

WHITE PAPER

Digital Sovereignty: From Policy to Practice, a Reference Guide for Risk Teams

By Ruben Renders,
Solutions Director, MSPs & Sovereign Platforms, Commvault



READIVERSE

Table of Contents

Introduction	4
A More Pragmatic Approach Takes Shape	7
The Inception of Minimum Viable Sovereignty	8
Digital Sovereignty: Strategic and Operational Implications	9
Governance and Ownership	9
Risk Management	9
Legal and Compliance	10
Procurement and Vendor Management	10
Enterprise Architecture and Infrastructure Architecture	10
Software Architecture	11
FinOps	11
Cloud Platform Architecture	11
Networking and Connectivity	11
Incident Response	12
Operations	12
The Introduction to Commvault Geo Shield	12
EU CSF: A Procurement Framework	15
EU CADA: A Regulatory Proposal to Strengthen Digital Infrastructure	17
The Regulatory Horizon	18
Practitioner Best Practices	20
Conclusion	21

Executive Summary

Digital sovereignty has moved from a compliance checkbox to a strategic imperative. Organizations that treat it as a technical problem – solved by selecting the right cloud region or deploying an on-premises alternative – will find themselves unprepared for the audit, the incident, and the examination that follows.

This paper provides a practitioner-level framework for organizations and their teams implementing a digital sovereignty strategy. It defines the four pillars of sovereignty and the overarching compliance and certifications layer that validates them, explains the governance model required to make it work, and introduces minimum viable sovereignty (MVS): the discipline of calibrating controls to actual obligations rather than pursuing maximum sovereignty at maximum cost.

Three themes run throughout:

- First, sovereignty is not a destination – it is a continuously demonstrated posture that spans procurement, architecture, legal, and operations.
- Second, it must be owned at the executive level, typically by the Chief Risk Officer or equivalent risk-accountable executive, with structured involvement from across the C-suite.
- Third, most organizations will not choose a single sovereign degree – they will span several simultaneously, and the governance challenge is maintaining consistent, auditable controls across that mixed estate.

This paper is written for the practitioners and cross-functional teams responsible for turning executive sovereignty commitments into operational reality. It is a companion to the [Digital Sovereignty Readiness Report](#), which addresses the same topic at the executive level.

INTRODUCTION

The global digital economy is built upon infrastructure that is largely transnational. Hyperscalers like Microsoft Azure or Google Cloud Platform are not designed as isolated environments. Although services are regionalized for latency and compliance, they rely on globally interconnected infrastructure, shared control planes, upstream services, and internet exchange networks to deliver consistent and resilient services worldwide.

While this model has accelerated innovation and economic growth, it also has introduced structural dependencies. Many organizations and governmental institutions rely on a small number of foreign technology providers for critical infrastructure, cloud services, and data platforms. This concentration raises concerns regarding regulatory jurisdiction, data access, supply chain resilience, and national security.

Digital sovereignty has rapidly evolved into a strategic priority for organizations, governmental institutions, and technology providers. As organizations become increasingly more dependent on cloud infrastructure, AI, and digital platforms, control over data, IT systems, and digital operations is no longer solely a technical matter. It is a matter of operational resilience, regulatory compliance, and strategic autonomy.

In recent years, many organizations have invested heavily in developing cyber resilience strategies designed to withstand and recover from digital disruptions. However, a growing number of technology and business leaders worldwide are recognizing that resilience alone is not sufficient.

Increasing geopolitical tensions, evolving regulatory frameworks, and concerns around jurisdictional control have elevated digital sovereignty to the executive agenda. Organizations embarking on this journey often find that sovereignty is far more complex and multidimensional than initially anticipated, requiring a more structured, organization-wide framework that spans all functions.

We are entering the early phase of the next evolution in the IT industry, one shaped and accelerated by regulation, legislation, and pragmatic governance. Initial market signals are already visible:

- The ongoing development of the legislative and regulatory framework by governmental bodies such as the European Union.
- The continued development of hybrid extensions like Azure Local.
- The emergence of trusted/partner cloud models.
- The rollout of sovereign regions by public hyperscalers.
- The maturation of partner ecosystems delivering sovereign cloud services.
- The increasing clarity of vendor and public hyperscaler sovereign strategies.

In parallel, both customers and partners are formalizing their own sovereignty frameworks, increasingly anchored in MVS principles. These approaches prioritize achieving required levels of compliance, control, and risk mitigation while deliberately balancing the financial trade-offs between cloud elasticity and cost efficiency. This helps organizations meet sovereignty objectives without undermining the economic advantages that underpin cloud adoption.

The regulatory frameworks, certification schemes, and legislative initiatives referenced in this paper are summarized for general informational purposes only and are current as of the date of publication. Digital sovereignty is a rapidly evolving domain, and applicable laws, regulations, and standards may change.

The information provided herein does not constitute legal, regulatory, or compliance advice, and organizations should evaluate their specific obligations based on their own circumstances, jurisdictions, and regulatory environment. Commvault makes no representation that the regulatory descriptions in this paper are complete, current, or applicable to any particular organization or use case.

Product descriptions and capability statements in this paper are general in nature and do not constitute warranties, guarantees, or binding commitments regarding the performance, functionality, or compliance of any Commvault product or service. Actual capabilities may vary based on configuration, deployment model, and operating environment.

THE KEY DIMENSIONS OF DIGITAL SOVEREIGNTY

Digital sovereignty can be understood as the capability for an organization to retain effective control over its digital assets, operations, and data, regardless of where technology platforms, or infrastructure are located.

Digital sovereignty provides the resilience organizations need to navigate contractual – and geopolitical – disruptions.

At a practical level, this means a platform or solution must enable an enterprise to operate locally within a globally interconnected technological ecosystem. Organizations must be able to maintain operational continuity and governance even when systems become partially or fully disconnected from external dependencies.

Most modern technology is created, owned, or managed by foreign or external providers. As a result, digital sovereignty often involves achieving sovereign outcomes while relying on non-sovereign actors. This arrangement is commonly described as “paper-backed sovereignty,” where contractual, legal, and policy mechanisms are used to enforce sovereignty objectives.

Paper-backed sovereignty alone is not sovereignty; when engaging with a non-sovereign actor, baseline sovereignty must be established through enforceable technical controls and operational controls, reflecting the emerging consensus that sovereignty is control-based rather than trust-based.

