VMware® SDDC and EUC Product Applicability Guide for NIST 800-53 Rev.4
# Table of Contents

Executive Summary ..................................................................................................................... 3  
Background ................................................................................................................................ 3  
VMware SDDC and NIST 800-53 Rev. 4 ..................................................................................... 3  
Introduction ............................................................................................................................... 4  
What is NIST 800-53 Rev. 4? ...................................................................................................... 4  
How does 800-53 rev. 4 work? .................................................................................................. 4  
Scope and Approach .................................................................................................................... 5  
Our Approach ............................................................................................................................. 5  
VMware’s Compliance Methodology .......................................................................................... 6  
In-Scope VMware Product List .................................................................................................. 6  
Overview of VMware and NIST 800-53 rev.4 Best Practices and Requirement Mapping .......... 9  
VMware Control Capabilities Detail ............................................................................................ 11  
VMware Validated Design and Software Development Process .............................................. 11  
Administrative Support for NIST Control Families ................................................................ 11  
Core NIST Control Families ...................................................................................................... 12  
Core NIST Control Family .......................................................................................................... 13  
Administrative NIST Control Families ..................................................................................... 20  
Conclusion .................................................................................................................................. 24  
Bibliography ............................................................................................................................... 25  
Appendix A: Summarized Product Mappings to NIST 800-53 Rev. 4 ........................................ 28
Revision History

<table>
<thead>
<tr>
<th>Date</th>
<th>Rev</th>
<th>Author</th>
<th>Comments</th>
<th>Reviewers</th>
</tr>
</thead>
<tbody>
<tr>
<td>July 2017</td>
<td>0.1</td>
<td>Tevora</td>
<td>Initial Draft</td>
<td>Carlos Phoenix and Anthony Dukes</td>
</tr>
<tr>
<td>August 2017</td>
<td>0.2</td>
<td>VMware</td>
<td>VMware SME Review</td>
<td>Product Teams and Security Specialists</td>
</tr>
<tr>
<td>August 2017</td>
<td>1.1</td>
<td>Tevora and VMware</td>
<td>Final</td>
<td>Legal</td>
</tr>
</tbody>
</table>

Design Subject Matter Experts
The following people provided key input into this whitepaper.

<table>
<thead>
<tr>
<th>Name</th>
<th>Email Address</th>
<th>Role/Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>David Grazer</td>
<td><a href="mailto:dgrazer@tevora.com">dgrazer@tevora.com</a></td>
<td>Co-Author</td>
</tr>
<tr>
<td>Christina Whiting</td>
<td><a href="mailto:cwhiting@tevora.com">cwhiting@tevora.com</a></td>
<td>Co-Author</td>
</tr>
<tr>
<td>Anthony Dukes</td>
<td><a href="mailto:adukes@vmware.com">adukes@vmware.com</a></td>
<td>Technology SME, VMware</td>
</tr>
<tr>
<td>Carlos Phoenix</td>
<td><a href="mailto:cphoenix1@vmware.com">cphoenix1@vmware.com</a></td>
<td>Compliance and Cybersecurity SME, VMware</td>
</tr>
</tbody>
</table>
## 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](http://www.vmware.com/go/patents). VMware is a registered trademark or trademark of VMware, Inc. in the United States and/or other jurisdictions. All other marks and names mentioned herein may be trademarks of their companies.

