David S. Safaii

2026

Table of Contents

Executive Summary

The term *Sovereign Cloud* has become one of the defining themes in enterprise infrastructure. Governments, regulated industries, and multinational organizations increasingly view sovereignty as essential for protecting critical data, ensuring regulatory compliance, and preserving operational control.

The spending data confirms it. Gartner forecasts worldwide sovereign cloud IaaS spending will reach $80 billion in 2026, a 35.6 percent increase over 2025, with governments the primary buyers, followed by regulated industries and critical infrastructure operators. Growth is sharpest outside the incumbent markets: 89 percent in the Middle East and Africa, 87 percent in mature Asia/Pacific, and 83 percent in Europe, where spending is projected to rise to $12.6 billion in 2026 and $23.1 billion in 2027 — overtaking North America. Gartner also expects "geopatriation" to move roughly 20 percent of existing workloads from global public clouds to local providers. The demand signal is equally clear on the buyer side: three-quarters of business leaders surveyed for Kyndryl's 2025 Cloud Readiness Report reported concern about the geopolitical risks of storing data in global cloud environments.

Intent, however, is running well ahead of execution. In SUSE's Navigating Digital Resilience 2026 study of 309 IT leaders across France, Germany, India, Japan, and the United States, 98 percent said they were prioritizing digital sovereignty — but only 52 percent were actively taking steps to achieve it, whether that meant developing a strategy or having one in place. Just over half (51 percent) had made digital sovereignty a formal requirement in technology purchasing.

Yet despite rapid market growth, one important question remains unanswered.

How do organizations measure whether their Sovereign Cloud strategy is actually effective?

Most current approaches focus on compliance. They evaluate whether data resides within approved jurisdictions, whether encryption standards are met, or whether regulatory controls have been implemented.

These are necessary requirements, but they do not measure sovereignty itself.

True sovereignty is demonstrated by an organization's ability to continue making independent technology decisions as infrastructure evolves, regulations change, artificial intelligence transforms workloads, and cyber threats disrupt operations.

In other words, sovereignty is not simply about where systems operate.

It is about how much strategic freedom an organization retains over time.

This article builds on the **Sovereignty Effectiveness Assurance Level (SEAL)**, the grading concept introduced by the European Commission in its Cloud Sovereignty Framework, and proposes a complementary five-level maturity lens: the Architectural Sovereignty Level (ASL). Where SEAL grades the jurisdictional question of whose law reaches a service, ASL assesses how effectively an enterprise preserves technological independence across infrastructure, operations, applications, AI, and recovery.

And as organizations move to higher assurance levels, one architectural characteristic consistently emerges as the enabler of that freedom — and it is the subject of this article:

Open source (and Open Ecosystems).

Not because open source is inherently sovereign, but because open ecosystems provide the interoperability, transparency, and portability that make long-term sovereignty achievable.

Why Compliance Is Not Enough

Many organizations consider themselves sovereign because they satisfy regulatory requirements.

- ✓ Their workloads execute inside national borders.
- ✓ Their data remains within approved jurisdictions.
- ✓ Their providers offer sovereign cloud services.

While these capabilities are important, they answer only one dimension of sovereignty.

They do not answer the critical questions of:

- Can applications migrate between infrastructure providers?
- Can AI platforms evolve without rebuilding operational processes?
- Can workloads recover independently after a ransomware attack?
- Can infrastructure modernization occur without replacing operational tooling?
- Can backup data remain usable if a vendor relationship changes?

These questions determine whether an organization possesses strategic independence (and a path to sovereignty).

Analysts see the same gap. Forrester finds that 84 percent of decision-makers treat digital sovereignty as a critical factor in vendor selection, while more than half cite sovereignty-related regulatory constraints as a top obstacle to public cloud adoption — and only a minority are

confident that their current stack actually satisfies regional mandates. IDC likewise describes Europe's sovereign cloud market as having moved in 2026 from conceptual debate to operational reality, with success depending on transparency, compliance automation, and the ability to bridge global innovation with local assurance. In both readings, the constraint is no longer awareness of sovereignty requirements. It is the architecture underneath them.

- ✓ Compliance demonstrates conformity.
- ✓ Sovereignty demonstrates freedom.

Sovereignty Is Really About Optionality

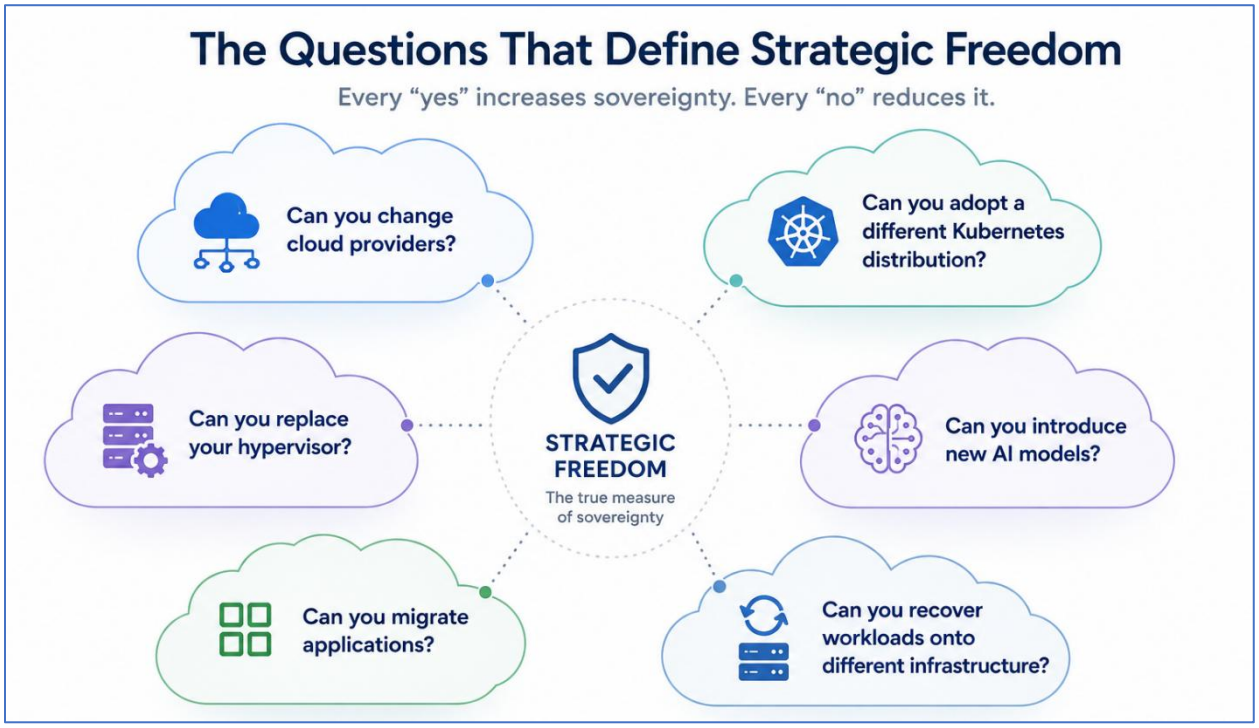
Perhaps the most important misconception surrounding Sovereign Cloud is the belief that sovereignty is primarily about control.