However, contractual assurances alone are insufficient. Organizations should consider implementing technical, operational, and governance controls that enable sovereignty requirements to be enforceable in practice, not merely guaranteed through contractual commitments. The four pillars of digital sovereignty according to Commvault are:

- **Data locality:** Where is the platform and the data it manages located? Are there any metrics or information shared with supporting infrastructure like monitoring systems or AI data that reside in a different location?
- **Operational sovereignty:** The ability to independently control and execute the operation of digital systems, including administration, access, and runtime governance, within defined authority boundaries and fenced off from extraterritorial access.
- **Technological sovereignty:** The degree to which an organization controls and understands its technology stack – architecture, dependencies, and lifecycle – without undue reliance on external providers.
- **Jurisdictional shielding:** The capability to protect data and operations from exposure to foreign legal claims or extraterritorial regulations through legal, technical, and organizational safeguards.

Spanning all four pillars is an overarching requirement: compliance and certifications, or the formal validation that technical and operational controls across each pillar are consistently enforced and auditable.

- **Certifications** such as Europe’s Cloud Certification Scheme (EUCS), Germany’s Bundesamt für Sicherheit in der Informationstechnik Cloud Computing Compliance Criteria Catalogue (BSI C5), France’s SecNumCloud Qualification, and ISO 27001 provide the documented evidence and external validation that sovereignty requirements are being met. But certifications describe intent. The strongest sovereignty postures treat them as the floor, not the ceiling.

- **Industry-led frameworks** such as the European Cloud Sovereignty Framework (CSF), the GAIA-X cloud sovereignty initiative and the earlier CIGREF Trusted Cloud Framework – developed and maintained by a consortium of major French enterprises – offer structured methodologies for assessing and quantifying sovereignty. As digital sovereignty remains an emerging domain, these frameworks serve as a solid baseline for developing a tailored qualification model.
- **Regulation and legislative acts** establish the legal and institutional framework that determine how data, digital infrastructure, and online services are governed. By setting rules on data localization, privacy, cybersecurity and platform accountability, they help enable regional blocs to exercise control over digital systems.

The overall model is designed to validate whether organizations can protect themselves today and in the future against risks related to digital sovereignty.

One illustrative example involves the acquisition of a Dutch-based company responsible for hosting certain Dutch government IT applications and associated data. Following the acquisition, the Dutch government's digital sovereignty posture was called into question, as an American parent entity could potentially be subject to disclosure obligations under frameworks such as the CLOUD Act or FISA.

This type of risk is precisely what frameworks like SecNumCloud in France aim to mitigate. As currently defined, SecNumCloud sets requirements to maintain effective EU/French control, including restrictions on non-EU ownership thresholds, with the objective of preserving operational and legal sovereignty over critical data and infrastructure.

Most organizations do not adopt a singular tier of sovereignty; rather, they engage with multiple tiers concurrently, applying the most rigorous sovereign controls to their sensitive workloads while accepting increased provider dependency for less critical systems.

The primary governance challenge is enabling consistent and auditable sovereignty controls across this diverse environment, which is the intended purpose of an MVS framework.

Consequently, organizations assess necessary levels of digital sovereignty based on corresponding costs, viewing it as a continuum instead of a fixed benchmark.

Requirements differ by geography and sector. For instance, Germany and France implement stricter regulations compared to Portugal, and financial services or government organizations typically face more demanding obligations than those in manufacturing or healthcare. Addressing these variations is essential to harmonize sovereignty strategies with local regulatory requirements and industry-specific constraints.

We anticipate the emergence of a standardized labeling mechanism – based on Union Assurance Levels as described in the Cloud & AI Development Act, which follows a similar principle as Europe's Nutri-Score rating system – to transparently communicate the level of digital sovereignty a solution provides. This would enable organizations to quickly assess and compare offerings based on clearly defined sovereignty criteria.

A MORE PRAGMATIC APPROACH TAKES SHAPE

Digital sovereignty extends far beyond technology architecture. It encompasses where systems and data are hosted, who can access them, how they are operated and supported, and which legal jurisdictions ultimately govern them.

Achieving sovereignty requires a comprehensive, layered evaluation of the entire digital ecosystem – from colocation facilities and cloud infrastructure to network routing, application platforms, operational processes, and the personnel who manage or access critical data.

That's where a more pragmatic approach comes into play. Digital sovereignty becomes a practice that flows through all functions of the organization, and which is aimed at balancing the benefits of cloud technologies and services against associated sovereignty requirements and risk exposure.

Most organizations are likely to adopt an MVS strategy, deliberately distributing data and platforms across a range of sovereign deployment models to optimize control, compliance, and economic value.

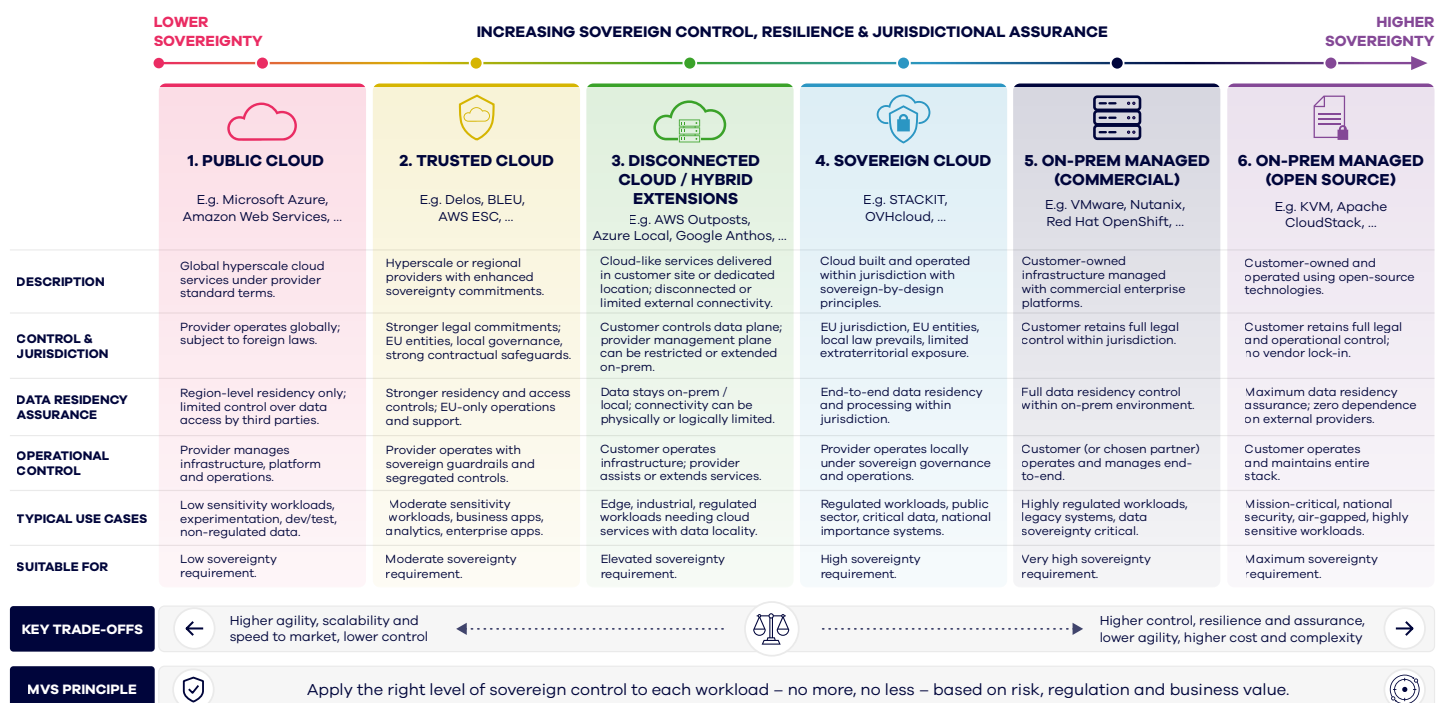
The primary deployment modalities through which organizations place and operate workloads today are:

- **Public cloud**, e.g., Microsoft Azure, Google Cloud Platform, and Amazon Web Services.
- **Trusted cloud**, e.g., Delos Cloud, BLEU, and AWS ESC.
- **Disconnected cloud/hybrid extensions**, e.g., AWS outposts, Azure Local, and Google Anthos.
- **Sovereign cloud**, e.g., STACKIT and OVHcloud.
- **On-prem managed (commercial)**, e.g., VMware, Microsoft Hyper-V, Nutanix, and Red Hat OpenStack Services on OpenShift (RHOSO).
- **On-prem managed (open source)**, e.g., Apache CloudStack.

The solutions referenced in the last bullet point are commercially supported by organizations such as ShapeBlue and Red Hat, while preserving the flexibility to engage directly with the upstream open-source community. This allows customers to transition away from commercial support, if desired, without losing access to ongoing community-driven development and support.

MINIMUM VIABLE SOVEREIGNTY (MVS) – SIX DEGREES OF CLOUD SOVEREIGNTY

Applying the right level of sovereign control to the right workload, based on risk, regulation, and business need.



In specific operating contexts, the scalability and on-demand capacity of public cloud infrastructure can deliver superior economic and operational efficiency compared to equivalent on-premises deployments.

Where this trade-off is justified, organizations can adopt a paper-based sovereignty posture – relying on contractual, legal, and governance controls rather than full technical isolation – supported by rigorously defined, documented, and periodically validated exit strategies that enable workload portability and controlled provider disengagement.

To further mitigate transition risk, organizations should incorporate Temporary Service Agreements (TSAs) into their exit planning. TSAs establish predefined terms under which the incumbent provider continues delivering critical services for a limited period post-termination. This helps reduce the likelihood of service discontinuity by:

- Enabling continuity of essential operations while migration or repatriation activities are completed.
- Providing a structured buffer period to stabilize replacement environments.
- Defining service levels, support scope, and timelines upfront to avoid ambiguity during disengagement.
- Enabling phased cutovers rather than abrupt termination, helping minimize operational and customer impact.

When properly scoped and contractually enforced, TSAs act as a safety net, converting a potentially disruptive exit event into a controlled, managed transition.

Enterprise organizations approaching the digital sovereignty threshold generally take one of two paths: They adopt end-to-end solutions that address all requirements holistically, or they distribute data across different data silos to try to satisfy emerging sovereignty expectations. In contrast, heavily regulated sectors (e.g., government institutions) typically implement comprehensive, or near-comprehensive, digital sovereignty strategies.

THE INCEPTION OF MINIMUM VIABLE SOVEREIGNTY

Most organizations cannot – and should not – apply maximum sovereign controls uniformly across their entire digital estate. Doing so introduces disproportionate cost, operational complexity, and service constraints that often exceed what regulators explicitly mandate.

In practice, an overly uniform approach also might reduce agility and slow down innovation without delivering commensurate compliance benefit. MVS is the discipline of first determining the appropriate level of sovereign control required for each workload, data set, or system before design and deployment decisions are made.

That requirement is not static; it varies based on business criticality, data sensitivity, regulatory classification, contractual obligations, and the legal jurisdiction of data subjects. Establishing this classification upfront is what differentiates a deliberate sovereignty strategy from a blanket sovereignty posture applied indiscriminately across the estate.

A practical MVS approach can be structured around three core steps:

- **First, classify workloads according to their sovereignty requirements**, recognizing that not all data carries equal jurisdictional or regulatory sensitivity. For example, regulated financial processing systems differ materially from internal collaboration tools.
- **Second, map each sovereignty tier to an appropriate deployment model**, confirming that control levels are proportional to obligation rather than maximized by default.
- **Third, govern the resulting mixed estate through consistent policies**, so that auditability, control enforcement, and recovery capabilities are uniformly demonstrable across all tiers.

This model applies sovereignty precisely where needed, without over-engineering environments that do not warrant it.

DIGITAL SOVEREIGNTY: STRATEGIC AND OPERATIONAL IMPLICATIONS

Digital sovereignty must be established as a strategic framework, supported by a cross-functional governance model spanning the organization. Key stakeholders include procurement, compliance, enterprise architecture, software development, legal, security, and operations. Each function plays a role in verifying that platforms, services, and vendors align with regulatory requirements, internal risk policies, and the organization's sovereignty objectives.

For executive leadership, digital sovereignty should not be treated as a purely technical or operational topic. It represents a strategic shift in organizational thinking, requiring alignment from the board level down to the teams responsible for day-to-day IT operations.

Governance and Ownership

From a governance perspective, ownership of the digital sovereignty framework should typically sit within enterprise risk leadership, most commonly under the Chief Risk Officer (CRO). Digital sovereignty is fundamentally a risk management domain that spans regulatory exposure, operational resilience, supply-chain dependency, and data protection obligations.

Positioning ownership under the CRO treats the topic as an enterprise risk issue rather than a purely technical initiative, while also enabling structured oversight through existing risk governance frameworks.