<table>
<thead>
<tr>
<th>Solution Area</th>
<th>Key Products</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Software-Defined Compute</strong></td>
<td>VMware ESXi™, VMware vCenter™, VMware vCenter Server™, VMware vCenter Server“ Standard™, VMware vCenter™” Single Sign-On, VMware vCenter Server™ Appliance™, VMware vCloud Suite®, VMware vSphere® Data Protection™, VMware Tools®, VMware vSphere® Distributed Resource Scheduler®, VMware vSphere® Distributed Power Management®, VMware vSphere® Enterprise Plus Edition®, VMware vSphere® Fault Tolerance, VMware vSphere® Flash Read Cache™, VMware vSphere® High Availability, VMware vSphere® Storage DRS®, VMware vSphere® Storage vMotion®, VMware vSphere® vMotion®, VMware vSphere® Web Client, Platform Services Controller™</td>
</tr>
<tr>
<td><strong>Software-Defined Networking</strong></td>
<td>VMware NSX®, VMware NSX® Manager™, VMware NSX® Controller™, VMware NSX® Services™, VMware NSX® Virtual Switch™, VMware NSX® API™, VMware NSX® for vSphere®</td>
</tr>
<tr>
<td><strong>Management and Automation</strong></td>
<td>VMware vRealize® Suite Enterprise, VMware vRealize® Operations™, VMware vRealize® Operations Manager™, VMware vRealize® Hyperic®, VMware vRealize® Configuration Manager™, VMware vRealize® Infrastructure Navigator™, VMware vRealize® Log Insight®, VMware vRealize® Log Insight™ Content Pack for xxx, VMware vRealize® Operations Insight™, VMware vRealize® Orchestrator™, VMware vRealize® Orchestrator Appliance™, VMware vRealize® Operations for Horizon®, VMware vRealize® Operations for Published Applications™, VMware vRealize® Operations Manager™ for Horizon®, VMware vRealize® Automation™, VMware vRealize® Business™ Enterprise, VMware vRealize® Operations Management Pack™ for xxx, VMware vSphere® Service Manager®, VMware vSphere® Syslog Collector, VMware vSphere® Update Manager®, VMware vSphere® Update Manager Client™, VMware vSphere® with Operations Management™, VMware Power CLI</td>
</tr>
<tr>
<td><strong>Disaster Recovery Automation</strong></td>
<td>VMware vCenter™ Site Recovery Manager™, VMware vSphere® Replication™</td>
</tr>
<tr>
<td><strong>End User Computing</strong></td>
<td>VMware Workspace™ ONE™, VMware Horizon® Enterprise Edition, VMware Horizon® FLEX™, VMware Horizon®, VMware View®, VMware View® Composer™, VMware View® Manager™, VMware Horizon® Client, VMware Horizon Agent™, VMware Identity Manager™, VMware User Environment Manager™, VMware Workspace Environment Manager™, VMware App Volumes™, VMware App Volumes™ for Endpoints™, One Cloud, Any App, Any Device™, One Cloud, Any Application, Any Device™</td>
</tr>
<tr>
<td><strong>Enterprise Mobility Management</strong></td>
<td>VMware AirWatch®, VMware AirWatch® Yellow Management Suite™, VMware AirWatch® Agent™, VMware AirWatch® Appliance™, VMware AirWatch® App Catalog™, VMware AirWatch® App Wrapping™, VMware AirWatch® Cloud Connector™, VMware AirWatch® Connect™, VMware AirWatch® Enterprise Mobility Management™, VMware AirWatch® Container™, VMware AirWatch® Mobile Device Management™, VMware AirWatch® Mobile Application Management™, VMware AirWatch® Inbox, VMware AirWatch® Kiosk Mode™, VMware AirWatch® Laptop Management™, VMware AirWatch® Launcher™, VMware AirWatch® Mobile Access Gateway™, VMware AirWatch® Content Locker™, VMware AirWatch® Content Manager™, VMware AirWatch® Mobile Browsing Management™, VMware AirWatch® Mobile Email Management™ VMware AirWatch® Browser™, VMware AirWatch® Secure Email Gateway™</td>
</tr>
</tbody>
</table>
Executive Summary

Background
In this Product Applicability Guide (PAG), we will provide an evaluation of each VMware product that is within the Software-defined Data Center (SDDC) and End User Computing (EUC) suite of products. These products virtualize and abstract the physical technology layers such as compute, storage, and network. The changing technology landscape that is modernizing the data center is also modernizing the virtual desktop environment, mobile device management, and making inroads to consolidate and automate Information Technology (IT) resources. VMware prioritizes data protection and system security features within the Software-defined Data Center (SDDC) and End User Computing (EUC) suite of products. VMware’s Compliance and Cyber Risk Solution (CCRS) team developed a compliance capable platform framework that incorporates SDDC and EUC product capabilities aligned to NIST 800-53 controls. Using NIST 800-53 as a foundational risk framework and security control catalog, the compliance capable platform framework maps VMware products to control requirements to weave together VMware product capabilities with compliance requirements and cybersecurity controls.

NIST 800-53 (rev4) provides organizations with a tested baseline of controls. It can be used to establish and refine a comprehensive data protection and cyber security program. Ultimately, the risk an organization faces are mitigated by controls and the PAG provides one perspective on how VMware products can assist organizations with managing their cyber risks and implementing a stronger IT security control program.

VMware partnered with Tevora, an independent third-party IT audit firm, to conduct a review of the SDDC and EUC solutions’ alignment to NIST 800-53 (rev. 4). This document is the culmination of discussions with product teams to perform a thorough evaluation of VMware product capabilities mapped to NIST 800-53 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 800-53 (rev. 4) standard and highlight applicable VMware product capabilities.

VMware SDDC and NIST 800-53 Rev. 4
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 complex business and compliance requirements.

VMware approaches compliance with a view that understands the complexity in 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 Capable Platform 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 and EUC product capabilities to NIST 800-53 security requirements can result in a solution that has been vetted as compliance capable. This overlap between products and compliance requirements establishes a new standard marrying security and non-security product capabilities to also achieve operational innovation. Due to the breadth of the NIST compliance framework, VMware selected NIST 800-53 as its foundation for all future PAGs, and as the acknowledgement across industry standards that have been derived from the larger NIST risk framework.

Who is NIST?
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).