Control certainly matters.

But control without flexibility eventually becomes another form of dependency.

The more useful concept is optionality.

Optionality is the ability to change direction without unacceptable cost, operational disruption, or technological constraints.



Open technologies preserve optionality because they separate applications from infrastructure, data from platforms, and operations from vendor-specific implementations.

That separation enables organizations to make future technology decisions based on business requirements rather than technical constraints-imposed years earlier.

In this sense, open source is less about software licensing than it is about preserving strategic freedom.

Red Hat frames the same idea in nearly identical terms. In announcing its expanded sovereign and private cloud capabilities in May 2026, the company argued that discussions of sovereignty too often center on regulatory requirements, when sovereignty is really about control — an organization's ability to maintain oversight and command over its own trajectory regardless of geopolitical shifts, market dynamics, or changing vendor terms. Mike Barrett, Vice President and General Manager of Hybrid Cloud Platforms at Red Hat, made the point more directly a month earlier: digital sovereignty is no longer just about where data resides; it is about maintaining operational control over technology, strategic flexibility, and trust.

Red Hat makes the same argument more bluntly: "Digital sovereignty transcends compliance." In its own framing, sovereignty is a matter of equipping organizations with the autonomy to make independent decisions about their digital direction — which is another way of saying that the measure of sovereignty is how many decisions remain genuinely available.

Optionality is easiest to observe at its breaking point. The moment an organization has to restore its workloads somewhere other than where they were running — after a ransomware event, a licensing change, or a jurisdictional move — is the moment it discovers how much optionality it actually held. Everything before that is an assertion; recovery is the audit.

The practical question, then, is how much optionality an organization actually retains — and that is what the framework below sets out to measure.

Introducing the Architectural Sovereignty Level (ASL)

Any architectural measure of sovereignty has to begin with the jurisdictional one that already exists. The European Commission's Cloud Sovereignty Framework introduced the Sovereignty Effectiveness Assurance Level as a way to grade how much real control an organization retains over a cloud service, replacing binary "sovereign versus non-sovereign" claims with an auditable scale. As summarized by Atos in ‘Cloud sovereignty: Who holds the keys?’, the Commission's scale runs from SEAL-4 down to SEAL-0:

Level	Designation	What it means
SEAL-4	Full digital sovereignty	Everything in the EU, under EU law
SEAL-3	Digital resilience	EU law fully enforceable, with only marginal outside dependencies
SEAL-2	Data sovereignty	Significant non-EU dependencies and only indirect control
SEAL-1	Minimal jurisdictional sovereignty	Service still controlled by a non-EU entity
SEAL-0	No sovereignty	Full non-EU control and zero resilience to foreign law

Source: European Commission, Cloud Sovereignty Framework, as presented in Atos, "Cloud sovereignty: Who holds the keys?" (2026).

What makes the Commission's scale consequential is not the taxonomy but the procurement machinery attached to it. Sovereignty is assessed across eight objectives, each scored independently on the SEAL scale, so a provider does not hold a single SEAL rating — it holds eight, evaluated in the context of a specific tender.

The levels then operate in two distinct ways. They act as minimum floors: the contracting authority sets a required level for each objective, and a bid that falls below the floor on even one objective is rejected outright, however strong its remaining scores. For the bids that clear every floor, a weighted sovereignty score ranks them as an award criterion, with supply chain sovereignty carrying the heaviest weighting. Maybe sovereignty has moved, in other words, from an adjective in a marketing deck to a scored, documented, and rejectable line item in a tender response.

The first application showed what that means commercially. The Commission's own cloud procurement, run under its Cloud III dynamic purchasing system and awarded in April 2026 at roughly €180 million, set SEAL-2 as the minimum eligibility threshold; four consortia were selected, and none reached SEAL-4. The Commission has since signaled that it will extend the same assessment logic across the digital services it procures, and national authorities and private buyers are already borrowing the scale for their own tenders — the familiar path by which a public sector scoring matrix becomes a commercial default. Two consequences follow for Sovereign Cloud providers. Any provider selling into Europe now needs a defensible position on each of the eight objectives rather than a general sovereignty narrative. And the Commission's own commentary on the award is pointed: even non-European technology, when

operated inside a sufficiently strict framework, met the required minimum. That is the jurisdictional question being answered well — and it is also precisely why it is not the only question worth asking.

Red Hat approaches the same problem through four interconnected pillars of digital sovereignty, and they map closely onto what the assurance levels below are measuring.

- ✓ Data sovereignty concerns control over how data is collected, classified, processed, and stored.
- ✓ Technical sovereignty concerns the ability to run workloads without dependence on a given provider's infrastructure or software, and covers portability, open standards, interoperability, and lock-in mitigation.
- ✓ Operational sovereignty concerns visibility and control over how systems are provisioned, monitored, and maintained, and by whom.
- ✓ Assurance sovereignty concerns the ability to independently verify the integrity, security, and reliability of those systems, including the resilience of critical services.

The first pillar is largely jurisdictional; the remaining three are architectural.

The Commission's scale answers a jurisdictional question: whose law reaches the service? A second question sits alongside it — an architectural one: how much freedom the organization retains as its technology changes?

The two are complementary. An organization can satisfy the Commission's highest jurisdictional level and still be locked into a single proprietary stack it cannot leave. That architectural question is what the Architectural Sovereignty Level (ASL) measures. ASL measures the degree to which an organization can maintain operational and technological independence despite change; rather than evaluating individual products, it evaluates architectural outcomes. It is a distinct scale from the Commission's: it runs from ASL 1 to ASL 5, and its levels do not map onto SEAL-0 through SEAL-4.

The five stages below describe progressive architectural maturity.

ASL 1 – Compliant Sovereignty

What it means	Organizations have implemented the minimum controls necessary to satisfy regulatory or contractual obligations.
Characteristics	Data residency
	Regional cloud deployment
	Encryption
	Access controls
	Basic governance
Open source role	Incidental. Open components are present — Linux, PostgreSQL, container runtimes — but they are consumed as vendor-packaged

	products. Nothing in the architecture depends on their openness, and replacing one would be as disruptive as replacing any proprietary component.
Implication	Sovereignty is driven by compliance requirements rather than strategic architecture, and technology decisions remain heavily dependent on individual vendors.

