWare Product	Applicability
Business Continuity	
VMware Site Recovery Manager	AU.5.055
VMware vSphere Replication	-

Appendix A: VMware Control Capabilities Detail

In the tables below, the following products names have been shortened:

Software Defined Data Center (SDDC)

- VMware vCenter (**vCenter**)
- VMware ESXi (**ESXi**)
- VMware NSX-T (**NSX-T**)
- VMware vSAN (**vSAN**)

VMware Realize Suite

- VMware vRealize Operations Manager (**vROPs**)
- VMware vRealize Log Insight (**vRLI**)
- VMware vRealize Network Insight (**vRNI**)
- VMware vRealize Orchestrator (**vRO**)
- VMware vRealize Automation (**vRA**)

Business Continuity

- VMware Site Recovery Manager (**SRM**)
- VMware vSphere Replication (**vSphere Replication**)

Software-Defined Data Center (SDDC)

Product Name	Unique ID	Product Version	Product Capability	CMMC Citation Reference
ESXi	ESXI_001	6.0, 6.5, 6.7	Logon attempts can be logged.	AC.2.009
ESXi	ESXI_002	6.0, 6.5, 6.7	Concurrent sessions can be limited on web clients, and virtual machine consoles.	AC.1.001, AC.1.002, AC.2.007
ESXi	ESXI_006	6.0, 6.5, 6.7	ESXi supports integration with external authentication solutions such as Active Directory. Users that are members of a group that have been granted access to ESXi, can use single sign-on and will be able to log in using their user ID with elevated privileges. Password requirements (e.g., minimum password, account lockout, and account lockout threshold) will be managed via the external authentication solution.	AC.1.003, AC.1.004, AC.2.016, AC.4.023, SC.3.193
ESXi	ESXI_008	6.0, 6.5, 6.7	ESXi can push logs to be stored in an external log repository that supports Syslog, including vRLI. If vRLI is used, it can apply tamper protection for logs that can be used during after-the-fact investigations without altering the event logs.	AC.3.018, AU.2.044, AU.3.049, AU.3.052, AU.5.055
ESXi	ESXI_009	6.5, 6.7	ESXi supports the Secure Boot feature to monitor firmware and to validate version control and authorization. If a violation is detected during boot, the system will not boot. If the violation is detected at runtime, the command will be rejected and not be processed.	AU.5.055, CM.2.063
ESXi	ESXI_010	6.0, 6.5, 6.7	ESXi and vCenter audit-quality logging in 6.5 is enabled by default. Changing logging levels is only for troubleshooting logs used by GSS.	AC.3.018, AU.2.044, AU.3.049
ESXi	ESXI_011	6.5, 6.7	If ESXi has Secure Boot enabled, any attempt to execute unsigned binaries will be blocked. All shell commands are logged via Syslog and the attempt to install unsigned binaries will be logged.	AT.3.058, AU.2.044, AU.5.055
ESXi	ESXI_016	6.0, 6.5, 6.7	ESXi patching is performed via vCenter using VMware Update Manager (VUM).	CM.2.065, SI.1.210
ESXi	ESXI_017	6.0, 6.5, 6.7	vSphere Hardening Guide provides support for ESXi and vCenter hardening procedures.	AT.2.056
ESXi	ESXI_018	6.0, 6.5, 6.7	Logon authentication techniques includes multi-factor Authentication.	IA.3.083, MA.2.113, SC.2.179
ESXi	ESXI_019	6.0, 6.5, 6.7	ESXi supports configuration of access control via single sign-on or Active Directory services, such as requiring new users to change password on first logon, minimum password age, account lockout threshold, and account lockout duration. Logon authentication techniques includes multi-factor authentication.	IA.2.080