For Consideration
For more information about the general approach to compliance issues, please visit VMware Solution Exchange: Compliance & Cyber Risk Solutions. This whitepaper has been reviewed and authored by Tevora’s staff of Information Security Professionals in conjunction with VMware, Inc.
Introduction

What is NIST 800-53 Rev. 4?
NIST Special Publication (SP) 800-53 Rev.4 (NIST 800-53 Rev4.), has been developed by NIST to further its statutory responsibilities under the Federal Information Security Management Act (FISMA), Public Law (P.L.) 107-347. It represents the culmination of a year-long initiative to update the content of the security controls catalog and the guidance for selecting and specifying security controls for federal information systems and organizations. The project was conducted as part of the Joint Task Force Transformation Initiative in cooperation and collaboration with the Department of Defense, the Intelligence Community, the Committee on National Security Systems, and the Department of Home Land Security. The proposed changes included in Revision 4 are directly linked to the current state of the threat space (i.e., capabilities, intentions, and targeting activities of adversaries) and the attack data collected and analyzed over a substantial time period. NIST 800-53 (Rev. 4) is an extensive catalog of information security controls.

While the initial intent of NIST 800-53 was to provide guidance and criteria for federal information systems, over the past few years, revisions have been made for widespread adoption across various commercial and private industries.

The fourth revision was released in February 2012 and updates preceding publications within the areas of:
- Insider Threats
- Software Application Security (including web applications)
- Social Networking, Mobiles Devices, and Cloud Computing
- Cross Domain Solutions
- Advanced Persistent Threats
- Supply Chain Security
- Industrial/Process Control Systems
- Privacy

While the initial intent of NIST 800-53 and its revisions was to provide guidance and criteria for federal information systems, over the past few years, updates have been made for widespread adoption across various commercial and private industries.

How does 800-53 rev. 4 work?
The NIST 800-53 Rev.4 standard requires organizations to comply with a robust set of criteria. The criteria are broken down into 18 control families (listed below) and provided ratings of impact to the business or organization. Ratings are either Low-Impact, Moderate-Impact, or High-Impact. These risk ratings identify the specific controls to be implemented within each control family.

- Access Control (AC)
- Awareness and Training (AT)
- Audit and Accountability (AU)
- Security Assessment and Authorization (CA)
- Configuration Management (CM)
- Contingency Planning (CP)
- Identification and Authentication (IA)
- Incident Response (IR)
- Maintenance (MA)
- Media Protection (MP)
- Physical and Environmental Protection (PE)
- Planning (PL)
- Personnel Security (PS)
- Risk Assessment (RA)
- System and Services Acquisition (SA)
- System and Communications Protection (SC)
- System and Information Integrity (SI)
- Program Management (PM)

1 The PM family of controls are not in scope for this document, as they are operational in nature and are meant to be applied post installation and are operational in nature.
In order to derive the specific risk rating, a “Three-Tiered Risk Management” approach allows organizations a strategic viewpoint, not a solely compliance-based viewpoint, on security program development. The tiers are used to conclude the applicable risk rating that ultimately results in identifying the specific controls within each control family that are applicable. The risk is derived based on the following tiered risk approach:

- Tier 1 - Organization,
- Tier 2 - Mission/Business Processes
- Tier 3 - Information Systems

All control families may not be applicable to an organization, depending on their size and scope of business. Each control takes the “Three-tiered Risk Management” model into account and provides supplemental guidance on what a well-defined control looks like.

These controls will aid US-based entities moving forward within a shifting regulatory landscape. While the standard is lengthy, it would be advantageous for any organization to define and/or align their security program against, especially those organizations evaluating overseas expansion.

Scope and Approach

The SDDC platform and EUC suites cover a wide number of products and architectures. Each component product, and the suite collectively, contains features that could be mapped to some NIST 800-53 R4 controls. 17 of the 18 total control families had some mapping overlaps to VMware’s software capabilities. This guide expands to account for all products underneath the SDDC and EUC umbrella. The scope of this guide is limited to those requirements supported technically, or through direct API integration. Additional technologies required in addition to VMware products is not identified. People and process controls are not addressed within this guide either.

Our Approach

This Product Applicability Guide (PAG) is intended to provide information for all security and compliance practitioners on the optimal usage of VMware’s technical stack to address regulatory compliance obligations and enhance the security of their services through the security and compliance framework of NIST 800-53. It is up to each organization to identify the applicable NIST 800-53 controls and requirements that are in scope and, in addition, to determine the risk rating of NIST 800-53 High, Moderate, and Low impacts. The PAG is focused on the control family without the specific controls based on risk ratings because each organization will need to perform its own risk rating and selection of controls based on their scope and the organization’s conclusion of relevance. Thus, controls may vary within control families based on risk ratings.

In addition to the NIST 800-53 control families, there are eleven security lenses used to evaluate the SDDC and EUC products. These are included in VMware’s Compliance Capable Platform Framework (Exhibit 1). These eleven 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 security lenses include:

- Data Segmentation
- System Hardening
- Compliance Validation
- System Access
- System Monitoring
- Data Encryption & Protection
- Network Protection
- Endpoint Protection

Evaluating the SDDC and EUC 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 800-53 Rev. 4 standard but also to comport with general security best practices.

Tevora’s team 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 and EUC 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 and EUC’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’s products can be deployed with continuous compliance in mind.

**VMware’s Compliance Methodology**

VMware technology enablement can provide information and other supporting capabilities required by NIST 800-53. A compliance capable solution begins with a compliance context (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 undertaken with the goal of producing a whitepaper that outlines the validated compliance capable platform. The output is a compliance capable design that can be used to configure and address compliance requirements. Below is an overview of this process.