Depending on the organization's structure and regulatory environment, alternative ownership models also may be appropriate:

- **Chief Information Security Officer (CISO)** – where sovereignty requirements are closely tied to data protection, cryptographic control, and operational security.
- **Chief Information Officer (CIO)** – where the focus is primarily on architecture, platform strategy, and technology sourcing decisions.
- **Chief Compliance Officer (CCO)** – particularly in highly regulated sectors where sovereignty is driven primarily by regulatory obligations and supervisory expectations.

Regardless of the formal owner, effective implementation requires a steering committee structure or governance board involving risk, security, IT, legal, compliance, and procurement to confirm decisions are coordinated across strategy, architecture, vendor management, and regulatory alignment.

Risk Management

Risk management is responsible for enabling informed decision-making by balancing sovereignty risks with operational and strategic priorities. This includes:

- Identifying and quantifying digital sovereignty risks, including jurisdictional exposure, data residency violations, and dependency on foreign-controlled providers.
- Establishing risk frameworks and tolerances aligned with regulatory obligations and business objectives.
- Evaluating third-party, cloud, and cross-border data risks, confirming that mitigation strategies and controls are in place.
- Monitoring compliance through continuous risk assessment, reporting, and audit alignment.

Legal and Compliance

Legal and compliance functions enable the organization to operate across borders while maintaining defensible legal positions and regulatory adherence. This includes:

- Interpreting digital sovereignty requirements across jurisdictions and translating them into enforceable organizational policies.
- Assessing applicable laws on data residency, cross-border data transfers, privacy, and government access.
- Defining contractual standards with cloud providers and partners to maintain data control, audit rights, and jurisdictional safeguards.
- Guiding the organization on lawful processing, storage, and movement of sensitive data. Establishing compliance frameworks that align regulatory obligations with internal governance and risk tolerance.
- Advising on sovereignty risks related to vendor lock-in, foreign jurisdiction exposure, and third-party dependencies.
- Upholding auditability and evidentiary standards for regulators and legal proceedings. Collaborating with architecture and security teams to embed compliance into technical controls and operating models.

Procurement and Vendor Management

Procurement and vendor management teams must verify that solutions meet regulatory obligations and internal governance standards. This includes:

- Clearly understanding where SaaS platforms are hosted, where data is stored, where data is transferred (meaning where sub-processors are processing data matters as well), and under which jurisdiction it falls.
- Enabling transparency regarding access controls, encryption protocols, ownership of key management, and the implementation of operational safeguards such as service termination or “kill-switch” mechanisms.
- Providing defined exit strategies to protect the organization’s digital assets both during standard operations and in the event of service disruption.
- Confirming the existence of clear exit strategies where platforms manage critical data, including the ability to migrate data to alternative platforms or maintain access through archive-only capabilities for historical records.
- Verifying contractual clarity regarding service termination conditions and wind-down periods to enable continuity and orderly transition if agreements end.
- Partnering with legal and risk teams to address potential vendor lock-in, contractual exposure, and risks to service continuity.

Enterprise Architecture and Infrastructure Architecture

Enterprise architects align digital sovereignty with business strategy, risk, and regulatory requirements. This includes:

- Defining principles for data residency, control, and governance that guide technology choices.
- Operationalizing these principles through designs that enforce data locality, encryption, identity boundaries, and policy-based access.
- Evaluating cloud and hybrid models to balance compliance, performance, and cost while avoiding lock-in or extra-territorial exposure.
- Implementing workload classification, observability, and automated compliance to maintain auditable control and enable compliant innovation at scale.

Software Architecture

Software architects focus on designing applications that remain portable, interoperable, and resilient to vendor lock-in, which enables strategic flexibility to shift providers or repatriate workloads without disrupting core business services. This includes:

- Prioritizing open standards, open APIs, and widely adopted runtimes to allow workloads to move across environments with no or minimal refactoring.
- Defining modular, loosely coupled architectures that support redeployment between cloud providers or back on premises when repatriation is required.
- Enforcing abstraction layers to decouple application logic from proprietary cloud services.
- Standardizing data formats and integration patterns to maintain compatibility across platforms.
- Evaluating dependencies for portability risk and favor ecosystems with strong multi-cloud support and potential on premise hosting.
- Incorporating containerization and orchestration patterns to enable consistent deployment across environments.
- Validating that migration pathways are tested and documented as part of the delivery lifecycle.

FinOps

FinOps is responsible for:

- Evaluating the cost impact of digital sovereignty requirements, including data residency, multi-cloud deployment, and provider diversification.
- Optimizing spending while accommodating constraints such as local hosting, redundancy, and portability to avoid lock-in or extra-territorial exposure.
- Providing financial visibility and scenario modeling to balance compliance obligations with cost efficiency and strategic flexibility.

Cloud Platform Architecture

Cloud platform architects provide a scalable, secure foundation that enables sovereignty, operational consistency, and strategic flexibility, including potential cloud repatriation. This includes:

- Designing and governing foundational environments that enforce digital sovereignty through standardized landing zones, identity controls, encryption, and policy enforcement.
- Enabling platform services to meet jurisdictional requirements while abstracting provider-specific dependencies to support multi-cloud and hybrid portability.
- Implementing guardrails and connectivity models that control data residency, cross-border flows, and compliance by design.

Networking and Connectivity

Networking and connectivity functions form the controlled communication layer that underpins sovereign and compliant digital operations. They do this by:

- Enforcing digital sovereignty by controlling how and where data moves across regions, providers, and trust boundaries.
- Designing network architectures that enable data residency through regional isolation and policy-driven routing.
- Enabling secure hybrid and multi-cloud connectivity while minimizing exposure to foreign jurisdictions.

Incident Response

Incident response teams safeguard operational resilience while verifying all response activities remain compliant with digital sovereignty mandates. Their responsibilities include:

- Confirming digital sovereignty requirements are maintained during normal operations and in the event of disruptions or security incidents.
- Maintaining operational processes, including backups and recovery, that respect geographic and legal boundaries.
- Managing breaches or outages in compliance with local regulatory reporting timelines and evidentiary requirements.
- Coordinating with legal and compliance teams to properly handle cross-border incident data disclosure.
- Implementing procedures to contain incidents without violating sovereignty constraints, such as restricting data movement across regions.