Product Name	Unique ID	Product Version	Product Capability	CMMC Citation Reference
NSX-T	NSX-T_002	2.4, 2.5	NSX-T enables password enforcement rules such as setting Password Expiration (set to 3 months by default), Password Length (set to 12 characters by default), Password Complexity (turned on by default). Entering of passwords is masked. All stored passwords are encrypted. Password resets require the previous password to be provided.	IA.2.078, IA.2.081, IA.2.082
NSX-T	NSX-T_003	2.4, 2.5	NSX-T supports segmentation by firewall rules, port restrictions, and network segmentation via vLANs to restrict communication between VMs. This can provide additional security to applications and databases that are communicating over the network by enforcing isolation and security rules for security architecture leveraging segmentation concepts.	SC.1.176
NSX-T	NSX-T_006	2.4, 2.5	Session lockouts are enforceable and require users to re-authenticate after a session time-out.	AC.2.010, SC.3.186
NSX-T	NSX-T_007	2.4, 2.5	Account lockout threshold can be altered.	AC.2.009
NSX-T	NSX-T_008	2.4, 2.5	NSX-T supports logging and includes auditable event selections such as privileged actions (who did what and when), system changes, configuration changes, administrative events, account management of both users (including account lockout and password expiration), and alerts to specify the configurations to monitor. This information can be sent via Syslog to vRLI, or another log repository solution.	AU.2.042, AU.2.043, AU.3.045, AU.4.054
NSX-T	NSX-T_009	2.4, 2.5	NSX-T can be used to monitor the network for inappropriate usage and security violations. Network activity and traffic can be logged and evaluated, along with firewall traffic. This can support system monitoring for inappropriate usage and other security violations.	SI.2.214, SI.2.216, SI.5.222, SI.5.223
NSX-T	NSX-T_014	2.4, 2.5	NSX-T 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, as well as through configuration policies and firewall polices to manage internal information flow.	AC.2.016, AC.4.023
NSX-T	NSX-T_015	2.4, 2.5	Combined with Workspace One Access or another integrated Identity Access Management tool, NSX-T can support multi-factor authentication.	IA.3.083, MA.2.113, SC.2.179

Product Name	Unique ID	Product Version	Product Capability	CMMC Citation Reference
NSX-T	NSX-T_019	2.4, 2.5	NSX-T can distinguish between a Trusted Network and an Untrusted Network to support boundary protection. Rules can be assigned to protect the boundary and ensure external perimeter network access is managed accordingly.	SC.1.175, SC.4.197
NSX-T	NSX-T_020	2.4, 2.5	NSX-T can be implemented with a fault-tolerant architecture. This can also be used to schedule and restore backups.	RE.2.137, RE.3.139
NSX-T	NSX-T_026	2.4, 2.5	NSX-T provides some capabilities to facilitate detection of malicious code traffic. Using stateful scans and firewall traffic monitoring is one of the capabilities in identify malicious code. Third party vendors can also integrate with NSX-T to enhance detection of malicious activity.	SC.4.202, SI.1.211
NSX-T	NSX-T_032	2.4, 2.5	NSX-T comes with 13 pre-defined roles that can be assigned to enable role-based access control. In addition, new roles can be developed, based on an inventory of functionality, to be used as custom roles. This capability can support both separation of duties, as well as the concept of least privilege.	AC.1.001, AC.1.002, AC.2.007, AC.2.008, AC.3.017, AC.3.018, CM.2.061, CM.2.062, CM.2.064, SC.3.181
NSX-T	NSX-T_036	2.4, 2.5	NSX-T includes three default accounts. The "root" user is disabled by default. The "admin" account can be disabled. The "auditor" account is restricted to read-only and can also be disabled. The system can enforce changing default passwords.	IA.2.080, IA.3.086
NSX-T	NSX-T_045	2.4, 2.5	NSX-T has the capability to redirect logs to a SIEM or copy logs and send them to another logging tool for analysis. Logging is collected across the software-defined networking infrastructure and can be incorporated with system-wide, time-correlated audit trails. Logging can be used to track audit trails across system components such as nodes, type of event, location, user, and correlated with other data, to support adding additional elements. Data frequency and retention parameters can be set.	AU.2.041, AU.3.048, AU.3.051
NSX-T	NSX-T_047	2.4, 2.5	NSX-T can capture some events of unauthorized access, such as performing events that are not authorized. In some cases, the UI will inform the user that sufficient permission is unavailable to perform the desired action.	SI.2.217
NSX-T	NSX-T_048	2.4, 2.5	NSX-T system clocks can be synchronized to NTP to enable accurate and universal time source logging.	AU.2.043