---

### Exhibit 1: VMware Compliance Capable Platform—SDDC Framework

**In-Scope VMware Product List**

**Software-Defined Data Center (SDDC)**

**vSphere**

- **ESXi** – VMware 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.

- **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.

- **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.
Cloud Foundation

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

Virtualized Networking

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

vRealize Suite

**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.

**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.

**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 VMware NSX deployments.

**vRealize Orchestrator** – 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.

**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.

**vRealize Business** – provide an easy way for IT teams to understand their IT costs, communicate effectively with their business counterparts around these costs, and be able to plan better for future IT spending.

Business Continuity

**Site Recovery Manager** – is the industry-leading solution to enable application availability and mobility across sites in private cloud environments. Site Recovery Manager 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.

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

Enterprise Mobility Management

**AirWatch** - platform enables your organization to centrally manage every device, every app and every mobile use case, both corporate-owned and Bring Your Own Device (BYOD).
Digital Workspace

**Workspace One** - is the enterprise platform that enables IT to deliver a digital workspace that empowers the workforce to securely bring the technology of their choice—devices and apps—at the pace and cost the business needs.

**Identity Manager** - is identity management for the mobile cloud era that delivers on consumer-simple expectations like one-touch access to nearly any app, from any device, optimized with AirWatch Conditional Access. Empower employees to get productive quickly with a self-service app store while giving IT a central place to manage user provisioning and access policy with enterprise-class directory integration, identity federation and user analytics.

Desktop and Application Virtualization

**Horizon 7** - delivers virtualized or hosted desktops and applications through a single platform to end users, provides IT with a new streamlined approach to deliver, protect, and manage Windows and Linux desktops and applications while containing costs and ensuring that end users can work anytime, anywhere, on any device.

**VMware Horizon FLEX** - provides the flexibility IT needs to serve end users, while maintaining security and compliance with centrally managed, containerized desktops.

**App Volumes** – is the next generation of desktop and application delivery, providing radically faster application delivery, unified application and user management, while reducing IT costs.

**VMware ThinApp** - simplifies application virtualization and reduces the cost and complexity of application delivery.

**VMware 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 User Environment Manager** - offers personalization and dynamic policy configuration across any virtual, physical and cloud-based Windows desktop environment. User Environment Manager simplifies end-user profile management by providing organizations with a single, light-weight and scalable solution that leverages existing infrastructure. It accelerates time-to-desktop and time-to-application by replacing bloated roaming profiles and unmaintainable, complex logon scripts.
Overview of VMware and NIST 800-53 rev.4 Best Practices and Requirement Mapping

Exhibit 2 represents a high-level view of how VMware technology capabilities match up to best practices areas, as well as NIST 800-53 (Rev. 4) requirement topics.

<table>
<thead>
<tr>
<th>Best Practice Area (Lens)</th>
<th>NIST 800-53 R4</th>
<th>Capability Description</th>
<th>VMware Product Applicability</th>
</tr>
</thead>
<tbody>
<tr>
<td>Automated Security</td>
<td>CP, RA</td>
<td>Automated Deployment, Automated Remediation</td>
<td>vSphere Recovery Manager vRealize Operations</td>
</tr>
<tr>
<td>Data Segmentation</td>
<td>PL, SA, SC, SI</td>
<td>Network &amp; Host Firewall, Information Flow</td>
<td>VMware NSX VMware SDLC VMware Validated Design VMware Cloud Foundation vRealize Network Insight vRealize Operations vRealize Log Insight</td>
</tr>
<tr>
<td>System Hardening</td>
<td>CM, MP, PS, SA, SC, SI</td>
<td>Configuration Management, Patch Management, Vulnerability Management</td>
<td>vRealize Network Insight vRealize Operations vRealize Log Insight vSphere Update Manager VMware NSX AirWatch Workspace One vSphere ESXi 6.5</td>
</tr>
<tr>
<td>Compliance Validation</td>
<td>CM</td>
<td>Configuration Management</td>
<td>vRealize Network Insight vRealize Operations vRealize Log Insight VMware NSX AirWatch Workspace One</td>
</tr>
<tr>
<td>System Access</td>
<td>AC, AT, AU, IA, IR, PE, PL, PS, SC</td>
<td>Two-Factor Authentication, Identity and Access Management</td>
<td>VMware Identity Manager vCenter VMware NSX vRealize Network Insight vRealize Log Insight vRealize Operations AirWatch vSphere ESXi 6.5</td>
</tr>
<tr>
<td>System Monitoring</td>
<td>AT, AU, CA, CM, CP, IR, MA, PE, PL, PS, RA, SC, SI</td>
<td>Security Information Event Monitoring (SIEM), Database Monitoring</td>
<td>vRealize Log Insight vRealize Network Insight vRealize Operations Site Recovery Manager vSphere Replication AirWatch vCenter Workspace One vSphere Update Manager</td>
</tr>
<tr>
<td>Best Practice Area (Lens)</td>
<td>NIST 800-53 R4</td>
<td>Capability Description</td>
<td>VMware Product Applicability</td>
</tr>
<tr>
<td>--------------------------</td>
<td>----------------</td>
<td>------------------------</td>
<td>-----------------------------</td>
</tr>
<tr>
<td>Data Encryption &amp; Protection</td>
<td>CA, IA, MA, SA, SC, SI</td>
<td>Data At Rest Encryption, Data In Motion Encryption, System Backup &amp; Restore</td>
<td>vSphere ESXi 6.5 VM Encryption, vSAN 6.6 vSAN Encryption, vMotion Encryption, VMware NSX, vRealize Operations, vRealize Network Insight, vRealize Log Insight, vSphere, VMware SDLC, VMware Validated Design, VMware Cloud Foundation, vSphere Update Manager</td>
</tr>
<tr>
<td>Trusted Execution/Secure Boot</td>
<td>SC, SI</td>
<td>Execution Integrity, Configuration Integrity</td>
<td>vSphere ESXi 6.5, VMware NSX, vRealize Log Insight, vRealize Operations, vRealize Network Insight, vSphere Update Manager</td>
</tr>
</tbody>
</table>

