DIGITAL SOVEREIGNTY DECODED | COMPANION REFERENCE

Digital Sovereignty: Framework & Maturity Reference

Sovereignty is not a binary state. It spans four interdependent pillars, each requiring evidence, not just the documentation. Your deployment model determines which of these controls you own and which you inherit from a provider. Use the deployment reference to calibrate before applying the maturity model.

Pillar	The Question It Answers	Where Organizations May Fall Short	What Good Can Look Like
Data Locality	Where does data – and metadata – reside?	Assuming in-region storage resolves locality requirements. Control-plane traffic and telemetry flows are rarely mapped.	A comprehensive data map – primary data, metadata, and control-plane artifacts – with documented controls for each.
Technological Sovereignty	Who controls the encryption keys, and under what conditions? Are changes verified and traceable in a persistent log?	Assuming Bring Your Own Key (BYOK) provides the same protection as Hold Your Own Key (HYOK). In SaaS models, HYOK may require additional configuration or platform-tier selection.	Key is independently held (HYOK where required) and tested under crisis and legal-compulsion scenarios. In SaaS deployments, key is held within the accreditation boundary.
Operational Sovereignty	Who operates the environment, from where, and under which law?	Uninventoried vendor access and out-of-region operations. In SaaS, customer visibility into Commvault/partner operator jurisdiction requires explicit contractual confirmation.	Every access pathway is mapped, jurisdictionally documented, and audited on a defined cadence. In software deployments, this is fully customer-controlled. In SaaS, accreditation terms (e.g., EUSC citizen-operator requirements) govern this.
Jurisdictional Sovereignty	What legal framework governs access and recovery? Which legal entity owns the platform and the service? Where is that legal entity located? How is that legal entity formed, and can it be acquired or controlled by a non-sovereign entity?	They may face unclear data protection standards, cross-border legal inconsistencies, and weak accountability from providers. They may lack visibility and control over where their data resides, who can access it, and how it may be exposed to foreign jurisdictions without transparent safeguards.	Comprehensive understanding of what legal frameworks govern your data access and recovery.

THE OVERARCHING UMBRELLA: COMPLIANCE & CERTIFICATION

Certifications: Proven and achieved certifications – *such as C5 in Germany, SecNumCloud in France, ISO 27001, etc.* – provide verifiable evidence that sovereignty requirements are consistently enforced with regular audits, and ongoing evidence.

DEPLOYMENT MODEL REFERENCE

YOUR DEPLOYMENT MODEL DETERMINES YOUR SOVEREIGNTY POSTURE

SaaS in Sovereign Region

e.g., AWS EUSC

Sovereignty controls are largely inherited from the platform accreditation. The provider manages the environment; the customer's sovereignty posture depends on what that accreditation covers – and what it leaves open.

Data Locality: Residency enforced by platform tier. Verify that metadata, control-plane traffic, and telemetry are also scoped to the accredited region – not just primary data.

Technological Sovereignty: BYOK is typically available. HYOK (where the customer holds keys independently of the provider) may require a higher platform tier. Confirm key custody terms are within the accreditation boundary.

Operational Sovereignty: Governed and defined by platform operators augmented with customer sovereignty level. The overall achievement is governed by both the customer and partner. Verify what the accreditation covers and what requires contractual confirmation.

Jurisdictional Sovereignty: Legal jurisdiction is inherited from the platform.

Certifications: Describe what the platform provider has committed and achieved.

Software in Partner Infra, Customer Infra, Sovereign/Trusted Cloud subscriptions

e.g., on-premises, sovereign cloud, trusted cloud, private cloud, partner-managed data center, disconnected/air-gapped environments

The customer or partner owns and operates the full environment. Sovereignty controls are defined, enforced, and evidenced by the operating organization – not inherited from a provider.

Data Locality: Full control over where data, metadata, and control-plane artifacts reside. No dependency on hyperscaler region selection or provider data-flow governance.

Technological Sovereignty: HYOK is fully achievable. Key custody sits entirely within the sovereignty boundary, independent of any cloud provider.

Operational Sovereignty: All access pathways, platform operators, and administrative operations are within the customer or partner boundary. Jurisdictional exposure is entirely within the operating organization's control.

Jurisdictional Sovereignty: Is inherited from the operating organization.

Certifications: Earned and maintained internally – not received from a provider.

Commvault is designed to operate across both models. Whichever deployment path your organization takes, the same questions apply: what controls do you own, what have you inherited, and can you evidence both under real conditions?

SOVEREIGNTY MATURITY MODEL

	Reactive: **Awareness Without Evidence**	**Defined:** **Documented, Not Yet Tested**	**Validated:** **Demonstrated Under Realistic Conditions**
Data Locality	Know where primary data lives.	Map metadata and control-plane flows.	Test flows regularly and document the results.
Technological Sovereignty	Utilize provider-managed encryption keys. No access to architectural documentation or data flow maps.	Bring your own keys (BYOK). Architectural documentation, data flows, and service dependencies are available.	Hold keys independently (HYOK) strictly outside the provider's environment. Documentation is current, independently verified, and tested against actual system behavior. Note: In SaaS deployments, HYOK availability depends on platform-tier selection.
Operational Sovereignty	Access dependencies have not been inventoried. Note: In SaaS models, operator jurisdiction is governed by platform accreditation – not directly by the customer.	Map who can access your environment and from where.	Test access pathways with ability to verify compliance. In SaaS: Accreditation terms are verified and tested. In software: All access pathways are within the sovereignty boundary.
Jurisdictional Sovereignty	Rely on certifications as sovereignty proof.	Certifications are tied to active controls. In SaaS: We understand which controls are platform-inherited vs. our own responsibility.	Controls are tested and verified. In SaaS: Inherited platform certifications are validated against actual obligations. In software: Certifications are earned and maintained by the operating organization.

Most organizations find they are validated in fewer areas than expected – and reactive in at least one area they considered covered.
The gaps are the program. Full Readiness Report at **readiverse.com/digital-sovereignty.**