Product Name	Unique ID	Product Version	Product Capability	CMMC Citation Reference
vCenter	VCENTER_001	6.0, 6.5, 6.7	vCenter supports access control configuration, via single sign-on or Active Directory services to implement session timeout, logon attempts, account lockout threshold, account lockout duration, minimum password age, and requiring re-authentication.	AC.1.001, AC.1.002, AC.2.007, AC.2.009, IA.2.080
vCenter	VCENTER_002	6.0, 6.5, 6.7	Concurrent sessions can be limited on web clients, and virtual machine consoles.	AC.1.001, AC.1.002, AC.2.007
vCenter	VCENTER_005	6.0, 6.5, 6.7	Super user capabilities in vCenter are a combination of privileges, which can be assigned to administrator roles. Assignment of elevated privileges can be restricted to only those users that are approved as designated system administrators.	AC.1.001, AC.1.002, AC.2.007
vCenter	VCENTER_008	6.0, 6.5, 6.7	Remote access to vCenter via SSH, or web client or API over HTTPS, can be configured as the secure communication protocol. The vCenter appliance runs on Linux and can be restricted to only accept HTTPS. Session identifiers are invalidated after session termination.	AC.1.003, AC.1.004, AC.2.016, AC.3.021, AC.4.023, SC.3.193
vCenter	VCENTER_011	6.0, 6.5, 6.7	vCenter can push logs to be stored in an external log repository that supports Syslog, including vRLI. vRLI can apply tamper protection for logs that can be used during after-the-fact investigations without altering the event logs.	AC.3.018, AU.2.044, AU.3.049, AU.3.052, AU.5.055
vCenter	VCENTER_012	6.0, 6.5, 6.7	vCenter supports monitoring a set of standardized settings, which may indicate inappropriate usage or security violations. Alarms and alerts can be configured to notify users via email when triggered.	AC.3.018, AU.2.044, AU.3.049, AU.5.055, SI.2.214, SI.2.216, SI.5.222, SI.5.223
vCenter	VCENTER_013	6.0, 6.5, 6.7	vCenter has inherent capabilities to log events at specific frequencies. The log event characteristics captured can be adjusted. Additionally, the log retention, based on disk space, can be enhanced through use of a separate logging repository via Syslog, or vRLI.	AC.3.018, AU.2.044, AU.3.049
vCenter	VCENTER_015	6.0, 6.5, 6.7	vCenter supports enhanced logging of audit level events to support third party integration with tools such as introduction detection systems (IDS).	AC.3.018, AU.2.044, AU.3.049, AU.5.055
vCenter	VCENTER_020	6.0, 6.5, 6.7	vCenter can push audit trail logs to be archived in an external log repository that supports Syslog, including vRLI.	AC.3.018, AU.2.044, AU.3.049, AU.5.055
vCenter	VCENTER_021	6.0, 6.5, 6.7	vCenter can patch ESXi hosts through VMware Update Manager (VUM).	CM.2.065, SI.1.210

