TECHNICAL WHITE PAPER
June 2025

Introducing Security and Compliance for VMware Telco Cloud Platform 4.0

vmware by Broadcom

Table of contents

About Introducing Security and Compliance for VMware Telco Cloud Platform 4.0

The *Introducing Security and Compliance for VMware Telco Cloud Platform 4.0* document offers general guidance for Communication Service Providers (CSPs) who have chosen VMware Telco Cloud Platform as their infrastructure platform and seek assistance in navigating on-premise compliance requirements. This document introduces the Compliance Kit for VMware Telco Cloud Platform and serves as its foundational element.

Legal Disclaimer: *This document is intended to provide general guidance for CSPs to address on-premise compliance requirements and the information contained in this document is for educational and informational purposes only. This document is not intended to provide regulatory advice. Broadcom makes no claims, promises or guarantees about the accuracy, completeness, or adequacy of the information contained in this document. CSPs should engage appropriate legal, business, technical, and audit expertise for the review of regulatory compliance requirements.*

Intended Audience

This document is intended for cloud architects, cloud administrators, and platform administrators who have an understanding of the VMware Telco Cloud Platform stack. It aims to introduce key concepts related to security and compliance as they pertain to VMware Telco Cloud Platform, offering insights and guidance for addressing these areas within your cloud platform.

Applicable Cloud Components

The guidelines laid out in the *Introducing Security and Compliance for VMware Telco Cloud Platform 4.0 and the Compliance Kit for VMware Telco Cloud Platform* are based on various components of VMware Telco Cloud Platform and are specifically tailored to its standard architecture model.

The compliance kit covers selected products from the VMware Telco Cloud Platform 4.0 bill-of-materials contained within the VMware Telco Cloud Platform Infrastructure Tier (foundational IaaS layer):

- VMware ESX™
- VMware vCenter Server®
- VMware vSAN™
- VMware NSX™

See VMware Telco Cloud Platform Release Notes for more information about supported product versions.

Compliance Kit for VMware Telco Cloud Platform

The Compliance Kit is a solution that builds on top of the VMware Telco Cloud Platform, incorporating core security principles. It addresses the most frequently requested compliance standards, regulations, and frameworks, providing targeted guidance.

The Compliance Kit is designed and validated to tailor security configurations without impacting the ability of VMware Telco Cloud Platform to meet its design and performance objectives. The kit can assist CSPs to secure infrastructure platforms while ensuring compliance with relevant standards and regulations.

Changes between subsequent releases of VMware Telco Cloud Platform are designed for stability and optimal upgrade experience. The guidance provided by the Compliance Kit for VMware Telco Cloud Platform has been validated and tested with a specific VMware Telco Cloud Platform release, but can still be used until a subsequent kit release is available. This guidance is not backward-compatible and must not be implemented for separate product components.

Download the Compliance Kit for VMware Telco Cloud Platform 4.0 here.

Composition

The Compliance Kit consists of documents, as detailed in Table 1, specific to the standard architecture model pertaining to the Infrastructure Tier of VMware Telco Cloud Platform.

Table 1: Components of the Compliance Kit for VMware Telco Cloud Platform

Document Name	Document Description	Intended Audience
VMware Telco Cloud Platform Product Applicability Guide	• Includes non-default configurations that can be implemented post-deployment of VMware Telco Cloud Platform for Standard Architecture	• System Integrator • Cloud Administrator • Platform Administrator
VMware Telco Cloud Platform Mapping Guide	• Includes audit procedures for auditors examining the VMware Telco Cloud Platform environment for compliance readiness	• System Integrator • Cloud Administrator • Security Professional • Auditor

The Compliance Kit is designed to work holistically. Each document listed in Table 1 supports the overall blueprint and fosters trust across multiple personas that may interact with the lifecycle of a system operating within a compliance context: architect, system administrator, system integrator, security professional, and auditor.

Each product in VMware Telco Cloud Platform stack can support a variety of default and non-default configuration settings that must be evaluated and if necessary, modified to meet security and compliance requirements.

The VMware Telco Cloud Platform Product Applicability Guide outlines the post-deployment best practices to implement non-default configurations for different products in the VMware Telco Cloud Platform. Default configurations can be verified and excluded from the configuration process considering that they are inherently configured in the products. For non-default configurations, following the complete best practices as prescribed in the product applicability guide is recommended to ensure that the foundational IaaS layer performance is not compromised.

The VMware Telco Cloud Platform Mapping Guide supports the post-implementation process and audit process. It includes procedures to validate both default and non-default configurations. In the VMware Telco Cloud Platform Mapping Guide, mappings between configurations and compliance controls provide a comprehensive inventory of configurations designated as default or non-default.

Coverage

The Compliance Kit for VMware Telco Cloud Platform covers the core (foundational IaaS layer) products in the Infrastructure Tier of VMware Telco Cloud Platform:

- VMware ESX™
- VMware vCenter Server®
- VMware vSAN™
- VMware NSX™ Data Center

Security by Design

Security and compliance guidance includes both default configurations that are available out-of-the-box for various products in VMware Telco Cloud Platform and non-default configurations that can be implemented post-deployment.