Operations

Operational teams are responsible for:

- Confirming that day-to-day IT activities comply with digital sovereignty requirements, including data residency, access control, and jurisdictional constraints.
- Managing service and incident workflows, including careful control of data and log sharing with vendors during ticketing, diagnostics, and remediation.
- Enforcing that only necessary and approved telemetry is shared using approved channels, with appropriate masking, minimization, and contractual safeguards being applied.
- Delivering stable and compliant operations while preserving control over sensitive data throughout support and remediation activities.

THE INTRODUCTION TO COMMVULT GEO SHIELD

Commvault views digital sovereignty as inherently contextual – defined by jurisdictional mandates, industry-specific obligations, and each organization’s operational model. To meet this need, enterprises require a unified approach to sovereign data protection.

The approach should deliver consistent enforcement across geographies and industry verticals while preserving resilience, compliance, and operational continuity under varying regulatory conditions. This imperative led to the development of Commvault’s common sovereignty framework, referred to as Geo Shield.



Not every organization requires full sovereign isolation across all data and workloads. In practice, most enterprises adopt a tiered approach – applying varying degrees of sovereignty based on data sensitivity, regulatory exposure, and business criticality.

This approach allows them to help retain the scalability and elasticity of public cloud services while preserving optionality through clear exit strategies and enforcing the strictest sovereignty controls where they matter most.

Commvault recognizes that the highest levels of sovereignty assurance require local operational control. Commvault Geo Shield is therefore designed to place a trusted partner ecosystem at the center of delivery, helping enable customers to meet stringent sovereignty requirements with greater confidence, transparency, and alignment to local regulatory expectations.

- **Data residency requirements** are addressed through Commvault Cloud SaaS, underpinned by Commvault's Site Reliability Engineering (SRE) and Site Reliability Operations (SRO) functions. This represents the foundational tier of the Commvault Geo Shield strategy, designed to meet baseline data residency requirements.
- **Regional Sovereign Cloud (RSC)** is delivered by the Commvault Cloud SaaS motion hosted on a regionalized sovereign hyperscaler (e.g., AWS European Sovereign Cloud). The service is maintained by Commvault's SRE and SRO functions.
- **National Sovereign Cloud (NSC)** is delivered through Commvault's Managed Service Provider ecosystem, with partners operating the Commvault platform in fully isolated environments designed to prevent extra-territorial access. These providers deliver in-region expertise and localized operations, helping enable alignment with national regulatory and sovereignty requirements. They also assume responsibility for L1/L2 customer support and onboarding services. This model represents the highest level of sovereignty achievable within an as-a-service framework.
- **Private Sovereign Cloud (PSC)** reflects Commvault's long-standing delivery approach for highly controlled environments, including air-gapped and "dark site" deployments. Delivered entirely through a software-based model, PSC helps enable organizations to operate fully locally, maintain physical and network isolation, and enable continuity of the data protection platform independent of external connectivity.

Within the PSC model, Commvault offers enhanced delivery options to help further align with customer sovereign requirements.
- **Commvault Cloud Dedicated Private Instance** helps enable the platform to remain fully under the physical control of the customer or partner, while being supported by Commvault Remote Managed Services (RMS) and Commvault Professional Services (PS).

RMS responsibilities are defined on a per-customer basis, enabling a tailored operating model that specifies access controls, connectivity parameters, and service scope in line with organizational and regulatory requirements. This approach helps organizations maintain local control and isolation while selectively leveraging Commvault's operational expertise.

- **Secure Storage on Sovereign Cloud** helps deliver secure, immutable, and air-gapped backup copies hosted on sovereign cloud platforms such as STACKIT. It helps extend the capabilities of Commvault AirGap while inheriting the sovereignty assurances of the underlying cloud infrastructure, helping enable organizations to meet stringent regulatory and data protection requirements without compromising resilience.
- **Commvault Cloud Validated Designs for Trusted Clouds** help provide pre-validated architectures for protecting workloads hosted on trusted cloud platforms such as BLEU and S3NS in France. These designs help enable organizations to build sovereign-aligned private cloud environments confidently while leveraging the scalability and elasticity of trusted cloud infrastructure.

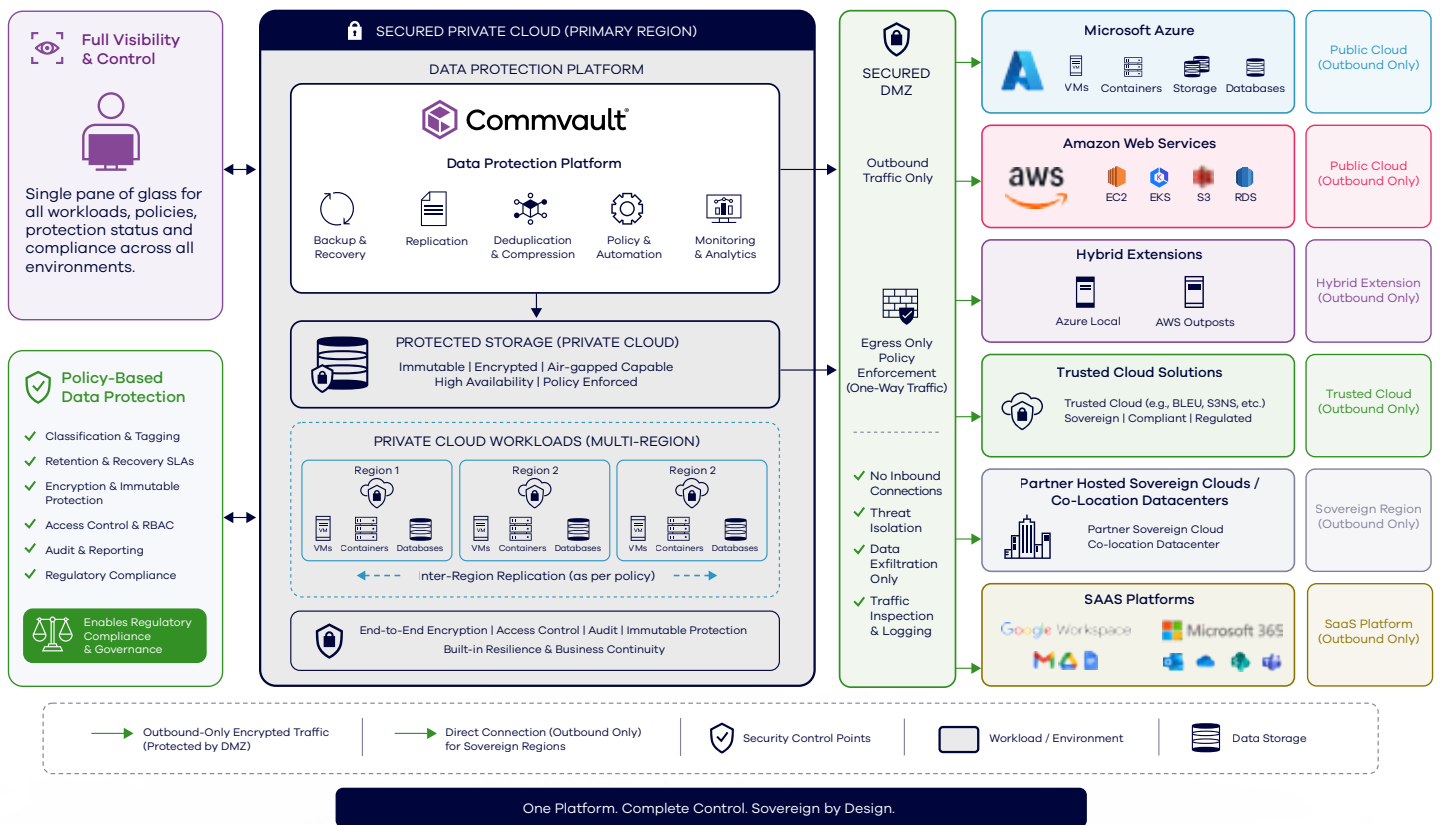
In highly regulated environments where local support processes and resources are required – and where Commvault may not directly provide these services – we optionally and strategically leverage our Commvault Authorized Regional Expert (CARE) program. The program has three different pillars: Support, Services, and Success.