Exhibit 2: VMware Product Applicability and Solutions
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 proper integration points of the components at the detail level required to securely and confidently deploy SDDC. The VVD is available to anyone and is published on VMware’s website. Soon, the VVD intends to include EUC. In the meantime, it is possible to deploy a VVD SDDC and include EUC products.

The VMware Software Development Life Cycle (SDLC) designs security into all phases for both SDDC and EUC products (Exhibit 3). This principled approach to designing security in from the start is important to NIST 800-53 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 compliance-capable platform that can support organizations using the NIST 800-53 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 VMware’s approach. These lenses are trademarks of a mature security program addressing common areas of vulnerabilities.

Exhibit 3: VMware SDLC Activity Timeline

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 800-53 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 800-53 includes supplemental, or complimentary controls. As a framework, NIST 800-53 provides organizations an opportunity to enhance controls using additional, complimentary controls beyond the baseline of controls associated with each risk rating.
An example of an administrative control family is Incident Response Planning (IR). This control family may require a documented incident response plan or a detailed run-books on audit procedures. Using VMware products such as NSX, vRealize Network Insight, or vRealize Log Insight to strengthen and accelerate discoveries and corrective actions during incident responses is possible because these products provide monitoring, troubleshooting, and remediation capabilities. 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 support are:

- Awareness and Training (AT)
- Security Assessment and Authorization (CA)
- Contingency Planning (CP)
- Incident Response (IR)
- Maintenance (MA)
- Media Protection (MP)
- Physical and Environmental Protection (PE)
- Planning (PL)
- Personnel Security (PS)
- Risk Assessment (RA)

Core 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 800-53 that best highlight how each product provides capabilities to strengthen the security and support a compliance capable platform.

The details below showcase SDDC and EUC 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 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.
Core NIST Control Family

Access Control (AC)

*NIST Controls AC1-AC22*

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, in addition to the integrity of the entire authentication process.

Applicable Security Lens:
- System Access
- Endpoint Protection

Applicable VMware Product:
- NSX
- AirWatch
- vSphere
- vRealize Log Insight
- vRealize Network Insight
- vRealize Operations

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.

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. Organizations can also integrate their Active Directory (AD) / Lightweight Directory Access Protocol (LDAP) instance through use of VMware’s published Application Programmable Interfaces (API) to refine access at all levels of their virtual stack.

To ensure that only trusted IPs, subnets, or IP devices are allowed into the environment, AirWatch enables detailed blacklisting and whitelisting capabilities. This capability is complementary to vCenter and NSX that can provide access restriction to an organization’s East-West traffic, or Virtual Machine (VM) to Virtual Machine communications.

NSX allows access control through the implementation of micro-segmentation via security policies. The NSX identity-based firewall enhances the access control down to the virtual networking level, permitting only approved users with need to access specific virtual machines. These authentication mechanisms can be managed through security groups and policies configured within the vSphere Web Client.

Monitoring can be done 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 firewall and security group policies.
Core NIST Control Family

Audit and Accountability (AU)

NIST Controls AU1-AU16

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:
- vCenter
- vRealize Log Insight
- AirWatch
- vRealize Operations
- vRealize Network Insight

VMware Product Capabilities

The Audit and Accountability control family speaks to the need for a security program to conduct regular 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.

Further, vRealize Log Insight gives IT and IT Security Teams the ability to point all products in their stack to vRealize Log Insight to help manage and correlate any incidents or perceived incidents. AirWatch goes a step further providing the functionality to set the frequency of logs deploying making the process of finding useful insights that much more user friendly.

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 to specify a specific day retention. vRealize Log Insight retains data based on defined storage capacity. vRealize Operations assists by monitoring the data stores health, 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.