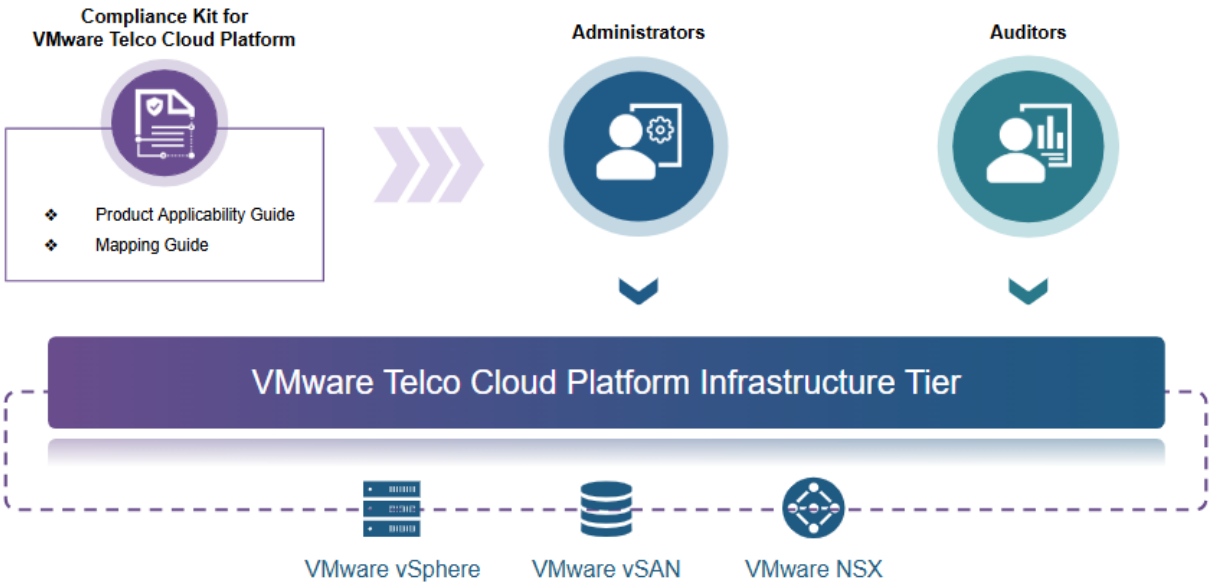

Figure 1: Compliance Kit for VMware Telco Cloud Platform

The Compliance Kit for VMware Telco Cloud Platform is designed with two key personas in mind: System administrators/implementation teams and auditors. System administrators and implementation teams use the VMware Telco Cloud Platform Product Applicability Guide to assess and implement non-default configurations, ensuring that the VMware Telco Cloud Platform is tailored to meet the specific needs and compliance requirements of the CSPs. In some cases, it is essential to evaluate the default configurations to confirm that they align with the organization's policies, procedures, and regulatory requirements.

For auditors, the VMware Telco Cloud Platform Mapping Guide provides detailed information on evaluating both default and non-default configurations. It provides auditors a foundational guidance required to assess whether the configurations are fully compliant with the industry standards and organizational policies, enabling a thorough and accurate audit process.

Default configurations

Security configurations based on compliance requirements that are available out-of-the-box in various products of VMware Telco Cloud Platform. While the parameter values may need to be adjusted to meet specific regulatory requirements, these configurations are designed with security best practices in mind and are included in the current implementation by default.

Non-default configurations

Custom security configurations that CSPs might need to implement to meet specific regulatory requirements. These configurations require additional input to identify relevant compliance requirements, select appropriate settings based on the guidance provided, and set configurations to align with the target regulation.

Now that you understand the Compliance Kit for VMware Telco Cloud Platform, let's outline some of the security and compliance principles and concepts that served as the fundamentals in the development of the Compliance Kit.

Security Principles

Across all regulations or standards, security principles dictate the mindset for applying security controls in the VMware Telco Cloud Platform. The security concepts outlined in this document are treated as guiding principles for developing a secure VMware Telco Cloud Platform environment, leveraging the capabilities available across all products of the stack. These principles are not only reflected in the recommended configurations in the kit but are also inherent in the product's core capabilities. CSPs that adopt these guidelines can expand these capabilities across the Telco Data Center to include people, processes, and technology controls. However, each organization must tailor these principles to its specific needs and align the implementation with its security objectives.

