Digital Operational Resilience Act

Product Applicability Guide for VMware Cloud Foundation 5.2

November 19, 2024

Table of Contents

Disclaimer

This document is intended to provide general guidance for organizations that are considering Broadcom solutions. The information contained in this document is for educational and informational purposes only. This document is not intended to provide advice and is provided “AS IS.” Broadcom 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 requirements and effectiveness of implementations.

Introduction

The European Union's Digital Operational Resilience Act (DORA) is a comprehensive regulatory framework designed to ensure the financial sector's resilience against Information and Communications Technology (ICT) related disruptions and threats. Implemented in 2023 with a compliance deadline of January 2025, DORA establishes uniform requirements for the security of network and information systems of financial entities and critical ICT third-party service providers operating in the EU. The regulation aims to consolidate and upgrade ICT risk requirements to address all facets of digital operational resilience in the financial sector, covering areas such as ICT risk management, incident reporting, digital operational resilience testing, and third-party risk monitoring. This harmonized approach seeks to establish a more consistent and robust digital operational resilience across the EU financial sector.

This document intends to help organizations who are implementing DORA compliance understand how their VMware Cloud Foundation (VCF) environment is well-suited to operational resilience, by listing features and capabilities present in VCF.

Intended Audience

The audience for this guidance is organizations that have deployed, or are considering deployment, of VMware Cloud Foundation 5.2.x as shipped by Broadcom.

There are engineered data center and hybrid cloud infrastructure products that implement VMware Cloud Foundation as part of their solution(s). If this is how you consume Cloud Foundation you should check with those products’ support before making changes based on this information. Broadcom cannot speak on behalf of third-party solutions.

Organizations must determine for themselves if they fall within the scope of the DORA legislation.

Format of this Document

This document is aligned to categories of requirements found in the Digital Operational Resilience Act, and are not a complete catalogue of requirements, as many of DORA’s articles and requirements cover organizational processes.

Security Hardening & Design

This document does not make specific security hardening recommendations. For baseline security guidance please consult the Security Configuration & Hardening Guides at https://bit.ly/vcf-scg.

Third Party Identifiers & Mappings

This document includes regulatory compliance and security control identifiers from external sources as a convenience to end users. This does not constitute endorsement, in either direction.

There is not a one-to-one mapping of product capabilities to third-party controls. A product capability, or set of capabilities, may be applicable to multiple controls. Conversely, a control may be satisfied with the use of multiple capabilities.

Control identifier numbers have been included from the Secure Controls Framework, version 2024.3, under the terms of the Creative Commons Attribution-NoDerivatives 4.0 International Public License. No modifications have been made to the control identifier numbers under the terms of the license.

References

Information about the European Union Digital Operational Resilience Act (DORA) can be found at:

https://www.eiopa.europa.eu/digital-operational-resilience-act-dora

Feedback

The primary source for this document is within our repository at:

https://github.com/vmware/vcf-security-and-compliance-guidelines

Feedback and issues can be filed through the Issues mechanism in that repository.

Access Control

VMware Cloud Foundation (VCF) integrates with third-party Privileged Access Management (PAM) solutions and identity providers through APIs, supporting both on-premises and cloud-based authentication for user and programmatic access. The platform enforces granular permissions through role-based access control (RBAC) while VMware vDefend Firewall capabilities manage network access controls.

Relevant Framework & Article:

- DORA: Article 9.4(c), 9.4(d)

Key Products:

- VMware Cloud Foundation (Core)
- VMware vDefend Distributed Firewall
- VMware vDefend Gateway Firewall

Cross Reference:

- SCF IAC-01, IAC-02

API, Ecosystem, and Integration

VMware Cloud Foundation (VCF) provides extensive API integration support for third-party tools such as IT asset management (ITAM), configuration management databases (CMDB), and security assessment tools.

The VMware Aria and VMware vDefend product suites deliver security assessment and continuous monitoring functionality.

Security teams can generate custom reports, export data, and automate tasks using product interfaces, PowerCLI, and APIs to maintain security and compliance requirements.

Relevant Framework & Article:

- DORA: Article 4.1, 4.2, 4.3, 5.4, 8.4, 8.5, 8.6, 9.1, 9.2, 23, 25.1, 25.2, 25.3

Key Products:

- VMware Cloud Foundation (Core)
- VMware Aria Operations
- VMware Aria Operations for Logs
- VMware Aria Operations for Networks
- VMware vDefend Distributed Firewall
- VMware vDefend Gateway Firewall

Cross Reference:

- SCF AST-01.1, AST-02, AST-02.1, CPL-01, CPL-01.2, OPS-01, VPM-06

Architecture Documentation

The VMware Aria Operations suite provides network topology mapping and infrastructure visualization tools to support architectural documentation and deployment planning. These built-in capabilities enable teams to diagram infrastructure and workload relationships and document implementations across the VMware Cloud Foundation (VCF) environment.