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 time real-time action.
Core NIST Control Family

Configuration Management (CM)  
*NIST Controls CM1-CM11*

This control family establishes management of information system 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:
- NSX-V
- NSX-T
- vSphere
- AirWatch
- WorkspaceOne
- vRealize Operations

VMware Product Capabilities

The VVD architecture contains specified requirements for each components configuration. This provides a “gold standard” for deployment across all the 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 either NSX-V or NSX-T. Routing specifications can be set and protected by tamper-proof logging. Active Directory can be integrated to enforce least privilege functionality, based on requirements across the user-base.

Knowing that the protection or adherence to standards is difficult without knowing what resides in the network, vSphere has features to provide a list 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.

With mobile being a main and significant traffic source, AirWatch provides Mobile Device Management (MDM) functionality. This will provide users with the capability to define blacklist/whitelists and report unauthorized access. WorkspaceOne can establish a stable blacklist/whitelist across all devices and offer identity device management. AirWatch provides the ability for configuration management, and for patching for mobile devices.
Core NIST Control Family

Identification and Authentication (IA)

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 & Protection
- System Access

Applicable VMware Product:
- NSX-V
- NSX-T
- vRealize Operations
- vSphere
- vSphere ESXi 6.5 VM Encryption
- vSAN 6.6 vSAN Encryption
- VMware Cloud Foundation

VMware Product Capabilities

Products require 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, timeouts and re-authentication can be set across all SDDC products, by following the standard VVD requirement. Both vSphere ESXi 6.5 VM Encryption and vSAN 6.6 vSAN Encryption certify that all data stored within a customer's SDDC environment is encrypted to industry standards.

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 set to require that upon the initial logon session with ROOT, users will be prompted to reset the password. All products in accordance with the VVD and SDLC are required to have minimum password standards are stored in an encrypted fashion, never maintained in clear text format.

Administrators viewing all passwords through the Graphic User Interface (GUI) will have passwords for all credentials obscured or masked with asterisks.

In addition, 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.
Core NIST Control Family

System and Services Acquisition (SA)

NIST Controls SA1-SA19

System and Services Acquisition spans the underlying makeup of an organization’s SDLC and how security is applied. It hones in on understanding resource allocation, the security engineering principles employed, supply chain protection and how developers, engineers and other product development personnel are prepared to perform the duties defined by the organization.

Applicable Security Lens:
- Data Segmentation
- Data Encryption & Protection
- System Hardening
- Software Development Lifecycle (SDLC)

Applicable VMware Product:
- VMware Validated Design
- VMware’s SDLC
- VMware Compliance Capable Platform
- vSphere ESXi 6.5 VM Encryption
- VMware Cloud Foundation
- vSAN 6.6 vSAN Encryption

VMware Product Capabilities

VMware’s approach to security extends into its development process. While constant iteration is a priority, security is interwoven into every stage from ideation and design to development and into production. Static code analysis, security and privacy considerations at the design phase run through multiple levels of approval, in addition to performance level assessments. Developers participate in extensive secure code training and regularly attend working sessions in collaboration with security compliance and privacy teams to stay abreast of evolving trends and vulnerabilities. This is important because VMware customers. The overlap in security emphasis between VMware internal SDLC processes and the System and Service Acquisition (SA) NIST control family fulfills requirements including process isolation at both personnel level and code level, encryption protocols in transmission and permission granularity.

Particularly important for this control family is the ability to meet security requirements can be met during the acquisition process. For organizations looking to secure all levels of their infrastructure, it is should be understood that the SDLC extends out into the supply chain and products that are acquired by VMware to deliver virtual solutions to the marketplace. Through the VMware Cloud Foundation (including vSAN 6.6 and vSphere ESXi 6.5 Encryption), all elements of your virtualized environment are encrypted and secure throughout internetwork transit.

The VMware Compliance and Cyber Risk Solutions (CCRS) team develops whitepapers and other documentation to show the mapping between VMware product capabilities and compliance requirements. CCRS designed the VMware Compliance Capable Platform framework. On an on-going basis, CCRS provides product engineering with feedback to further solidify product capabilities in support of compliance controls and cyber risk requirements. VMware product mappings and design architecture in support of a compliance capable platform augment the value of acquiring VMware products.
Core NIST Control Family

System and Communications Protection (SC)

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 & Protection
- Trusted Execution/Secure Boot

Applicable VMware Product:
- NSX-V
- NSX-T
- vRealize Networking Insight
- vRealize Log Insight
- vSphere ESXi 6.5 VM Encryption
- vSAN 6.6 vSAN Encryption
- VMware Cloud Foundation

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 backdoors. 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 Edge Gateways gives boundary protection and network isolation to user environments. Through its Dynamic Host Configuration Protocol (DHCP) service, 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. NSX and its micro-segmentation can then enforce defined information flow guidelines. The information contained within these data flows are then secured at rest with vSAN 6.6 and vSphere ESXi 6.5 Encryption capabilities.

VMware’s security program 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.

Core NIST Control Family

System and Information Integrity (SI)

NIST Controls SI1-SI12

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:
- vSphere ESXi 6.5
- vSphere ESXi 6.5 VM Encryption
- vRealize Network Insight
- vRealize Operations
- vSAN 6.6 vSAN Encryption
- vRealize Log Insight
- VMware Cloud Foundation
- vSphere Update Manager

VMware Product Capabilities

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

To highlight, vSphere 6.5 ESXi 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.