We are convinced that our unified approach to digital sovereignty, underpinned with our common model alongside with the predefined spectrum of sovereign deployment modalities and specific solutions, can help provide customers the confidence to build out their sovereign strategy with Commvault.

Built on Commvault's modular architecture, flexible networking capabilities, and the Commvault Cloud Unity capabilities, the platform help provides a secure and adaptable foundation for sovereign data management. This helps enable organizations to confidently adopt both MVS and multi-sovereign strategies, knowing they are working with a proven, resilient, and future-ready platform.

UNIFIED DATA PROTECTION ACROSS EVERY SOVEREIGN SILO

Visibility. Control. Compliance.



EU CSF: A PROCUREMENT FRAMEWORK

The European Cloud Sovereignty Framework (EU CSF) is not a regulation or a formal European standard. It is a cloud sovereignty assessment and procurement framework developed by the European Commission for its Sovereign Cloud procurement, with the intention that it also can serve as a reference methodology for future cloud procurements across Europe.

The framework provides a structured set of sovereignty objectives and evaluation criteria to assess whether cloud services operate under European legal control, technical autonomy, and operational resilience. It was developed in response to concerns about extraterritorial jurisdiction – particularly from non-EU legal systems – and Europe’s strategic dependence on a limited number of global hyperscale cloud providers.

While originally created for a specific procurement, the commission has published it as an open reference framework that other public and private organizations are encouraged to adopt, making it an emerging benchmark for evaluating cloud sovereignty rather than a mandatory certification or regulatory requirement.

CSF Requirement	What It Demands	How Commvault Addresses It
SOV-1: Strategic Sovereignty	Anchoring services within EU legal, financial, and industrial ecosystem Resilience to control changes EU-based investment and operational continuity	Helps enable sovereign deployment models that support EU-based infrastructure strategies. Helps enable data protection continuity across ownership or service disruptions. Helps maintain recoverability independent of provider changes.
SOV-2: Legal & Jurisdictional Sovereignty	Operations governed under EU or member-state law Minimization of non-EU jurisdictional exposure Controlled access by foreign authorities	Helps enable sovereign deployment models that provide configurable data residency and control policies, encryption with customer-managed keys, and audit-ready governance to help support jurisdictional compliance and regulatory alignment.
SOV-3: Data & AI Sovereignty	Full control of data and AI assets Cryptographic exclusivity EU-confined storage and processing Auditability of access	Helps support strong encryption with customer-controlled keys, immutable audit logging, and secure data protection architectures with bring-your-own-key and hold-your-own-key principles designed to support controlled access and recoverability across sovereign environments.
SOV-4: Operational Sovereignty	Independent operational capability Continuity of operations Reduced external dependency Availability of skilled control within EU	Helps enable operational sovereignty enforced with role- and scope-based access control, dual authorization, just-in-time access and PIM/PAM integrations – supported by CyberArk and BeyondTrust, among others – with auditable controls.

SOV-5: Supply Chain Sovereignty	Transparent and resilient technology supply chains EU control of critical components Reduced non-EU dependency	Helps provide comprehensive visibility into third-party libraries, open source dependencies, cloud services, operating systems, APIs, and runtime environments – helping enable organizations to maintain control over software composition and deployment across their environments.
SOV-6: Technology Sovereignty	Interoperability Transparency Avoidance of lock-in Adherence to open standards	Helps supports broad platform interoperability – including cross-hypervisor recovery and heterogeneous infrastructure support. Provides multi-cloud capabilities that help enable cloud provider exit strategies and the industry's broadest workload coverage, helping reduce vendor dependency and enhance portability.
SOV-7: Security & Compliance Sovereignty	EU-controlled security operations Compliance with GDPR, NIS2, and DORA Long-term operational assurance	Helps support policy-driven security controls, immutable backups and auditing, audit-ready reporting, and recovery validation designed to support alignment with EU regulatory frameworks. Includes integrated third-party security vendor support and the ability to offload key management to external key management systems or hardware security module systems using hardware- and storage-agnostic deployment models.
SOV-8: Environmental Sustainability	Energy efficiency Renewable sourcing Reduced carbon footprint Long-term resource sustainability	Helps support environmental sustainability through deduplication, compression, efficient data transfers, storage tiering, workload consolidation, automation, and infrastructure-agnostic deployment across hybrid and multi-cloud environments, helping minimize energy consumption and resource utilization.

EU CADA: A REGULATORY PROPOSAL TO STRENGTHEN DIGITAL INFRASTRUCTURE

The Cloud and AI Development Act (CADA) is a proposed EU regulation that aims to strengthen Europe's cloud and AI ecosystem by increasing investment in digital infrastructure, accelerating the deployment of cloud and datacenter capacity, and reducing strategic dependencies on non-EU technology providers.