Product Name	Unique ID	Product Version	Product Capability	CMMC Citation Reference
vCenter	VCENTER_022	6.0, 6.5, 6.7	vCenter can facilitate installation of critical security updates for ESXi. VMware Update Manager (VUM) alerts vCenter of any firmware issues that affect ESXi and can be used to install patches and automate installation of updates. vCenter has a manual feature to check for security or operational updates.	CM.2.065
vCenter	VCENTER_023	6.0, 6.5, 6.7	vSphere Hardening Guide provides support for ESXi and vCenter hardening procedures. https://www.vmware.com/security/hardening-guides.html	AT.2.056
vCenter	VCENTER_025	6.0, 6.5, 6.7	vCenter can natively provide multi-factor authentication techniques such as CAT Card and RSA 2FA.	IA.3.083, MA.2.113, SC.2.179
vSAN	vSAN_001	6.2, 6.5, 6.6, 6.7	Access to data storage in vSAN is managed by roles within vCenter. vSAN 6.5 introduced a new role to enable or disable encryption that can be applied to restrict non-cryptographic user access from configuring this feature.	AC.1.001, AC.1.002, AC.2.007, AC.2.008, AC.3.017, AC.3.018, AC.4.025, IA.2.078, IA.3.086, SC.3.181
vSAN	vSAN_002	6.2, 6.5, 6.6, 6.7	Logging capabilities can be enabled and customized to capture event information.	AC.3.018, AU.2.044, AU.3.045, AU.3.049, AU.5.055
vSAN	vSAN_003	6.2, 6.5, 6.6, 6.7	Logging can be synchronized to system clocks (NTP) and date and time stamp capture.	AU.2.043
vSAN	vSAN_004	6.2, 6.5, 6.6, 6.7	vSAN can push logs to be stored in vRLI. A default vSAN Dashboard is available in vRLI as a content pack.	AC.3.018, AU.2.044, AU.3.049, AU.3.052, AU.5.055
vSAN	vSAN_005	6.2, 6.5, 6.6, 6.7	vCenter or ESXi controls and enforces session lockouts which require users to re-authenticate after a session time-out.	AC.2.010
vSAN	vSAN_007	6.2, 6.5, 6.6, 6.7	vSAN can be patched via vCenter's VMware Update Manager patching capabilities. Additionally, vSAN 6.6 can patch firmware controller drivers for participating vendors.	CM.2.065
vSAN	vSAN_008	6.2, 6.5, 6.6, 6.7	Maintenance activity is logged and can be accessed via reports, which can be archived for historical reference. The maintenance logs are captured at each component vCenter, ESXi, and vSAN, which can be holistically analyzed via vRLI or custom API log reporting tool.	AU.2.044, AU.3.049, AU.5.055

VMware vRealize Suite

Product Name	Product Unique ID	Product Version	Product Capability	CMMC Citation Reference
vRealize Automation	VRA_001	7.3, 7.5, 7.6	Security and protection software can be installed using NSX Rest API and Guest Introspection.	SI.3.218
vRealize Automation	VRA_002	7.3, 7.5, 7.6	A proof of maintenance log is available to report on archived maintenance activity.	AU.2.044, AU.5.055, PE.1.131
vRealize Automation	VRA_003	7.3, 7.5, 7.6	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.	AC.1.003, AC.1.004, AC.2.016, AC.3.021, AC.4.023, SC.3.193
vRealize Automation	VRA_005	7.3, 7.5, 7.6	vRA can push logs to Syslog supported logging solutions, or vRLI. vRLI can then apply tamper protection for logs that can be used to support after-the-fact investigations without altering the event logs.	AC.3.018, AU.2.044, AU.3.049, AU.3.052, AU.5.055
vRealize Automation	VRA_006	7.3, 7.5, 7.6	vRA 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.2.061
vRealize Automation	VRA_007	7.3, 7.5, 7.6	vRA 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.3.068
vRealize Automation	VRA_008	7.3, 7.5, 7.6	vRA supports multiple roles to separate user functionality from system management functionality, as well as the capability to support the principle of lease privilege user access control.	AC.1.001, AC.1.002, AC.2.007, SC.3.181
vRealize Automation	VRA_009	7.3, 7.5, 7.6	vRA can automate log capturing and transmission to logging solutions.	AC.3.018, AU.2.044, AU.3.049