If signatures are not validated, the hypervisor fails to activate. ESXi 6.5 does not report intelligence back on the failure to the session’s origin. This is important as it protects the integrity of an organization’s virtual servers from adversaries targeting intelligence to exploit.

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 being accessed, brute force attack, or attempt to attack an ESX 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 Operations 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. vSphere Update Manager and vRealize Operations can be configured to automate remediation on identified vulnerabilities. 3rd Party solutions can be inserted to combine both on-premise and cloud-based synchronization of updates.

Finally, all VMs can be set for destruction upon completion of use.
Administrative NIST Control Families

 Awareness and Training (AT)  
* NIST Controls AT1-AT5

This control family is managed through Administrative action on the client-side and is not applicable to VMware natively.

**Applicable Security Lens:**
- System Monitoring
- System Access
- Network Protection

**Applicable VMware Product:**
- Administrative support

 Security Assessment and Authorization (CA)  
* NIST Controls CA1-CA7

Most of this control family will be managed through Administrative policies as defined by the organization. All products under the SDDC and EUC umbrella will provide context and insight to allow for management and Boards of Directors to understand and provide their guidance to enhance the entity’s security.

vRealize Operations and vRealize Log Insight, along with the other products that comprise the SDDC suite, will support the implementation of continuous monitoring. vRealize Operations gives administrators the ability to craft custom security tags that align with NIST 800-53 and other security frameworks to maintain up-to-the-minute assessment and authorization across the environment.

**Applicable Security Lens:**
- System Monitoring
- Data Encryption & Protection
- Network Protection

**Applicable VMware Product:**
- vRealize Operations
- vRealize Log Insight
- vSAN 6.6 vSAN Encryption
- vSphere ESXi 6.5 VM Encryption
- VMware Cloud Foundation
Administrative NIST Control Families

Contingency Planning (CP)

NIST Controls CP1-CP13

Contingency Planning in accordance to NIST 800-53 will be governed by Administrative policy. VMware products such as Site Recovery Manager and vSphere will support the needs for data back-ups, or site replication as detailed within the policy. Site Recovery Manager can also house contingency plans and drive any automated corrective actions needed to sustain required operating levels.

Further, for components of the control family relating to Predictable Failure and System Recovery and Reconstitution, vRealize Operations has been designed to support high availability. This means that if one virtual machine fails, vRealize Operations can be configured, at the organization’s discretion, to automatically failover to an alternative VM (or start a new one) to ensure uptime as required by SLAs or other operating needs. Replication can additionally allow for a new VM to be constructed automatically upon trigger. vSphere Replication is a replication tool completely autonomous from the underlying storage. It acts as the transport mechanism for the VM to the failover site.

Applicable Security Lens:
- System Monitoring
- Network Protection
- Automated Security

Applicable VMware Product:
- Site Recovery Manager
- vRealize Operations
- vSphere Replication

Incident Response (IR)

NIST Controls IR1-IR8

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:
- Administrative Support
Administrative NIST Control Families

**Maintenance (MA)**

*NIST Controls MA1-MA6*

Most controls listed underneath this control family are performed in accordance with organizational policy. VMware Update Manager and vRealize Operations allow for maintaining up-to-date patching. 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 & Protection

**Applicable VMware Product:**
- vRealize Operations
- vSphere Update Manager
- vSAN 6.6 vSAN Encryption
- vSphere ESXi 6.5 VM Encryption
- VMware Cloud Foundation

**Media Protection (MP)**

*NIST Controls MP1-MP8*

VMware products will support the controls of this family through organizationally developed policy. Products within the SDDC do not natively provide features that directly apply to the family’s intent.

**Applicable Security Lens:**
- System Hardening

**Applicable VMware Product:**
- Administrative support

**Physical and Environmental Protection (PE)**

*NIST Controls PE1-PE18*

VMware products will support the controls of this family through organizationally developed policy. All SDDC platform components provide backup and recovery capabilities, which will aid the employment of the policy for requirements such as data protection, recovery time objectives (RTO) and recovery point objectives (RPO).

**Applicable Security Lens:**
- System Access
- System Monitoring
- Network Protection

**Applicable VMware Product:**
- Administrative support
Administrative NIST Control Families

Planning (PL)

*NIST Controls PL1-PL4*

VMware products will support the controls of this family through organizationally developed policy. Across all products VMware employs secure information sharing processes, natively available throughout the VMware Cloud Foundation suite. These processes are critical pieces of the VVD and includes the need for strict design testing requirements. Each product must clear requirements thresholds prior to deploying for public use.

Applicable Security Lens:
- Data Segmentation
- System Access
- System Monitoring
- Software Development Lifecycle (SDLC)

Applicable VMware Product:
- Administrative support
- VMware Cloud Foundation

Personnel Security (PS)

*NIST Controls PS1-PS8*

VMware products will support the controls of this family through organizationally developed policy. Products within the SDDC do not natively provide features that directly apply to the family’s intent.