Separation of duties

- Assign specific roles to users to separate conflicts of duty
- Roles can be customized and further tailored as needed
- Restrict the use of super users
- Create service accounts where possible
- Create separate accounts for system-to-system communication
- Separate production from development environments
- Evaluate access to create, edit, or delete permissions
- Assign read-only access where possible

Least privilege

- Deactivate unused services
- Do not grant or retain permissions longer than needed

Confidentiality - Integrity - Availability (CIA)

- Protect the data and the assets used to access it
- Confidentiality pertains to the authorization required to access the data
- Integrity applies to the authorization required to modify the data
- Availability refers to the accessibility of the data for authorized users

Defense in depth

- Do not allow lateral movement
- Isolate environments
- Patch systems
- Implement layered security

Zero trust

- Implicit access denial regardless of origin
- Treat the internal network as a potential threat vector
- Access is restricted via a trust broker
- Applications are hidden from discovery

Secure Software Development Life-Cycle (SDLC)

- Broadcom performs static code analysis
- Broadcom performs penetration testing
- Broadcom performs the vulnerability scan
- Align development with Broadcom internal software development security guidelines/procedures

Data in transit protection

- Encryption of virtual machines during migration between hosts
- Use of encryption mechanism when a super user is interacting with server consoles

Data at rest protection

- Encryption of virtual machines while powered off (at rest)

Trusted Computing Base (TCB)

- Architecture view that brings together the collection of all the hardware, software, and firmware components (including the security kernel and reference monitor)
- Brings a unified security policy and baseline consistent across various layers, abstractions, and detailed components to meet security requirements.

Security Architecture

Security in VMware Telco Cloud Platform is evaluated with a clear objective to balance best practices with usability and performance. For VMware Telco Cloud Platform implementations, post-deployment, security must be handed over to a dedicated team to augment and monitor the security posture. Attack vectors and compliance guidelines are constantly evolving so the information provided is often used to establish a baseline, not an absolute, or complete picture.

NIST 800-53 Revision 5, risk rating Moderate, forms the security baseline used to evaluate VMware Telco Cloud Platform. NIST 800-53 is chosen to be the baseline because of its vast array of controls and is often used by other regulations as part of their reference framework.

NIST is a risk-based framework, which requires each organization to assess its own risk posture and identify applicable controls. The Compliance Kit for VMware Telco Cloud Platform does not remove this step. The VMware Telco Cloud Platform security design and compliance mappings inform the reader of both design decisions and security configurations.

However, the security design of VMware Telco Cloud Platform is insufficient on its own. Each CSP must implement a comprehensive security framework that includes the supporting security architecture, technologies, processes, and personnel to conduct thorough evaluations. Factors such as applications, workload domains, software-defined networking topology, customer data, privacy, and myriad other factors must be evaluated as part of the broader security architecture.

Super users of the system inherit various technologies and typically work with security specialists to implement controls effectively. VMware Telco Cloud Platform has evaluated many design decisions that are incorporated with the overall design as outlined by VMware Telco Cloud Platform Reference Architecture.

Subsequent deployments benefit from post-implementation security health checks to enhance the security posture of the CSPs as it relates to the VMware Telco Cloud Platform Reference Architecture used in conjunction with the VMware Telco Cloud Platform.

Governance, Risk, and Compliance and Mapping

This guidance describes the security configurations that can support Governance, Risk, and Compliance (GRC) considerations. Due to the variety of compliance standards and different business needs, CSPs should exercise due care to identify and map VMware Telco Cloud Platform configurations against a targeted regulation.

Where applicable, examples of audit artifacts are included as evidence in the VMware Telco Cloud Platform Mapping Guide Appendix, with a focus on compliance and producing evidence to meet control requirements. To map configurations across regulatory standards, we use a third-party tool developed by the Unified Compliance Framework (UCF). This approach eliminates a subjective, manual control cross-walk approach and replaces it with a repeatable and data-driven methodology. The crosswalk or reference across regulatory standards is not a mapping matrix but instead utilizes the UCF as a shared library of controls, linked to the underlying citation text within each standard. This shift removes subjective mapping and replaces it with a programmatic, software-driven mapping engine.

In some cases, the regulation may be too generic or vague and that can reduce the mapping efficacy. In these cases, an additional review is performed to isolate new citation text and then included in the engine through the corresponding and newly identified UCF control. No mapping is provided with an accompanying UCF control and accompanying citation text for each regulation. If no mapping is identified, the mapping uses the best practice text to clarify that mapping was not found but to keep up with the security principles, the configuration is recommended.

The compliance mapping is a subject of expansion, as more security controls are evaluated, including additional compliance domains and regulations.

Control Definition

Controls are designed to mitigate risk. These are derived by using a Risk Framework, such as the Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy, published by NIST, special publication number 800-37, Revision 2. NIST 800-53 R5 control catalog is used to develop a baseline of controls compared to the software-defined data center technical and security configurations. These security configurations must be evaluated and considered against the risk management framework used by your organization. Furthermore, frameworks such as ISO27001, which is widely used by CSPs, can be coupled with its Annex A, ISO27002, or ISO27005 to evaluate controls to mitigate risk.

Cybersecurity Considerations

It is the responsibility of security, compliance, and audit teams in your organization to verify that configurations meet the appropriate compliance requirements. The attack vectors and compliance guidelines are constantly evolving, which requires constant monitoring and risk management processes.

Business Impact Assessment

Measuring risk and evaluating scope may require performing a business impact assessment. This analysis can inform IT security and audit professionals about the different areas of the Telco Data Center that require more controls, tightened access restrictions, micro-segmentation, enhanced disaster recovery, and additional monitoring.

Item No: vmw-bc-wp-tech-a4-word-2025 Jun-25