ASL 2 – Operational Sovereignty

What it means	Organizations begin taking ownership of operational processes, while infrastructure providers continue delivering the underlying services.
Characteristics	Independent governance
	Customer-controlled identity
	Security policy ownership
	Operational visibility
	Infrastructure automation
Open source role	Operational. Open tooling for identity, configuration management, automation, and observability lets the organization run the platform rather than merely consume it. The provider still supplies the substrate, but operating knowledge becomes transferable rather than provider-specific.
Implication	Operational control increasingly belongs to the customer rather than the provider.

ASL 3 – Technology Sovereignty

What it means	Technology decisions become portable as organizations intentionally reduce architectural dependency.
Characteristics	Kubernetes
	Open APIs
	Infrastructure as Code
	Open virtualization
	Hybrid cloud
	Portable storage
	Standardized automation
Open source role	Structural. Open standards become the interfaces the architecture is built on — Kubernetes, open APIs, declarative infrastructure, portable storage. This is where openness stops being a property of individual components and becomes a property of the architecture itself.
Implication	Modernization becomes significantly easier because technology choices are no longer permanent commitments. This is also where open source begins playing a transformative role.

ASL 4 – Adaptive Sovereignty

What it means	Organizations can continuously evolve infrastructure without disrupting operations. Applications increasingly operate independently of the underlying infrastructure.

Characteristics	Multi-platform workload mobility
	AI platform flexibility
	Infrastructure modernization
	Cross-cloud deployment
	Policy portability
	Platform abstraction
Open source foundations	Linux
	Kubernetes
	OpenStack
	KubeVirt
	Cloud Native Computing Foundation (CNCF) projects
	OpenTelemetry
	GitOps
Open source role	Load-bearing. Workload mobility across platforms, clouds, and AI frameworks depends on shared open abstractions; without them, every move becomes a migration project rather than a routine operation. Remove the open layer and the capability the level describes collapses.
Implication	The objective is no longer avoiding vendors. It is preventing any individual vendor from becoming indispensable.

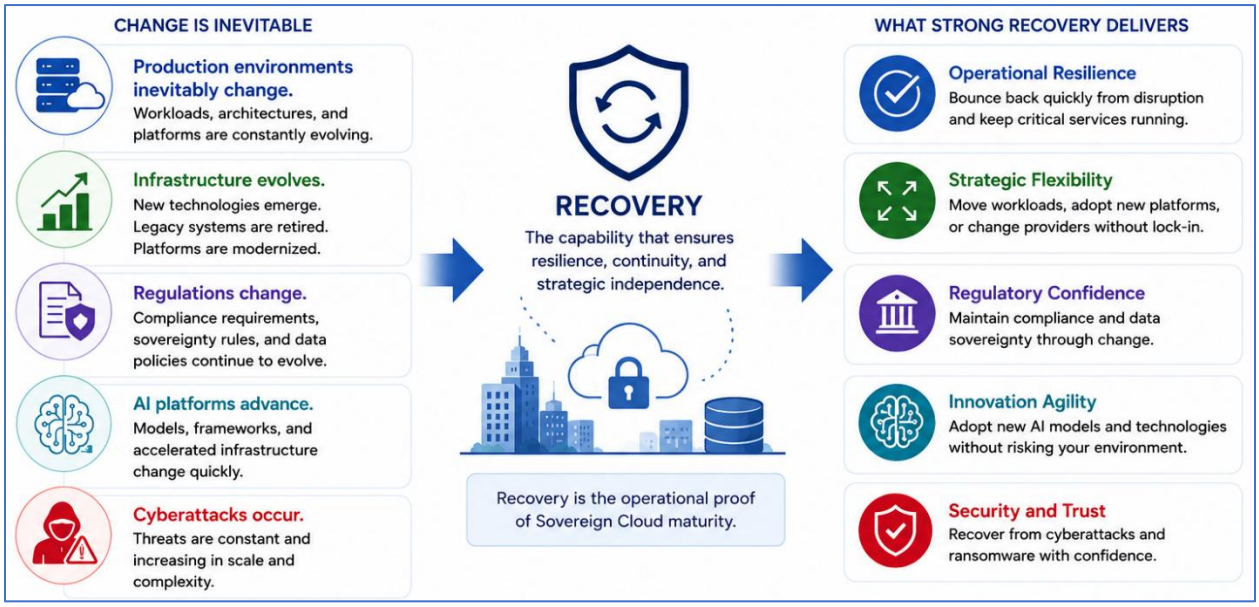
ASL 5 – Autonomous Sovereignty

What it means	ASL 5 represents strategic independence. Organizations can adopt new technologies, replace infrastructure, respond to geopolitical change, and recover from cyber incidents while preserving operational continuity. Recovery Sovereignty is the determining capability at this level: the other characteristics describe what an organization can change, while recovery determines whether those changes remain possible under duress.
Characteristics	Recovery Sovereignty
	AI portability
	Cross-platform recovery
	Open backup formats
	Independent operational governance
	Continuous modernization
	Technology optionality
Open source role	Determinative. Open formats govern whether the organization can rebuild at all — Kubernetes objects, CSI snapshots, OCI images, S3-compatible storage, and open model and data formats. Sovereignty here is bounded by what can be reconstituted elsewhere, and that boundary is set by format openness.
Implication	Sovereignty is measured not by infrastructure location but by organizational freedom. Applications, operations, and recovery all remain portable, technology decisions remain reversible, and the architecture adapts without wholesale replacement.

Why Recovery Completes the Model

As organizations approach higher SEAL and ASL levels, one capability increasingly distinguishes mature Sovereign Cloud strategies from immature ones.

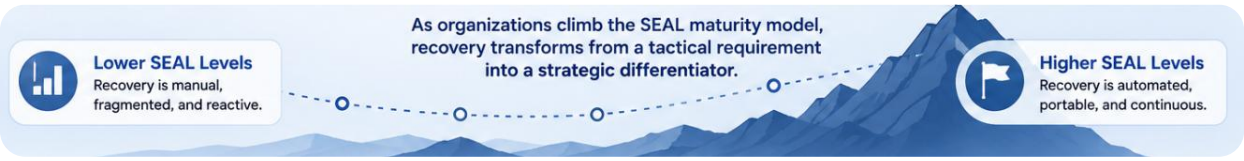
Recovery is where architectural flexibility is tested rather than asserted. In steady-state operations, dependencies stay invisible: the hypervisor is already running, the storage array is already attached, the control plane is already provisioned. A recovery event removes those assumptions all at once and forces the organization to rebuild somewhere else, often under time pressure. Whatever cannot be rebuilt independently is, by definition, a sovereignty gap.