Product Name	Product Unique ID	Product Version	Product Capability	CMMC Citation Reference
vRealize Log Insight	VRLI_001	4.5, 4.6, 4.7, 4.8	vRLI supports role-based access control (RBAC) to access the data collected. Data collection is supported on TCP, as well as secure TCP which offers protection from unauthorized disclosure. vRLI further offers the ability to manage data sets that can limit one user's access to specific sources based on need to know. Syslogs can be forwarded to various SIEM tools that store and encrypt logs while offering non-repudiation. Using third party software, vRLI can be configured to support non-repudiation of log entries and monitor access to logs to ensure transactions are reputable. The access restriction would be applied at the operating system (OS) and manage access to the underlying file system or database since Super Users administering the OS would be able to access log information.	AC.1.001, AC.1.002, AC.2.007
vRealize Log Insight	VRLI_002	4.5, 4.6, 4.7, 4.8	A proof of maintenance log is available to report on archived maintenance activity.	AU.2.044, AU.5.055, PE.1.131
vRealize Log Insight	VRLI_004	4.5, 4.6, 4.7, 4.8	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, which can be manually configured to enhance system monitoring.	AC.3.018, AU.2.041, AU.2.042, AU.2.044, AU.3.046, AU.3.049, SI.2.214, SI.2.216, SI.5.222, SI.5.223
vRealize Log Insight	VRLI_005	4.5, 4.6, 4.7, 4.8	vRLI supports standard Syslog and secure Syslog. In addition, when using an internal vRLI agent, a secure, encrypted protocol is enforceable.	AU.4.054
vRealize Log Insight	VRLI_006	4.5, 4.6, 4.7, 4.8	Audit Dashboard is provided to analyze log data and support after-the-fact investigations. In addition, vRLI can provide tamper protection by deploying a log system architecture configured to support multiple storage locations to minimize the risk of a central location from being corrupted or altered.	AC.3.018, AU.2.044, AU.3.049, AU.3.052, AU.5.055, IR.2.092
vRealize Log Insight	VRLI_007	4.5, 4.6, 4.7, 4.8	vRLI 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.3.018, AU.2.044, AU.3.048, AU.3.049, AU.3.051, AU.5.055
vRealize Log Insight	VRLI_010	4.5, 4.6, 4.7, 4.8	vRLI can perform backups of logs for all products. Remote archival of vRLI logging data is supported.	AU.3.049

Product Name	Product Unique ID	Product Version	Product Capability	CMMC Citation Reference
vRealize Log Insight	VRLI_011	4.5, 4.6, 4.7, 4.8	Hosts can use a vRLI agent or send logs via Syslog to the centralized vRLI log database to manage storage, retention, and protection of logs from unauthorized activity.	AC.3.018, AU.2.044
vRealize Log Insight	VRLI_012	4.5, 4.6, 4.7, 4.8	By default, remote access to vRLI is set to HTTPS. Session identifiers are discarded upon session termination.	AC.1.003, AC.1.004, AC.2.016, AC.3.021, AC.4.023, SC.3.193
vRealize Log Insight	VRLI_013	4.5, 4.6, 4.7, 4.8	vRLI allows access control settings to be configured to manage sessions, including account lockout threshold, account lockout duration, and password policies. vRLI can integrate authentication with vCenter's PSC to enable enforcement of authentication parameters directly from Active Directory.	AC.1.001, AC.1.002, AC.2.007
vRealize Log Insight	VRLI_015	4.5, 4.6, 4.7, 4.8	vRLI 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. vIDM or an external authentication solution is required to administer this capability. vRLI can integrate authentication with vCenter's PSC to enable enforcement of authentication parameters directly from Active Directory.	AC.1.001, AC.1.002, AC.2.007, SC.3.181
vRealize Log Insight	VRLI_016	4.5, 4.6, 4.7, 4.8	vRLI 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.1.001, AC.1.002, AC.2.007, AU.3.049
vRealize Log Insight	VRLI_017	4.5, 4.6, 4.7, 4.8	If local accounts are created in vRLI, users can be required to change their password upon first logon.	IA.2.080
vRealize Log Insight	VRLI_018	4.5, 4.6, 4.7, 4.8	Alerts are generated when agents are unresponsive, or offline after a defined period of time.	AU.2.044, AU.5.055, IR.3.098
vRealize Log Insight	VRLI_019	4.5, 4.6, 4.7, 4.8	vRLI collects logs in real time. Content packs to enhance dashboards and provide custom queries tailored to many VMware products.	AC.3.018, AU.2.044, AU.3.049, AU.5.055, IR.2.092
vRealize Network Insight	VRNI_001	3.4, 4.0, 4.1, 4.2, 5.0	vRNI receives NetFlow from vSphere Distributed Switches (VDS), which connects virtual machines together. This can be used to monitor information flows and network flows.	AC.3.018, AU.2.044, AU.3.049, AU.5.055
vRealize Network Insight	VRNI_002	3.4, 4.0, 4.1, 4.2, 5.0	A proof of maintenance log is available to report on archived maintenance activity.	AU.2.044, AU.5.055, PE.1.131