Relevant Framework & Article:

- DORA: Article 8.4

Key Products:

- VMware Cloud Foundation (Core)
- VMware Aria Operations
- VMware Aria Operations for Networks

Cross Reference:

- SCF AST-04

Automated Response

VMware vDefend provides automated threat detection and containment through integrated IDS/IPS, network sandboxing, traffic analysis, and network detection and response features. Upon threat detection, the platform can automatically initiate forensic snapshots, network isolation, workload suspension, or power state changes. VMware Live Recovery enables automated workload recovery from protected states for incident remediation. VMware vSAN, vSphere High Availability (HA), and vSphere Distributed Resource Scheduler (DRS) provide automated failover between configured fault domains.

Relevant Framework & Article:

- DORA: Article 9.4(b), 10.2, 14.1, 14.2, 14.3, 18.1, 18.1(a), 18.1(b), 18.1(c), 18.1(d), 18.1(e), 18.1(f), 18.2

Key Products:

- VMware Cloud Foundation (Core)
- VMware Live Recovery
- VMware vDefend Advanced Threat Prevention
- VMware vDefend Distributed Firewall
- VMware vDefend Gateway Firewall
- VMware vSAN

Cross Reference:

- SCF IRO-02, IRO-02.1, IRO-02.6, NET-08

Change Management Governance

VMware Cloud Foundation (VCF) with VMware Aria Automation provides workflow processes including change approval mechanisms to support organizational change management requirements. The platform implements granular role-based access control (RBAC) and additional authorization mechanisms to enforce access policies across infrastructure operations, as well as detailed logging to monitor changes.

Relevant Framework & Article:

- DORA: Article 9.3(a), 9.3(b), 9.3(c), 9.3(d), 9.4(e)

Key Products:

- VMware Cloud Foundation (Core)
- VMware Aria Automation
- VMware Aria Operations for Logs

Cross Reference:

- SCF CHG-01, CHG-02, CFG-01

Continuous Control Validation & Event Detection

VMware Cloud Foundation (VCF) integrates security monitoring capabilities through VMware Aria Operations suite (Operations, Operations for Logs, Operations for Networks) and VMware vDefend Firewall services. The platform combines signature-based intrusion detection with behavioral analysis for advanced threat detection. Real-time system alerts flag security misconfigurations and potential threats across the infrastructure stack, including policy and system health violations such as vSAN storage alerts. Security and operations teams can leverage interfaces, CLI tools, and APIs to automate security posture assessment and remediation workflows, as well as integrate third-party monitoring tools.

Relevant Framework & Article:

- DORA: Article 7(a), 7(b), 7(c), 7(d), 9.1, 9.2, 10.1, 10.3

Key Products:

- VMware Cloud Foundation (Core)
- VMware Aria Operations
- VMware Aria Operations for Logs
- VMware Aria Operations for Networks
- VMware vDefend Advanced Threat Prevention
- VMware vDefend Distributed Firewall
- VMware vDefend Gateway Firewall
- VMware vSAN

Cross Reference:

- SCF GOV-15.3, GOV-15.5, MON-01, MON-16, PRM-04, OPS-01

Data Backup & Recovery

VMware Live Recovery enables customizable business continuity and disaster recovery (BC/DR) management in VMware Cloud Foundation (VCF), either on an ad-hoc basis or part of a pre-existing playbook/runbook. The platform supports granular recovery time and point objectives (RTO/RPO) configurable at the object level. Organizations can perform non-disruptive BC/DR testing through VMware Live Recovery and VMware NSX integration.

The platform integrates with third-party storage replication solutions and backup providers through standardized APIs, while supporting flexible network connectivity options to meet data transfer requirements.

VMware HCX and the core VCF platform also offer data mobility and replication options, both locally and to remote targets.

Relevant Framework & Article:

- DORA: Article 11.1, 11.2, 11.2(a), 11.2(b), 11.2(c), 11.2(d), 11.2(e), 11.3, 11.4, 11.5, 11.6(a), 11.6(b), 11.7, 11.8, 11.9, 11.10, 11.11, 12.1, 12.1(a), 12.1(b), 12.2, 12.3, 12.6, 12.7

Key Products:

- VMware Cloud Foundation (Core)
- VMware HCX
- VMware Live Recovery
- VMware NSX

Cross Reference:

- SCF BCD-01, BCD-01.4, BCD-11, BCD-11.1, BCD-11.5, BCD-11.6

Metrics & Data Reporting Capabilities

VMware Cloud Foundation (VCF) offers comprehensive monitoring and analytics capabilities accessible through its interfaces, command line tools, and APIs. The platform provides operational metrics across compute, storage, networking, and security domains, including resource utilization, performance analytics, and capacity planning. Administrators can configure custom dashboards and automated reports with role-based access control, supporting integration with external monitoring and security systems. These capabilities enable organizations to maintain robust cybersecurity programs, meet compliance requirements, and track infrastructure analytics through detailed audit trails.