Consider what that means in practice. After a ransomware event, the compromised environment is rarely the right place to restore into — recovery typically targets clean hardware, a different cluster, or an isolated region. If backups can only rehydrate onto the same proprietary platform that was encrypted, the recovery plan inherits the compromise. When a virtualization vendor changes its licensing model, organizations whose workloads are captured in open disk and manifest formats can re-instantiate them on KubeVirt, OpenStack, or another distribution; organizations holding vendor-specific backup images cannot, and end up negotiating from a position of no alternatives. When a regulator or a geopolitical event requires workloads to move jurisdictions, the constraint is almost never the application — it is whether the data and its operational state can be reconstituted on infrastructure the organization does not already run.

This is also where lock-in tends to hide. Compute and orchestration choices are visible and frequently debated; backup formats are not. A proprietary backup catalog quietly makes every future infrastructure decision conditional on one vendor's roadmap, because the organization's history — not just its current workloads — lives inside a format only that vendor can read. Data protection built on open formats and standard interfaces inverts that: workloads captured as Kubernetes objects, persistent volumes, CSI snapshots, OCI images, and S3-compatible object storage can be restored onto whatever platform the organization chooses next.

Recovery therefore reinforces flexibility in the underlying infrastructure rather than depending on it. When the recovery path is portable, the infrastructure beneath it becomes replaceable — hypervisors can be swapped, storage vendors changed, Kubernetes distributions modernized, and clouds exited, because none of those decisions put the organization's ability to restore at risk.



The gap between recovery confidence and recovery outcomes is well documented, and it is wide. Sophos's analysis of nearly three thousand ransomware victims found that organizations whose backups were compromised faced recovery costs roughly eight times higher than those whose backups survived. The confidence gap behind that outcome is equally well documented: as Scality's 2026 cyber resilience analysis notes, 90 percent of security leaders surveyed were very or extremely confident in meeting their defined recovery time objectives, yet 38 percent of organizations that actually experienced an incident in the preceding twelve months suffered extended downtime of critical systems.

None of this is caused by proprietary formats alone, and it would be wrong to claim otherwise. What the data establishes is the stakes. Recovery is the point at which stated capability and actual capability diverge, the divergence is large, and an organization that discovers at restore time that its only viable target is the platform it has just lost is discovering it in the worst available circumstances.

Recovery scenario	Closed stack	Open architecture
Ransomware event	Restore is only possible onto the same platform that was compromised	Workloads restore onto clean infrastructure, a different cluster, or an isolated region
Hypervisor or licensing change	Backup images are readable only by the incumbent virtualization vendor	Open disk and manifest formats re-instantiate on KubeVirt, OpenStack, or another distribution

Recovery scenario	Closed stack	Open architecture
Jurisdictional or geopolitical move	Relocation requires a migration project and vendor cooperation	Data and operational state reconstitute on any compliant provider
Cloud exit or repatriation	Application and data are re-architected to leave	Kubernetes objects, CSI snapshots, and S3-compatible storage restore on-premises or to a local provider

Organizations that can recover applications independently of their original infrastructure retain strategic freedom. Organizations whose recovery depends upon proprietary platforms do not. This is why Recovery Sovereignty becomes the defining characteristic of ASL 5.

Recovery is not an ASL 5 concern that only arrives at the end of the journey.

It is present at every level; what changes is how much of it the organization actually controls.

- ✓ ASL 1, recovery is a contractual commitment — the provider states an objective and the organization takes it on trust.
- ✓ ASL 2, the organization runs and tests the restore itself, but still inside the platform it was given.
- ✓ ASL 3, the recovery target becomes a choice rather than a default, because workloads are captured in formats more than one platform can read.
- ✓ ASL 4, recovery and migration converge: the same mechanism that restores after an outage is the mechanism that relocates workloads when a license, a jurisdiction, or a commercial relationship changes.
- ✓ ASL 5, recovery is fully independent of the original infrastructure, and it is that independence — not the backup schedule — that defines the level.

Regulators have reached the same conclusion from a different direction. The EU Digital Operational Resilience Act, which has applied to financial entities since January 2025, requires more than the existence of backups: firms must maintain ICT continuity and recovery plans, define and test recovery time and recovery point objectives, and hold documented exit

strategies for critical ICT third-party providers — meaning they must be able to demonstrate that they could actually leave. The NIS2 Directive imposes parallel business continuity, backup management, and disaster recovery obligations across a far wider population of essential and important entities. Neither regime is satisfied by a recovery plan that works only if the incumbent vendor cooperates. An exit strategy that depends on the provider being exited is not an exit strategy, and a recovery objective that can only be met on the platform that failed is not a recovery objective. Open formats are what make these obligations demonstrable rather than aspirational.

The operator architectures described later in this paper are where the requirement is tested. Red Hat's move to in-region software delivery matters for recovery specifically: an organization rebuilding under time pressure needs its update streams and package sources to be locally authoritative and reachable, not dependent on a content network in another jurisdiction. Core42's Signature Private Cloud offers dedicated, multi-tenant, and air-gapped deployment models across three availability zones, which means the realistic recovery target for a classified workload is another sovereign environment under the same national controls — not a public region that would breach the classification on restore. Both point to the same conclusion. The recovery path has to terminate somewhere the organization is permitted to operate, and the set of permitted destinations is determined by the portability of the backup format long before it is determined by available capacity.

AI workloads sharpen the problem further, and most recovery plans have not caught up. A production inference service is not a single application. It is model weights, adapters and fine-tuning artifacts, vector indexes and their embedding provenance, feature stores, prompt and guardrail configuration, accelerator scheduling state, and the audit trail establishing which model version produced which output. Restoring the container without the vector index yields a service that runs and answers incorrectly — a failure mode that conventional recovery testing rarely detects. Sovereignty compounds it. Weights and embeddings are derived from training data and carry its residency and classification obligations with them, so a restore into the wrong jurisdiction can itself constitute a transfer of the underlying data. If an organization cannot rebuild its AI stack on infrastructure it chooses, in a jurisdiction it is permitted to use, with lineage intact, then its AI sovereignty is a claim about steady-state operations only.

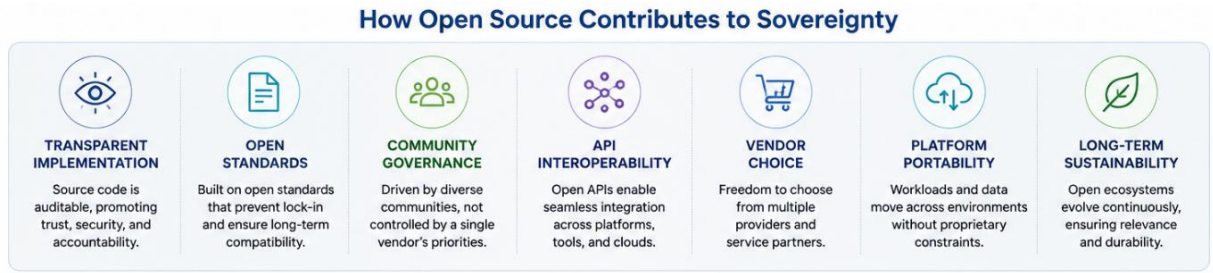
Recovery, in short, is what transforms sovereignty from a compliance exercise into an operational capability.