Product Name	Product Unique ID	Product Version	Product Capability	CMMC Citation Reference
vRealize Network Insight	VRNI_003	3.4, 4.0, 4.1, 4.2, 5.0	Remote access to administrative features can be restricted to SSH or other secure communication protocols. The configuration files can be altered manually in vRNI 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.1.001, AC.1.002, AC.2.007
vRealize Network Insight	VRNI_004	3.4, 4.0, 4.1, 4.2, 5.0	After fifteen minutes of inactivity, users are locked out and required to re-authenticate.	AC.3.021
vRealize Network Insight	VRNI_005	3.4, 4.0, 4.1, 4.2, 5.0	vRNI can push logs to Syslog, or vRLI. vRLI can then apply tamper protection for logs that can be used to support after-the-fact investigations without altering the event logs.	AC.3.018, AU.2.044, AU.3.049, AU.3.052, AU.5.055
vRealize Network Insight	VRNI_006	3.4, 4.0, 4.1, 4.2, 5.0	vRNI can be used to monitor data center traffic and provide visibility to support monitoring activities.	SI.2.214, SI.2.216, SI.5.222, SI.5.223
vRealize Network Insight	VRNI_008	3.4, 4.0, 4.1, 4.2, 5.0	vRNI logs network traffic has a default retention period of thirty days, which can be extended to thirteen months. This log data can provide audit trail support.	AU.2.044, AU.3.049, AU.5.055
vRealize Network Insight	VRNI_009	3.4, 4.0, 4.1, 4.2, 5.0	vRNI can provide visibility into the information flow, including information flow insight for managing policies of the system and between interconnected systems.	AC.1.003, AC.1.004, AC.2.016, AC.4.023, SC.3.193
vRealize Network Insight	VRNI_010	3.4, 4.0, 4.1, 4.2, 5.0	vRNI administrator can manage User Interface (UI) users. Users connect via a web portal UI. These user accounts can be reviewed, and access control can be managed using roles (Administrator, or read-only member user). Password complexity can be configured.	AC.1.001, AC.1.002, AC.2.007, SC.3.181
vRealize Orchestrator	VRO_001	7.3, 7.4, 7.5, 7.6	Remote access to products can be restricted to SSH or other secure communication protocols. Configuration files can be manually 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.1.003, AC.1.004, AC.2.016, AC.4.023, SC.3.193
vRealize Orchestrator	VRO_002	7.3, 7.4, 7.5, 7.6	vRealize Orchestrator can provide user information responsible for creating or modifying the virtual machine, virtual infrastructure asset information, or other information. This can also be used to trace creation or modification of ownership.	CM.2.061
vRealize Orchestrator	VRO_003	7.3, 7.4, 7.5, 7.6	A proof of maintenance log is available to report on archived maintenance activity.	AU.2.044, AU.5.055

Product Name	Product Unique ID	Product Version	Product Capability	CMMC Citation Reference
vRealize Orchestrator	VRO_004	7.3, 7.4, 7.5, 7.6	vRO 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.1.001, AC.1.002, AC.2.007, SC.3.181
vRealize Operations	VROPS_001	6.6, 7.5	A proof of maintenance log is available to report on archived maintenance activity.	AU.2.044, AU.5.055
vRealize Operations	VROPS_002	6.6, 7.5	Outbound plugin notifications are available in Vrops. These have to be configured to enforce the flow of data to a third-party system. Remote access to vROPS is restricted by default. vROPS appliance remote access can only be enabled to use SSH via the vCenter VM Console. vROPS user interface is only accessible via a secure URL. Upon session termination, session identifiers are invalidated.	AC.1.003, AC.1.004, AC.2.016, AC.3.021, AC.4.023, SC.3.193
vRealize Operations	VROPS_004	6.6, 7.5	Using a management pack specific to the compliance area (PCI and HIPAA only at this time), vROPS 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.2.065
vRealize Operations	VROPS_007	6.6, 7.5	vROPS can perform capacity planning, forecasting, and reporting. An input into this planning process can include comparing capacity between production and backup sites.	IR.3.098
vRealize Operations	VROPS_008	6.6, 7.5	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.2.080
vRealize Operations	VROPS_010	6.6, 7.5	vROPS can be configured to support account lockout duration, number of failed attempts, password length and complexity.	AC.1.001, AC.1.002, AC.2.007
vRealize Operations	VROPS_011	6.6, 7.5	vROPS can push audit trail logs to be archived in an external log repository that supports Syslog, including vRLI.	AU.3.049, AU.3.052
vRealize Operations	VROPS_012	6.6, 7.5	vROPS permits creating roles and groups using role-based access control (RBAC). Granularity can be applied to view or edit objects, run reports, and other functionality. vROPS permits the creation of roles and groups using RBAC. Granularity can be applied to view or edit objects, run reports, and other functionality. A separate Administrative UI is available for the admin to perform actions related to vROPs infrastructure changes (like adding node, HA configuration).	SC.3.181