Relevant Framework & Article:

- DORA: Article 13.4

Key Products:

- VMware Cloud Foundation (Core)
- VMware Aria Operations
- VMware Aria Operations for Logs
- VMware Aria Operations for Networks
- VMware vDefend Advanced Threat Prevention
- VMware vDefend Distributed Firewall
- VMware vDefend Gateway Firewall

Cross Reference:

- SCF GOV-05

Operational Security and Privacy Requirements

Nearly every feature and capability of VMware Cloud Foundation (VCF) aligns to one or more pillars of the CIA Triad: confidentiality, integrity, and availability, allowing for granular operationalization of security and privacy policies at many levels according to how an organization would like to function. This includes identity federation and role-based access control, VMware vDefend network security, VMware Aria Automation for governance, VMware Aria Operations suite (Operations, Operations for Logs, Operations for Networks) for continuous system and security event monitoring, and VMware Live Recovery for disaster recovery/business continuity.

Relevant Framework & Article:

- DORA: Article 7, 7(a), 7(b), 7(c), 7(d), 9.3

Key Products:

- All

Cross Reference:

- SCF GOV-15

Redundancy & Failover

VMware Cloud Foundation (VCF) enables distributed computing across multiple sites through integrated availability features. The platform leverages VMware High Availability, Fault Tolerance, and Proactive HA for workload protection and outage prevention. VMware vMotion and VMware HCX offer workload mobility, both local and to remote targets. Additional resilience features include VMware vSAN Stretched Clusters, VMware Live Recovery, and VMware NSX multi-site networking. The platform implements redundancy and failover mechanisms across compute, storage, and network components to maintain workload availability and data protection.

Relevant Framework & Article:

- DORA: Article 12.4

Key Products:

- VMware Cloud Foundation (Core)
- VMware HCX
- VMware Live Recovery
- VMware NSX
- VMware vSAN

Cross Reference:

- SCF BCD-11.7, BCD-12.2

Secure Configuration Baselines

VMware Cloud Foundation (VCF) security configurations are documented in the VMware Security Configuration Guide. Broadcom also provides Defense Information Systems Agency (DISA) Security Technical Implementation Guides (STIGs) and STIG Readiness Guides and collaborates with the Center for Internet Security (CIS) to maintain synchronized security benchmarks.

Relevant Framework & Article:

- DORA: Article 9.3(a), 9.3(b), 9.3(c), 9.3(d), 9.4(e)

Key Products:

- VMware Cloud Foundation (Core)
- VMware NSX

Cross Reference:

- SCF CFG-02

Secure System Design

VMware Cloud Foundation (VCF) supports flexible infrastructure architectures while maintaining security controls through its modular design and policy-driven automation. Organizations can implement secure system designs that align with their specific security requirements and compliance frameworks.

Relevant Framework & Article:

- DORA: Article 9, 9.3(a), 9.3(b), 9.3(c), 9.3(d)

Key Products:

- All

Cross Reference:

- SCF SEA-01, SEA-03

Supply Chain

As an organization, and to the extent applicable for VMware Cloud Foundation implementations, Broadcom supports customer supply chain and procurement security processes.

Relevant Framework & Article:

- DORA: Article 28.1(a), 28.6, 28.7, 28.7(a), 28.7(b), 28.7(c), 28.7(d), 28.8, 28.8(a), 28.8(b), 28.8(c), 29.2, 30.1, 30.2, 30.2(a), 30.2(b), 30.2(c), 30.2(d), 30.2(e), 30.2(f), 30.2(g), 30.2(h), 30.2(i), 30.3, 30.3(a), 30.3(b), 30.3(c), 30.3(d), 30.3(e), 30.3(e)(i), 30.3(e)(ii), 30.3(e)(iii), 30.3(e)(iv), 30.3(f)(i), 30.3(f)(ii), 30.4

Key Products:

- All

Cross Reference:

- SCF TPM-05, TPM-05.2, TPM-05.7, TPM-08

System Lifecycle & Patching

VMware Cloud Foundation (VCF) provides integrated lifecycle management tools for infrastructure updates and patch deployment with zero-downtime maintenance capabilities. The platform includes built-in alerts for security vulnerabilities and available updates. Broadcom maintains a security advisory system through web publications and email notifications to inform customers of security updates and patches.

Relevant Framework & Article:

- DORA: Article 9.4(f), 13.1, 25.1, 25.2, 25.3

Key Products:

- All

Cross Reference:

- SCF THR-03, VPM-01, VPM-05

Unlisted Controls

Where an article is not listed the requirements are process requirements within the end user organization.

vmware®
by Broadcom

The term “Broadcom” refers to Broadcom Inc. and/or its subsidiaries. For more information, go to www.broadcom.com. All trademarks, trade names, service marks, and logos referenced herein belong to their respective companies. Broadcom reserves the right to make changes without further notice to any products or data herein to improve reliability, function, or design. Information furnished by Broadcom is believed to be accurate and reliable. However, Broadcom does not assume any liability arising out of the application or use of this information, nor the application or use of any product or circuit described herein, neither does it convey any license under its patent rights nor the rights of others.