Why Open Source Matters More at Higher ASL Levels

One of the most revealing observations from the Architectural Sovereignty Level (ASL) framework is that the role of open source evolves as organizations mature.

At lower levels of sovereignty, open source is often viewed simply as an infrastructure component. Linux powers servers, PostgreSQL supports applications, Kubernetes orchestrates containers, and numerous open source projects provide foundational capabilities throughout the technology stack. While these technologies are important, they are not necessarily strategic. Organizations can achieve regulatory compliance while relying heavily on proprietary infrastructure, commercial software, and vendor-managed services.

As enterprises progress toward higher levels of sovereignty, however, the role of open source changes fundamentally.



It shifts from being a collection of technologies to becoming an architectural strategy that preserves long-term flexibility.

This distinction is critical: the objective is not to eliminate proprietary software, but to ensure that no single technology decision permanently limits future choices.

That is where open ecosystems become increasingly valuable.

One misconception surrounding Sovereign Cloud is that sovereignty requires only domestic infrastructure.

But history demonstrates otherwise.

Organizations can operate entirely within national borders while remaining dependent upon proprietary operating systems, virtualization platforms, storage architectures, AI frameworks, or recovery software.

The opposite is also true.

Organizations using open technologies often possess significantly greater strategic independence despite operating across hybrid environments. That hybrid posture is the norm, not the exception: SUSE found that 59 percent of enterprises are prioritizing hybrid cloud for workloads where sovereignty is required, with 16 percent going purely private, and 65 percent still consider hyperscalers relevant to supporting sovereign workloads. Sovereignty, in practice, is being pursued alongside the global providers rather than by withdrawing from them — which is precisely why open, interoperable architecture carries the weight.

Open source contributes to sovereignty because it encourages characteristics that proprietary ecosystems often limit.

Buyers are already voting this way. In the 2026 State of Open Source Report from Perforce, the Open Source Initiative, and the Eclipse Foundation, avoiding vendor lock-in emerged as a leading driver of open source adoption, cited by 55 percent of respondents — a 68 percent year-over-year increase. The pattern is sharpest in Europe, where 63 percent of EU and UK organizations named lock-in as a top reason for choosing open source, against 51 percent in North America. Policy is moving in the same direction: the European Commission's Technological Sovereignty Package includes the first full EU Open Source Strategy and frames concentration of digital infrastructure among a few dominant proprietary providers as a strategic vulnerability rather than merely a competition issue.

Red Hat makes the strongest version of this argument. Its stated position is that the only credible path to digital sovereignty is a foundation built on open source, because open source inherently delivers the transparency and auditability that regulators and organizations require — a posture the company contrasts explicitly with proprietary "sovereign" offerings built on closed software and opaque architectures. Chris Wright, Chief Technology Officer and Senior Vice President of Global Engineering at Red Hat, framed it in terms of ‘destiny’ rather than ‘jurisdiction’: "Digital sovereignty means keeping control over your own technology destiny,

from data location to software and operations." Navigating the EU's regulatory and compliance frameworks, he added, demands an open source-driven, transparent, auditable foundation together with a local operational support model. The pressure is sharpest in AI. An IDC Market Perspective cited by Red Hat found that nearly nine in ten organizations globally want choice and control when deploying AI at scale, and more than half prefer open models to closed, proprietary ones — the same optionality argument, arriving one layer up the stack.

SUSE's research puts a number on the architectural conviction behind that shift: 94 percent of the IT leaders surveyed rated open source as very or extremely important to digital resilience — 41 percent extremely, 53 percent very — with none dismissing it as unimportant. The lock-in anxiety driving that view is no longer a European phenomenon either. In SUSE's Cloud and AI Pulse Survey of nearly 600 enterprise technology leaders across the United States, United Kingdom, Japan, India, and Germany, 39 percent of U.S. enterprises cited concern about vendor lock-in, well above the 25 percent global average, and roughly a third of U.S. respondents ranked digital sovereignty a top technology priority.

That conviction is now showing up in national-scale deployments. In May 2026, Red Hat announced a collaboration with Core42, a G42 company providing sovereign cloud and AI infrastructure, to architect and deliver sovereign cloud and AI services for the public sector, defense, and other regulated industries across the UAE — positioned explicitly as combining open source transparency with the operational control those environments demand. It is a useful reference point precisely because it pairs the two properties this paper argues are inseparable: an open technology base, and sovereign operational control exercised over it.

Importantly, open source does not automatically create sovereignty.

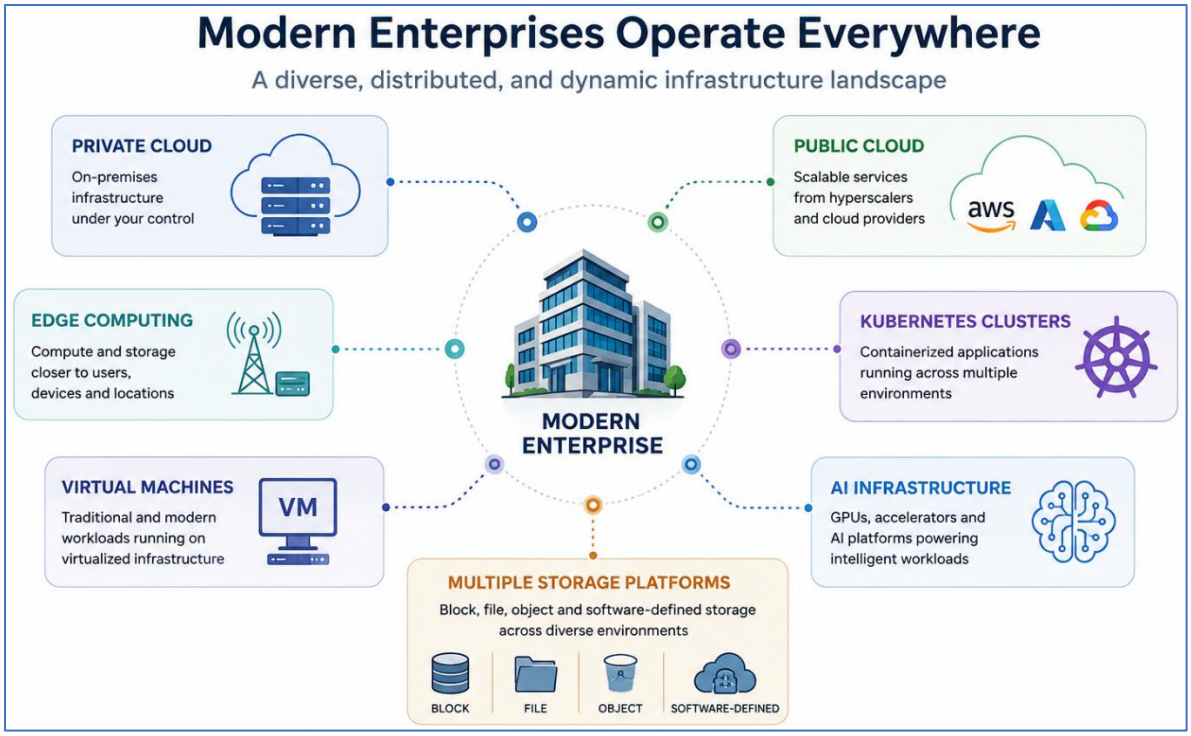
An enterprise can still become operationally dependent on a single commercial distribution, service provider, or managed platform.