Business Continuity

Product Name	Product Unique ID	Product Version	Product Capability	CMMC Citation Reference
SRM	SRM_002	6.5,8.2	SRM can push logs to be stored in vRLI. A content pack is provided to facilitate SRM logging and dashboard visualization of logging. SRM can push logs to be stored in vRLI. A content pack is provided to facilitate SRM logging and dashboard visualization of logging. In addition, logs can also be sent to a remote Syslog server. The vRealize Operations Management Pack for VMware Site Recovery Manager provides capabilities for monitoring the connectivity between Site Recovery Manager instances, the availability of a remote Site Recovery Manager instance, andthe status of Protection Groups and Recovery Plans in Site Recovery Manager. Alarms are generated when there are Site Recovery Manager Server connectivity issues encountered or Protection Groups and Recovery Plans are in error state	AC.3.018, AU.2.044, AU.3.049, AU.3.052, AU.5.055
SRM	SRM_005	6.5,8.2	SRM 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. For Photon OS, SRM can push logs via Syslog including vRLI. SRM 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.	AC.3.018, AU.2.044, AU.3.049, AU.5.055
SRM	SRM_007	6.5,8.2	Remote access is possible via Remote Desktop Protocol (RDP) to the SRM system in Windows OS, and SSH to SRM in Photon OS. This can be managed through external authentication solutions. Use of SRM does not require RDP access mechanism and RDP is usually allocated for administrative access only. This access is usually allocated for administrative access only and not necessary to be made available on external network. The internal SSH communications can be secured by approved list of ciphers (not completely FIPS approved)	AC.1.003, AC.1.004, AC.2.016, AC.3.021, AC.4.023, SC.3.193
SRM	SRM_008	6.5,8.2	SRM relies on vCenter to manage assigned user access and user accounts, including assignment of roles to restrict functionality.	AC.1.001, AC.1.002, AC.2.007, SC.3.181

Product Name	Product Unique ID	Product Version	Product Capability	CMMC Citation Reference
SRM	SRM_009	6.5,8.2	SRM 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 logon.	IA.2.080
vSphere Replication	VSPHERE REPLICATION_005	8.2	To enhance the security of data transfer, you can enable the network encryption of the replication traffic data for new and existing.	SC.3.177, SC.3.185

About VMware

VMware, a leading innovator in enterprise software, powers the world's digital infrastructure.

Our cloud, app modernization, networking, security, and digital workspace platforms form a flexible, consistent digital foundation on which to build, run, manage, connect, and protect applications, anywhere.

A digital foundation built on VMware enables rapid, technology-driven innovation and continuous integration of emerging technologies. Organizations can move quickly without disrupting business operations, while maximizing return on investments in people, processes, and systems.

We help businesses become digital at their core—so they can meet the needs of customers and employees, and more quickly take advantage of market opportunities.

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 serve institutional and government clients.

Tevora's assessment methodology is accredited by the *American Association for Laboratory Accreditation (A2LA)* for NIST 800-171. (Certification number: 5062.01). Please note, the recommendations included within this report are the opinions of Tevora. All opinions or interpretations identified or expressed in this report are outside the scope of Tevora's A2LA Accreditation.

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 can fully implement whatever it recommends, Tevora works with all the industry's top vendors, yet is beholden to none. Our hard work and dedication have 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 HITRUST Assessor, Qualified Security Assessor (QSA) and Payment Application Qualified Security Assessor (PA-QSA) in good standing with the PCI Security Standards Council, and ISO27001 Certified cybersecurity organization. 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.

Go forward. We've got your back.

Compliance – Enterprise Risk Management – Data Privacy – Security Solutions – Threat Management