Professional Services for VMware Cloud Foundation Assessment

At a glance

Reduce cybersecurity risk and ensure your environment is in alignment with regulatory compliance standards by evaluating the technical security configurations of your VMware Cloud Foundation infrastructure for VMware and industry security best practices.

Key benefits

- Gain valuable insights into how security controls are implemented in your VCF components
- Reduce the risk of exposure to increasingly frequent and dangerous cyberthreats
- Prioritized roadmap and actionable recommendations to remediate gaps and achieve target state
- Ensure VCF components are in alignment with compliance requirements

Availability

Please contact your VMware Client Solutions Executive for more information about this Statement of Work (SOW) service.

Business Challenge

In today's ever-changing environment, it can be challenging to know if your organization is fully leveraging your VMware architecture suite with cybersecurity best practices that protect your investments. Improving and evolving VMware configurations for the most effective vigilance and resilience against cyberthreats will help your operations maintain continuity and reduce risk footprint.

Understanding your current security posture and risk profile will help you set up security best practices that reduce your risk while maintaining required industry standards and meeting compliance regulations.

Service Overview

VMware's Professional Services security experts will perform a detailed technical security assessment of your VMware Cloud Foundation (VCF) infrastructure to VMware and industry security best practices. The service evaluates over 200 individual VCF configurations across five (5) VMware products: ESXi, vCenter Server, NSX-T Data Center, vSAN and SDDC Manager. The service utilizes a combination of workshops and technical configuration reviews to analyze the current state environment to desired target state. The service delivers a detailed findings report outlining assessment findings, actionable recommendations to achieve the target state and a roadmap to help prioritize remediation activities.

With the VMware VCF Compliance Assessment service, our team will help you:

- Assist in meeting industry and regulatory security requirements by mapping each individual configuration to the following security industry and regulatory frameworks:
    - NIST 800-53
    - PCI DSS
    - ISO 27001:2013

    - NIST 800-171/Cybersecurity Maturity Model Certification (CMMC).
- Identify configuration gaps to VMware and industry best practices
- Develop a clear roadmap with recommendations for advanced security controls
- Leverage proven VMware security expertise and guidance

In-Scope Products

This service can be used to evaluate the technical configurations for the following VCF Components:

Service Engagement At-a-Glance

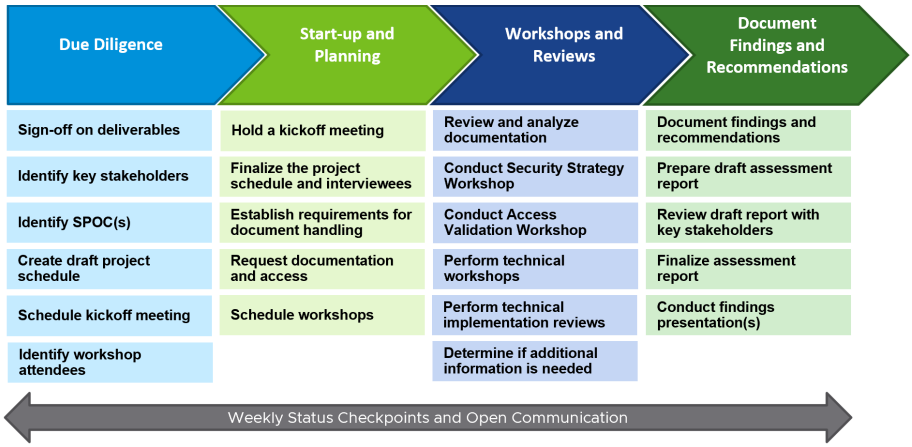
The service is delivered leveraging a four phased approach. During the Due Diligence phase, VMware security consultants and Project Manager will work with the Customer to identify a Single Point of Contact (SPOC) to ensure efficient communication between the Customer and VMware during the engagement. During this phase VMware will work with the Customer SPOC to identify key stakeholders and schedule the kickoff meeting.

In phase 2, Start-up and Planning, VMware will hold the project kickoff meeting, finalize the project schedule, document handling and access requirements, as well as identify Customer interviewees, contacts, and schedule technical workshops.

The Workshops and Reviews phase begins with the security consultant conducting the Compliance Strategy Workshop which is designed to review and align the Customer's compliance goals and objectives with the assessment. Next the security consultant will conduct an Access Validation Workshop to ensure the consultant has all required access and permissions to perform technical reviews. Once these workshops are completed the security consultant will work with Customers subject matter experts to review the current state environment. This is done via a series of technical workshops and technical implementation reviews leveraging scripts and manual configuration reviews.

During the final phase, Document Findings and Recommendations, the security consultant will perform the gap analysis of the current state environment to the target state. A draft findings report will be provided to key Customer

stakeholders for review and input. Once Customer feedback is received, the security consultant will conduct a findings presentation for Customer key stakeholders. The findings presentation will provide an overview of the engagement, technical findings, and prioritized recommendations/next steps.



Deliverables

At the conclusion of the security assessment, the Customer will be provided with the following deliverables:

Detailed Findings Report

- Detailed report highlighting all findings and recommendations for in-scope products and evaluation criteria
- Aligned to technical best practices

Scan Result Workbook

- Supplemental Excel Workbook documenting all product findings individually. Aids in remediation of settings identified in the Findings Report

Findings Presentation

- Consolidated presentation of prioritized recommendations
- Provide the customer with an executive level overview of current state in relation to target state. The presentation will highlight key gaps and recommendations
- Provide prioritized roadmap to achieve target state

Learn more

Visit vmware.com/services.

Benefits

VMware consultants' knowledge and expertise will help you make the most of your VCF architecture with cybersecurity best practices. When we help you with a VMware Cloud Foundation Compliance Assessment, you will achieve:

- Gain insights into the current security configurations of your VCF infrastructure
- An understanding of any possible gaps in your VCF components and how to remedy those gaps
- A prioritized roadmap and actionable recommendations to remediate gaps and achieve a target state
- Alignment of VCF security configurations to regulatory and industry frameworks