However, as organizations progress toward higher ASL levels, open ecosystems provide significantly more opportunities to preserve architectural freedom.

Open Source Creates Common Operating Models

Another reason open source becomes more important at higher ASL levels is that it establishes common operating models across increasingly diverse environments.

Modern enterprises rarely operate within a single infrastructure platform.



Managing each environment independently quickly becomes operationally unsustainable.

Open technologies address this challenge by providing consistent abstractions.

- ✓ Linux provides a common operating system across hardware vendors.
- ✓ Kubernetes provides a common orchestration layer across cloud providers.
- ✓ Containers standardize application packaging.
- ✓ GitOps standardizes deployment workflows.
- ✓ OpenTelemetry standardizes observability.
- ✓ S3-compatible object storage standardizes data access.
- ✓ OCI image specifications standardize software distribution.

A common operating model is what turns a collection of open components into something an organization can actually run at scale, and the sovereignty gain always comes from the same property: “a standardized, open control plane that behaves identically wherever it runs”. These standards reduce operational complexity while simultaneously increasing scale and portability. Furthermore, organizations gain consistency without sacrificing flexibility.

The major open source vendors describe the same mechanism in their own terms. Red Hat frames its open source model as producing a consistent "operating layer" — grounded in

transparency, upstream contribution, and open standards — that builds trust, mitigates vendor lock-in, and supports an ecosystem of local partners.

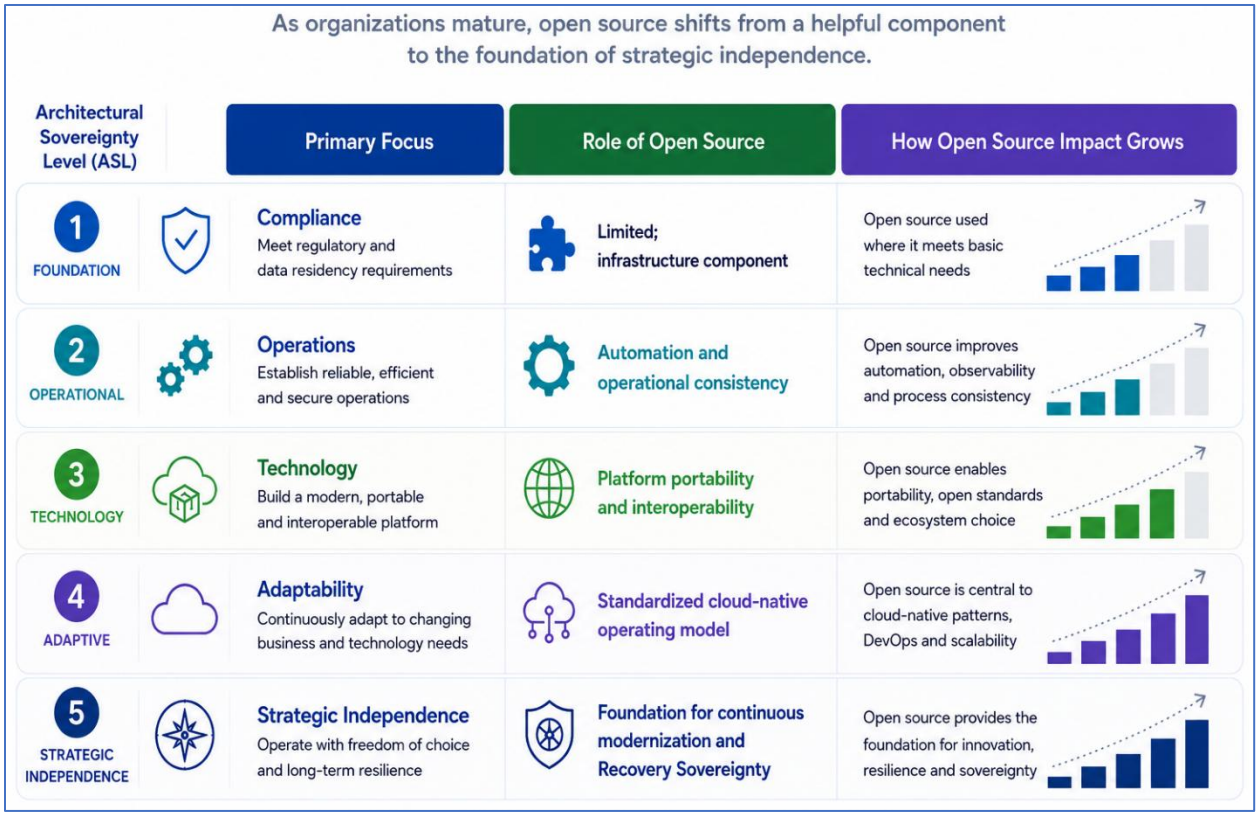
The Relationship Between Open Source and ASL

One of the most interesting observations emerging from this framework is that the importance of open source increases at every maturity level.

The progression is visible in the level definitions themselves:

- ✓ ASL 1, open components are present but incidental — the architecture would behave much the same if they were proprietary.
- ✓ ASL 2, open operational tooling makes the organization's own knowledge transferable rather than provider-specific.
- ✓ ASL 3, open standards become the interfaces the architecture is assembled from, which is the first point at which openness changes what is structurally possible rather than merely what is convenient.
- ✓ ASL 4, the open layer is load-bearing: workload mobility across platforms and clouds exists because shared abstractions exist.
- ✓ ASL 5, open formats determine whether the organization can rebuild at all. The relationship inverts along the way. Early on, open source is something the architecture happens to contain; by the highest level, it is what the architecture's freedom is made of.

One qualification is worth stating plainly. The evidence assembled in this paper establishes that enterprises are choosing open technologies specifically to avoid lock-in, that they regard open source as central to digital resilience, and that regulators and public buyers are converging on transparency, portability, and exit capability as procurement requirements. It does not establish a measured causal link between open architecture and higher sovereignty outcomes, because no longitudinal study of that question yet exists. The argument here is structural rather than statistical: open formats and open interfaces enlarge the set of moves available to an organization over time, and the assurance levels are a way of counting those moves. It should be weighed on that basis.