Introduced by the European Commission in June 2026 as part of its broader Tech Sovereignty Package, CADA complements the AI Act by focusing on the infrastructure that powers AI rather than regulating AI systems themselves.

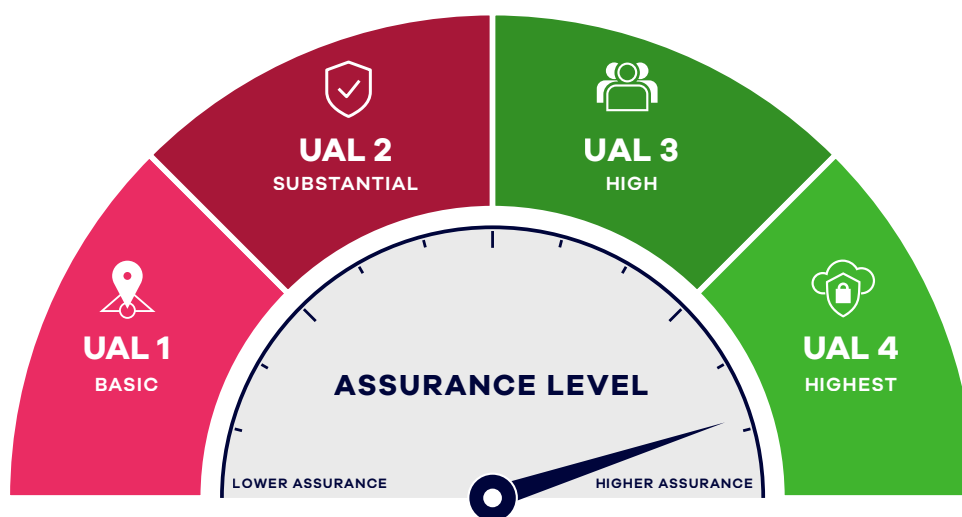
- **Research, development, and innovation:** Support next-generation cloud and AI technologies (notably for frontier AI, industrial AI, and physical AI), and accelerate adoption across strategic industries and the public sector.
- **Capacity:** Expand Europe's datacenter and cloud capacity by simplifying permitting, improving access to energy, land and financing, and maintain sufficient compute resources for AI.
- **Autonomy:** Introduce a common EU-wide framework to assess cloud and AI sovereignty, promote resilient European digital infrastructure, and establish a shared procurement approach for public administrations.

Unlike the AI Act, which regulates the development and use of AI systems, CADA is primarily an industrial and infrastructure policy. It seeks to verify that Europe has the cloud, computing capacity, and sovereignty needed to support AI innovation while strengthening the resilience and competitiveness of the European digital economy.

CADA defines cloud and AI sovereignty through four assurance levels, to be used by public sector bodies based on their risk assessments. Cloud service providers can be recognized under this framework by Member States after undergoing an audit. The four levels are:

CADA UNION ASSURANCE LEVELS (UAL)

Increasing Sovereignty. Stronger Protection. Greater Control.



UAL 1 BASIC

EU-established provider, data stays in EU, state-of-the-art cybersecurity. Some flexibility on non-EU subcontractors with safeguards.

UAL 2 SUBSTANTIAL

UAL 1 + EU subcontractors, EUCS certification, no third-country AI training, SBOM transparency, legal/technical separation from third-country parent.

UAL 3 HIGH

EU citizen personnel, NO third-country control (unless exemption), all support from EU residents, full supply chain independence.

UAL 4 HIGHEST

UAL 3 + for sensitive/classified data, "high" cybersecurity cert, absolute prohibition on third-country control (no exemptions).

THE REGULATORY HORIZON

The regulatory landscape governing digital sovereignty is not static. The frameworks, certifications, and acts below deserve particular attention from practitioners planning sovereignty programs today, because each creates binding operational requirements – not merely documentation obligations.

CADA (Cloud and AI Development Act): Currently in draft stage, CADA seeks to strengthen Europe's cloud and AI ecosystem, infrastructure, and technological sovereignty. Its measures focus on research and innovation, sustainable datacenter capacity, and reduced dependence on non-European providers. CADA also would establish an EU-wide sovereignty assessment framework and support public-sector adoption of qualifying cloud services. If adopted, it could reshape cloud procurement and competition by making sovereignty, resilience, and operational control central market differentiators.

EU CSF (EU Cloud Sovereignty Framework): An EU policy initiative and procurement methodology designed to strengthen control over digital infrastructure by reducing reliance on non-EU cloud providers, and keeping data, services, and critical workloads governed under European law. It aims to enhance security, regulatory compliance, and strategic autonomy by promoting trusted EU-based cloud solutions, interoperability standards, and governance models that keep sensitive data within the EU's legal and operational jurisdiction.

EU CS (EU Cloud Services): Covers cloud computing offerings provided within the European regulatory and operational framework, designed to maintain compliance with EU data protection, security, and sovereignty requirements. The intent is to provide organizations with trusted cloud environments where data residency, access control, and governance remain subject to EU law, supporting regulatory alignment (e.g., GDPR), helping reduce dependency on non-EU providers, and strengthening digital sovereignty and resilience across critical workloads.

EU CC (EU Cybersecurity Certification): A framework for certifying information and communications technology (ICT) products, services, and processes against common EU-wide security standards. Its purpose is to create a unified assurance baseline for cybersecurity across the single market, helping organizations and governments assess trustworthiness, reduce fragmentation in national certifications, and strengthen overall resilience by verifying that certified solutions meet defined security, assurance, and compliance requirements.

BSI C5 (BSI Cloud Computing Compliance Criteria Catalogue): A German Federal Office for Information Security standard that defines a baseline of security and transparency requirements for cloud service providers, particularly for handling sensitive and regulated data. It is intended to provide independent, audit-based assurance that cloud environments meet stringent controls around security, data protection, operational reliability, and transparency, thereby enabling customers – especially in regulated sectors – to assess and trust cloud services in compliance with German and EU regulatory expectations.

SecNumCloud: The French national cloud security certification issued by ANSSI that sets strict requirements for cloud service providers handling sensitive or regulated data. It is designed to enable a high level of security, operational control, and legal sovereignty by requiring strong guarantees around data protection, access control, resilience, and immunity from non-EU jurisdictional interference. Its purpose is to enable trusted cloud adoption in critical sectors while maintaining compliance with French and EU security, and sovereignty expectations.

