VMware Sovereign Cloud

Native Sovereign Data Protection with the ultimate choice and control

VMware Sovereign Cloud is the most complete and secure solution for data sovereignty that protects against unauthorized access, breaches, or cyberattacks. By working with verified partners, Sovereign Cloud keeps data completely within the jurisdiction and under the owner's control, yet isolated from the provider's core network and the internet.

Along with data independence, protection, management, and control, VMware Sovereign Cloud providers offer local expertise and value-added sovereign cloud services to help organizations comply with regulations and data privacy laws. The locally implemented and operated sovereign cloud ensures flexibility, choice, and control so you don't need to worry about vendor lock-in or excessive cost.

1. Local Residency (Data/Metadata)

All data must reside in the relevant sovereign country and be subject to and compliance with the applicable local data protection law(s).

2. Full Jurisdictional Control

Governmental authorities in the relevant sovereign country where the data was obtained, have sole jurisdictional control and power over the data and that it is not within the legal or technological purview of foreign governmental bodies, legal authority or access from outside the sovereign country.

3. Encryption with external keys to Clients (BYOK)

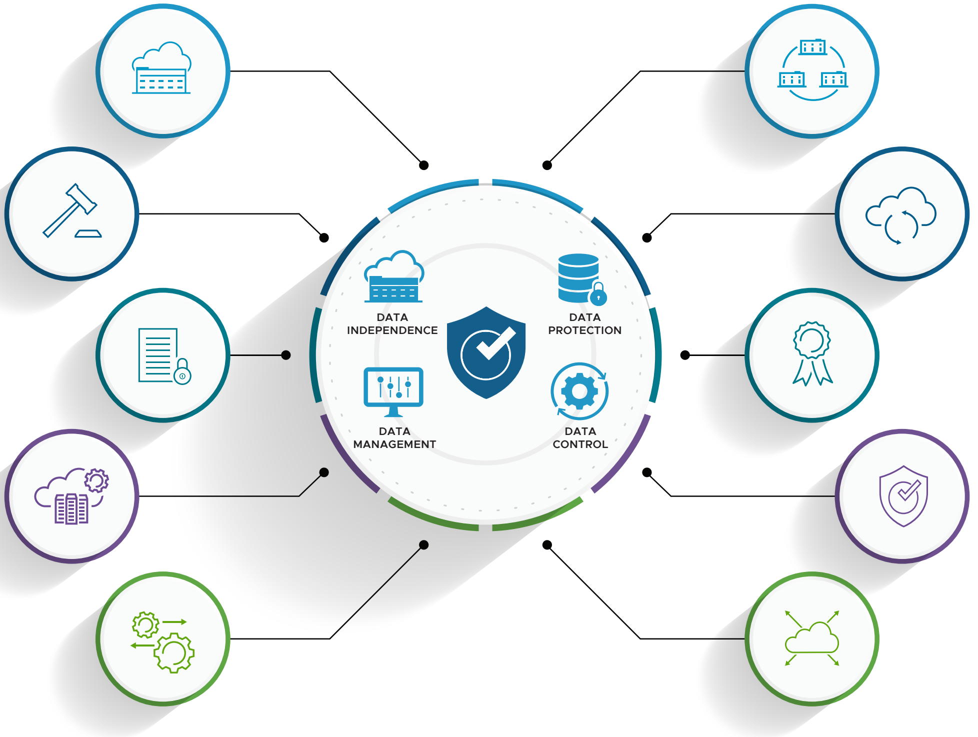
Data encryption at rest, network encryption for data in transit and key management system (KMS) that remains under the control of the customer or partner within the respective country.

4. Local Entity

Managed by a legal entity that will own, operate and manage the Sovereign Cloud Offering which is located and incorporated in the applicable sovereign country where such offering will be made available, and has no affiliate (including but not limited to, controlling entities, controlled entities, and entities under common control) or any corporate relationship with any corporate entity located outside the sovereign country where the Sovereign Cloud Offering is made available.

5. Local Operations

Authorized personnel who operate and manage the Sovereign Cloud offering to specific individuals who have applicable sovereign country-specific security clearances for the applicable sovereign country; and full privilege access auditing and management.



6. Resiliency with 2 data center locations (plus offline Archives)

The Sovereign Cloud Offering is managed and operated from at least two data center locations within the applicable sovereign country. The data centers must meet Tier III (or equivalent) or higher data center classification, per Uptime (99.982% availability or higher) and backup services with multiple copies.

7. Full Reversibility (portability without lock-in)

Support and manage hybrid cloud deployments across different locations (e.g., customer on-premises and cloud), with a consistent architecture (such as VCF) that ensure interoperability between different locations….and ability to migrate workloads to or from the cloud without changing or reworking applications, with full reversibility to prevent cloud vendor lock-in.

8. Security certification

Has relevant industry and/or government certifications and attestations that the Sovereign Cloud offering holds and are required in your jurisdiction for end user workloads (e.g. ISO/IEC 27001, ISO 27017, ISO 27018, CSA STAR, Cyber Essentials, FedRAMP, SecNumCloud, ENISA, IRAP, ISMAP, HIPAA, PCI, etc.).

9. Zero Trust with Logical Network segmentation

Follow zero trust security posture with logical network segmentation in and across cloud country consistent with a common policy framework.

10. Isolation for some or all parts of the Sovereign Cloud offering in segregated spaces

Isolation for some or all parts of the Sovereign Cloud infrastructure in segregated space or environment.

vmware® by Broadcom

Item No: vmware-by-broadcom-10pt-criteria-one-pager-v1.2-c 5/24