This does not imply proprietary software has no place in Sovereign Cloud.

Commercial software delivers innovation, enterprise support, security, and operational capabilities that many organizations require.

Instead, the lesson is architectural.

Open technologies provide the connective tissue that allows commercial innovation to coexist with strategic flexibility.

- ✓ They reduce the cost of change.
- ✓ They increase interoperability.
- ✓ They preserve future choice.

The Role of Commercial Software Evolves

Commercial software continues to play a critical role in Sovereign Cloud strategies, even as organizations progress to higher levels of the Architectural Sovereignty Level (ASL). The goal of increasing sovereignty is not to eliminate proprietary software or replace commercial innovation with open source alternatives. Rather, it is to ensure that commercial technologies are deployed within an architecture that preserves **long-term flexibility and freedom of choice.**

In fact, many of the world's largest Sovereign Cloud deployments are built on a combination of open source foundations and enterprise commercial platforms. Organizations rely on commercial software because it delivers capabilities that are essential for operating mission-critical environments. These include enterprise-grade support, certified hardware and software integrations, security hardening, regulatory certifications, lifecycle management, advanced automation, and operational tooling that simplify deployment and ongoing operations.

The distinction, therefore, is not between open source and proprietary software — it is between open architectures and closed architectures. A Sovereign Cloud should be designed so that the underlying platform remains sufficiently open to allow organizations to replace or upgrade individual commercial components without requiring wholesale changes to the surrounding infrastructure. When an organization can adopt a new virtualization platform, change storage vendors, modernize its Kubernetes distribution, or introduce new AI capabilities without redesigning its entire technology stack, it has preserved the architectural flexibility that sovereignty requires.

This approach recognizes that commercial innovation and open source are not competing philosophies; they are in fact complementary. **Open source provides the standardized interfaces, interoperability, and portability that preserve long-term optionality**, while commercial software builds upon those foundations to deliver enterprise functionality, operational maturity, and support. Together, they enable organizations to innovate without becoming dependent on a single vendor or proprietary ecosystem.

This architectural model is increasingly reflected across the industry's leading enterprise platforms. Enterprise Linux distributions combine community innovation with commercial support and long-term maintenance. Kubernetes platforms provide certified enterprise capabilities while remaining built on upstream open standards. AI frameworks increasingly embrace open model interfaces and interoperable tooling, and cloud-native security, virtualization, and data protection platforms are adopting similar approaches. The result is an ecosystem where organizations can benefit from commercial innovation while retaining the strategic flexibility to evolve their infrastructure as business requirements, regulations, and technologies continue to change.

Red Hat
Red Hat's recent sovereign portfolio moves illustrate the pattern concretely. Red Hat OpenShift on Google Cloud Dedicated, announced in April 2026 and slated for general availability in the second half of that year, places a commercially supported Kubernetes platform on isolated hyperscaler infrastructure for financial services, healthcare, and public sector organizations, addressing data residency, technological autonomy, and supply chain resilience together rather than separately. The May 2026 portfolio expansion pushed the same logic into operations: cost management telemetry for OpenShift that remains entirely

within customer-controlled environments instead of crossing sovereign boundaries, and localized software delivery beginning in the EU, where customers and partners download Red Hat Enterprise Linux from in-region content delivery and establish local authority over their update streams. Red Hat Confirmed Sovereign Support, announced in November 2025, extends the principle to the support relationship itself by keeping diagnostic data inside jurisdictional boundaries. None of these are open source projects in themselves; each is a commercial capability built on an open foundation, which is exactly the arrangement this section describes.

The same pattern appears one layer up, among the providers actually operating sovereign environments at national scale. Core42, a G42 company, builds its Signature Private Cloud for governments and enterprises running secret and top-secret workloads, and is explicit that full-stack control comes from open source: the platform is built on open source technologies alongside Core42-owned intellectual property, which the company positions as the means of eliminating dependency on foreign-controlled cloud providers while preserving transparency and interoperability. The surrounding architecture is otherwise conventional sovereign-cloud engineering — dedicated, multi-tenant, and air-gapped deployment models mapped to national data classification levels; a three-availability-zone design linked by private dark fiber; integrated identity, key management, monitoring, and audit services; and in-country hosting operated by vetted personnel. What matters here is the layering. The sovereignty claim rests on an open foundation rather than on contractual assurances about a closed one.

Core42 extends the same model into the AI layer through its AI Cloud, which combines GPU-as-a-service and inference-as-a-service with unified orchestration, observability, and sovereignty controls under a single control plane. The company's stated premise is that **sovereignty and governance have to be foundational architecture rather than a procurement detail, because an enterprise cannot embed AI into critical workflows at scale without controlling where its data resides, how it moves, and which jurisdictions apply**. Operators of this kind are where the higher assurance levels stop being theoretical. They demonstrate that a provider can deliver hyperscale-grade capability, national-grade security, and classified-workload isolation without adopting a closed stack — and that the apparent trade-off between capability and optionality largely dissolves when the foundation is open.

Final Thoughts

Sovereign Cloud is entering its next phase of maturity. The conversation is moving beyond data residency toward strategic independence, architectural resilience, and long-term freedom of choice. Organizations now need a way to measure progress along that journey.

The **Architectural Sovereignty Level (ASL)** offers one possible framework. It shifts the discussion from **where** systems run to **how effectively** an enterprise preserves control over its technology decisions across changing business, regulatory, and operational conditions.

As organizations progress through higher assurance levels, one trend becomes increasingly clear: **openness enables optionality**. Open standards, open APIs, and mature open source ecosystems make it easier to modernize infrastructure, integrate new technologies, adopt sovereign AI, and recover from disruption without introducing new forms of vendor lock-in.

Sovereignty is therefore not achieved through isolation. ***It is achieved through architectural freedom.***

And in an era of constant technological change, the ability to adapt may be the highest assurance level of all.

Sources

- European Commission, Cloud Sovereignty Framework (SEAL-0 to SEAL-4 assurance levels); eight sovereignty objectives, minimum-level thresholds, and weighted sovereignty score.
- European Commission, "Commission advances cloud sovereignty through strategic procurement" (April 17, 2026) and "Sovereign Cloud Framework explained" (June 1, 2026) — Cloud III dynamic purchasing system award, SEAL-2 minimum threshold.
- Atos, "Cloud sovereignty: Who holds the keys?" (2026) — https://atos.net/en/blog/cloud-sovereignty-who-holds-the-keys
- Gartner, "Worldwide Sovereign Cloud IaaS Spending Will Total $80 Billion in 2026" (press release, February 9, 2026); Forecast Analysis: Sovereign Cloud IaaS, Worldwide.
- Forrester, The State of Digital Sovereignty in Public Cloud, 2026, and Forrester global cloud survey data on sovereignty in vendor selection.
- IDC, Sovereign Cloud in Europe 2026: From Inflection Point to Operational Mandate (Market Perspective, May 2026).