Banca Italia: The certification framework intended to confirm that cloud and ICT services used by supervised financial institutions meet stringent requirements for security, operational resilience, risk management, and regulatory compliance within the Italian banking system. In sovereignty terms, it functions as a financial-sector control mechanism that helps reinforce local regulatory authority over critical data and infrastructure, reduce exposure to external jurisdictional risks, and validate that sensitive financial workloads remain governed by EU/Italian supervisory oversight with verifiable assurance standards.

DORA (Digital Operational Resilience Act): Applies to financial entities across the EU and imposes binding requirements on ICT risk management, incident reporting, and operational resilience testing. Critically for sovereignty programs, DORA generally requires organizations to demonstrate control over third-party ICT providers – including the ability to exit a provider relationship without operational disruption. A sovereign architecture that cannot be exited cleanly fails the DORA test, regardless of its technical compliance with data residency requirements.

NIS2 (Network and Information Security Directive 2): Extends cybersecurity obligations to a significantly broader set of sectors than its predecessor, including energy, transport, healthcare, and digital infrastructure. It introduces supply chain security requirements that directly implicate sovereignty: Organizations must assess the cybersecurity practices of their technology suppliers, including cloud providers and data protection vendors. For sovereignty programs, this means vendor sovereignty posture is increasingly relevant to compliance and procurement assessments.

EU Data Act: A regulatory framework that governs access to and sharing of data generated by connected products and cloud services across the EU. Its purpose is to enable fair data access, prevent vendor lock-in, and stimulate competition by giving users and businesses greater control over their data. This includes the ability to switch cloud providers more easily and share data under clear legal conditions. It also establishes rules for interoperability, data portability, and safeguards for lawful access by public authorities under defined circumstances.

EU AI Act: Introduces tiered obligations for AI systems based on risk classification, with high-risk systems subject to strict data governance and documentation requirements. For organizations using AI systems that process personal or regulated data, the act's requirements on training data provenance, data quality governance, and audit trails intersect directly with sovereignty obligations. Organizations building AI capabilities on top of sovereign infrastructure should assess whether their AI governance framework meets the act's requirements for the risk tier their systems fall into.

EU Net Zero Industry Act: A regulatory initiative aimed at scaling up the manufacturing capacity of clean technologies within the EU. Its purpose is to strengthen industrial competitiveness and energy security while accelerating the transition to net-zero emissions by 2050. It does this by streamlining permitting, improving access to financing, and setting benchmarks to enable producing a significant share of strategic clean-tech deployment within the EU.

EU Public Procurement Act: Governed by a set of directives (notably 2014/24/EU, 2014/25/EU, and 2014/23/EU) that regulate how public authorities purchase goods, services, and works. The purpose of this framework is to confirm transparent, competitive, and non-discriminatory procurement across the single market, while enabling efficient public spending and compliance with EU.

EU CRA (Cyber Resilience Act): The first horizontally applicable European cybersecurity regulation, establishing binding minimum requirements for all products with digital elements placed on the EU market. Reporting obligations and full application are phased, with key dates currently set for September 2026 and December 2027. The CRA requires secure-by-design products, mandatory software bills of materials, and continuous vulnerability reporting to the EU Agency for Cybersecurity (also known as ENISA). For sovereignty programs, the CRA makes supply chain cybersecurity an auditable procurement requirement: Organizations must be prepared to demonstrate control over software composition, dependencies, and vendor security posture, reinforcing NIS2's supply chain obligations with product-level accountability.

EU Digital Network Act: Aimed at securing Europe's telecom infrastructure, reducing foreign dependence, harmonizing standards, strengthening European operators, and improving resilience. It is designed to give the EU greater control over critical digital systems, strategic autonomy in connectivity, and stronger influence over future technologies.

EU Cloud and AI Development Act: A proposed EU regulation designed to strengthen Europe's digital sovereignty by accelerating investment in sovereign cloud and AI infrastructure, expanding compute capacity, and fostering a more resilient European cloud ecosystem. Rather than regulating AI systems, CADA focuses on the infrastructure, capacity, and policy framework needed to support Europe's long-term technological autonomy.

PRACTITIONER BEST PRACTICES

The following best practices consolidate the guidance across this paper into actionable steps for practitioners building or maturing a digital sovereignty program.

- **Start with workload classification**, not deployment selection. Define what each workload requires across the four pillars before making any infrastructure decisions. Deployment model selection is an output of requirements analysis, not an input to it.
- **Establish governance ownership** before technology ownership. Assign sovereignty framework ownership – typically the CRO – and stand up a cross-functional steering structure before committing to architecture. Sovereignty decisions made without cross-functional governance tend to optimize for one dimension at the expense of others.
- **Treat paper-backed sovereignty as a risk**, not a solution. Contractual assurances are a starting point, not an endpoint. For any provider relationship in your sovereignty boundary, identify what technical and operational controls exist to enforce sovereign requirements independent of contractual commitments.
- **Apply sovereignty requirements to recovery infrastructure**, not just primary systems. Backup data, recovery personnel, and recovery tooling must meet the same jurisdictional and operational sovereignty requirements as the primary environment. Test this under realistic conditions before an incident forces the issue.
- **Document controls, not just policies.** Regulators are asking for evidence of consistent enforcement, not policy statements. Build your sovereignty program around auditable controls from the start – not documentation that describes intended behavior.
- **Build exit strategies into every vendor relationship.** Vendor lock-in is a sovereignty risk. Confirm that contracts include clear termination conditions, data portability provisions, and wind-down periods. Test exit capabilities – particularly data migration and archive access – before they are needed.
- **Review your sovereignty posture** when the regulatory landscape changes. DORA, NIS2, the EU AI Act, and the EU CSF are all either recently effective or still maturing. Build a cadence of annual sovereignty posture reviews that explicitly assess regulatory changes and their operational implications.

CONCLUSION

Digital sovereignty is not a project with a completion date. It is an ongoing governance discipline – one that must be continuously demonstrated, not merely established. Building sovereignty into governance models, procurement practices, architecture principles, and recovery capabilities should help organizations navigate the next wave of regulatory requirements, geopolitical pressure, and technology change with greater confidence.

Minimum viable sovereignty is not a shortcut. It is a recognition that the goal is not maximum control – it is the right level of control, applied consistently, across every workload that requires it. Getting that calibration right is the work of practitioners. This paper is intended to help them do it.

For the executive-level view of digital sovereignty readiness, see the companion Digital Sovereignty Readiness Report at readiverse.com.

To learn more, visit commvault.com



commvault.com | 888.746.3849



© 2026 Commvault. See [here](#) for information about our trademarks and patents. 10_26