Applicable Security Lens:
- System Access
- System Hardening
- System Monitoring

Applicable VMware Product:
- Administrative support

Risk Assessment (RA)

*NIST Controls RA1-RA5*

VMware products will support the controls of this family through organizationally developed policy. 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). SRM and vSphere Replication can support the assurance of meeting RTO and RPO criteria.

Applicable Security Lens:
- System Monitoring
- Network Protection
- Automated Security

Applicable VMware Product:
- Administrative support
- Site Recovery Manager
- vSphere Replication
Conclusion

To meet evolving regulatory needs, security programs now must define applicable controls at early states. From design, through to the end of a product lifecycle, VMware has focused on developing methodologies that set this tone.

Through the eight security lenses and in accompaniment of the VVD and VMware Cloud Foundation, the SDDC and EUC platform components provide users with a virtualization stack that adheres to the comprehensive requirements of NIST 800-53.

Organizations can seamlessly piece together full SDDC and EUC 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 comes from the 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 platform components and EUC suite within their architecture and NIST 800-53 security program.
Bibliography


2. “Secure Boot for ESXi 6.5 – Hypervisor Assurance.”
   https://blogs.vmware.com/vsphere/2017/05/secure-boot-esxi-6-5-hypervisor-assurance.html

3. “NIST Special Publication (SP) 800-53 Revision 4.”

Acknowledgements

VMware would like to recognize the efforts of the VMware product, marketing, legal, and sales teams that contributed to this paper and to the VMware Compliance and Cyber Risk Solutions Program team.

About VMware

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

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

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

About Tevora

Tevora is a leading security 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.

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 provides a verify of attestation and security services including ISO 27001, NIST, SOC1, SOC2 and is a Payment Card Industry Qualified Security Assessor (QSA), Payment Application Qualified Security Assessor (PA-QSA), and Point-to-Point Encryption Qualified Security Assessor (P2PE 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
DISCLAIMER: VMware solutions are designed to help organizations address various regulatory compliance requirements. This document is intended to provide general guidance for organizations that are considering VMware solutions to help them address such requirements. VMware encourages any organization that is considering VMware solutions to engage appropriate legal, business, technical, and audit expertise within their specific organization for review of regulatory compliance requirements. It is the responsibility of each organization to determine what is required to meet any and all requirements. The information contained in this document is for educational and informational purposes only. This document is not intended to provide legal advice and is provided “AS IS”. VMware makes no claims, promises or guarantees about the accuracy, completeness, or adequacy of the information contained herein. Nothing that you read in this document should be used as a substitute for the advice of an actual Cyber Security auditor or competent legal counsel.
## Appendix A: Summarized Product Mappings to NIST 800-53 Rev. 4

<table>
<thead>
<tr>
<th>VMware product</th>
<th>NIST 800-53 R4 Control Families Supported</th>
</tr>
</thead>
<tbody>
<tr>
<td>VMware NSX</td>
<td>AC, CM, IA, SC</td>
</tr>
<tr>
<td>vRealize Log Insight</td>
<td>AC, AU, CA, SC, SI</td>
</tr>
<tr>
<td>vRealize Network Insight</td>
<td>AC, AU, SC, SI</td>
</tr>
<tr>
<td>vRealize Orchestration</td>
<td>SI</td>
</tr>
<tr>
<td>vRealize Operations</td>
<td>AC, AU, CA, CM, CP, IA, MA, SI</td>
</tr>
<tr>
<td>vSAN</td>
<td>CA, IA, MA, SA, SC, SI</td>
</tr>
<tr>
<td>• vSAN Encryption</td>
<td></td>
</tr>
<tr>
<td>vSphere</td>
<td></td>
</tr>
<tr>
<td>• vCenter</td>
<td></td>
</tr>
<tr>
<td>• ESXi</td>
<td></td>
</tr>
<tr>
<td>• Replication</td>
<td></td>
</tr>
<tr>
<td>• Update Manager</td>
<td></td>
</tr>
<tr>
<td>• ESXi VM Encryption</td>
<td></td>
</tr>
<tr>
<td>vSphere encryption</td>
<td></td>
</tr>
<tr>
<td>vSphere</td>
<td></td>
</tr>
<tr>
<td>vCenter</td>
<td></td>
</tr>
<tr>
<td>ESXi</td>
<td></td>
</tr>
<tr>
<td>Replication</td>
<td></td>
</tr>
<tr>
<td>Update Manager</td>
<td></td>
</tr>
<tr>
<td>ESXi VM Encryption</td>
<td></td>
</tr>
<tr>
<td>Site Recovery Manager</td>
<td>CP, RA</td>
</tr>
<tr>
<td>AirWatch</td>
<td>AC, AU, CM</td>
</tr>
<tr>
<td>WorkspaceOne</td>
<td>CM</td>
</tr>
<tr>
<td>Common across all Products / Administrative</td>
<td>AT, CA, CP, IR, MA, MP, PE, PL, PS, RA</td>
</tr>
<tr>
<td>VMware Cloud Foundation</td>
<td>PL, SA, SC, SI, CA, IA, MA</td>
</tr>
</tbody>
</table>