- Perforce Software, Open Source Initiative, and Eclipse Foundation, 2026 State of Open Source Report (March 2026).
- SUSE, Navigating Digital Resilience 2026 (April 2026) — survey of 309 IT leaders across France, Germany, India, Japan, and the U.S.; respondents were not aware SUSE sponsored the research.
- SUSE, Cloud and AI Pulse Survey (March 2026) — 596 enterprise technology leaders in the U.S., U.K., Japan, India, and Germany.
- Kyndryl, 2025 Cloud Readiness Report.
- European Commission, European Technological Sovereignty Package, including the EU Open Source Strategy (2026).
- Red Hat, "Digital sovereignty solutions from Red Hat" (data, technology, operational, and assurance sovereignty pillars).
- Red Hat, "Red Hat Introduces Confirmed Sovereign Support for European Union" (press release, November 6, 2025) — quoted remarks by Chris Wright, CTO and Senior Vice President, Global Engineering.
- Red Hat, "Red Hat Introduces New Sovereign and Private Cloud Capabilities to Power Digital Autonomy" (press release, May 12, 2026).
- Red Hat, "Red Hat Further Drives Digital Sovereignty for the AI Era with Red Hat OpenShift on Google Cloud Dedicated" (press release, April 21, 2026).
- Core42, "Core42 Signature Private Cloud" (product overview) — https://www.core42.ai/products/signature-private-cloud
- Core42, Scaling Enterprise Intelligence with AI Cloud (whitepaper).
- European Union, Digital Operational Resilience Act (Regulation (EU) 2022/2554), applicable from January 17, 2025 — ICT continuity and recovery planning, recovery objectives, and exit strategies for critical ICT third-party providers.
- European Union, NIS2 Directive (Directive (EU) 2022/2555) — business continuity, backup management, and disaster recovery obligations for essential and important entities.
- Sophos, The Impact of Compromised Backups on Ransomware Outcomes (2024) — analysis of 2,974 ransomware victims; recovery cost differential where backups were compromised.
- Scality, 2026 Cyber Resilience Trends — survey of security leaders on recovery time objective confidence versus realized incident outcomes.

Glossary

ASL (Architectural Sovereignty Level) — The five-level maturity scale introduced in this paper, measuring how much freedom an organization retains to change its technology direction over time. Distinct from the European Commission's SEAL, which grades jurisdictional control; ASL levels do not correspond to SEAL levels.

Cloud Native Computing Foundation (CNCF) — The open source foundation that hosts Kubernetes and a broad portfolio of cloud-native projects, providing neutral governance and conformance programs that keep implementations interoperable.

CSI (Container Storage Interface) — A standard interface between container orchestrators and storage systems, allowing volumes and snapshots to be provisioned consistently across different storage vendors.

Geopatriation — The relocation of workloads and data from global public cloud providers to local or regional providers, typically driven by regulatory, geopolitical, or sovereignty requirements.

GitOps — An operational model in which the desired state of infrastructure and applications is declared in version control and reconciled automatically, standardizing deployment workflows across environments.

Hybrid Cloud — An architecture that combines private infrastructure with one or more public cloud environments, operated under a common set of tools and policies.

Infrastructure as Code (IaC) — The practice of defining and provisioning infrastructure through machine-readable configuration files rather than manual processes, making environments reproducible and portable.

Kubernetes — The open source container orchestration platform that has become the de facto standard control plane for cloud-native workloads across on-premises and public cloud infrastructure.

KubeVirt — An open source project that runs virtual machines as Kubernetes workloads, enabling VMs and containers to be managed through a single control plane.

OCI (Open Container Initiative) — The specifications governing container image and runtime formats, ensuring images built once can run on any conforming platform.

Open Source — Software distributed under a license that permits inspection, modification, and redistribution of the source code, typically developed under community or foundation governance.

OpenStack — An open source platform for building and operating private and public cloud infrastructure, widely used in sovereign and regulated cloud deployments.

OpenTelemetry — A vendor-neutral standard for generating and collecting telemetry data — traces, metrics, and logs — enabling consistent observability across heterogeneous environments.

Optionality — The ability to change technology direction without unacceptable cost, operational disruption, or architectural constraint; the practical measure of sovereignty used throughout this paper.

Recovery Sovereignty — The ability to restore applications, data, and operational state onto infrastructure other than the platform they originally ran on, without dependence on a single vendor's formats or tooling.

S3-Compatible Object Storage — Object storage that implements the widely adopted S3 API, allowing data to be written and read across different storage providers without application changes.

SEAL (Sovereignty Effectiveness Assurance Level) — A graded scale for assessing how much real control an organization retains over a cloud service. Introduced by the European Commission's Cloud Sovereignty Framework, it runs from SEAL-0 to SEAL-4 and is a jurisdictional measure; see ASL for the architectural counterpart used in this paper.

Sovereign Cloud — Cloud infrastructure designed to keep data, operations, and control subject to a specified jurisdiction and to the organization's own governance rather than a foreign or third-party authority.

Vendor Lock-In — A condition in which the cost, complexity, or technical difficulty of moving away from a supplier is high enough that the supplier's roadmap effectively constrains the organization's own decisions.

Workload Portability — The ability to move applications and their data between infrastructure platforms, clouds, or regions without re-architecting them.

About Trilio

Trilio builds cloud-native data protection for the platforms that sovereign and regulated organizations actually run on — Kubernetes and OpenShift, OpenStack, and open virtualization environments including KubeVirt and OpenShift Virtualization.

Trilio's approach is built around the principle described throughout this paper: recovery is where architectural freedom is proven. Rather than capturing workloads in a proprietary backup format, Trilio protects them as the open constructs they are built from — Kubernetes objects, persistent volumes, CSI snapshots, container images, and metadata — and stores them in NFS or S3-compatible object storage. Because the backup itself carries no vendor dependency, applications can be restored onto a different cluster, a different distribution, or a different cloud.

That portability is what allows data protection to support sovereignty rather than quietly undermine it. Organizations can modernize infrastructure, change virtualization platforms, respond to a ransomware event by restoring into clean infrastructure, or relocate workloads across jurisdictions without their recovery plan becoming the constraint.

Trilio works with public sector agencies, telecommunications providers, financial institutions, and enterprises operating mission-critical open infrastructure, and partners closely with the broader open source ecosystem to keep recovery an open capability rather than a point of lock-in.

To learn more, visit trilio.io.