Elements of cloud sovereignty

The sovereign challenge

Organizations are increasingly recognizing the need for digital sovereignty, which is the ability of a nation or organization to independently control and protect its critical digital infrastructure in alignment with its policies, values, and strategic objectives. The need for digital sovereignty is prompted by regulatory compliance, geopolitical uncertainty, security concerns, and the desire for greater control over data and technology. Implementing a sovereign cloud is one way to help meet these requirements, particularly for sensitive data and workloads that could have severe consequences if leaked or compromised.

A sovereign cloud is an environment designed to adhere to a nation's data residency, operational independence, and regulatory compliance mandates, ensuring that all data, applications, and operations remain within its borders and under its control.

A sovereign cloud environment goes beyond data residency, which is typically maintained within a jurisdictional, often national, compliance boundary. It also involves using in-country datacenters, geo-fencing policies for data localization, maintaining operational independence through local staffing and supply chain control, workload protection, access control, and auditing. While many of these elements are already in place, meeting and documenting sovereignty requirements while keeping the agility and flexibility of a cloud-native experience remains a challenge.

In addition, sovereignty emphasizes strong isolation from external dependencies, built-in regulatory compliance tools, transparency in data flow, secure connectivity, and scalable, resilient infrastructure, all working in concert to safeguard critical national infrastructure and foster trust.

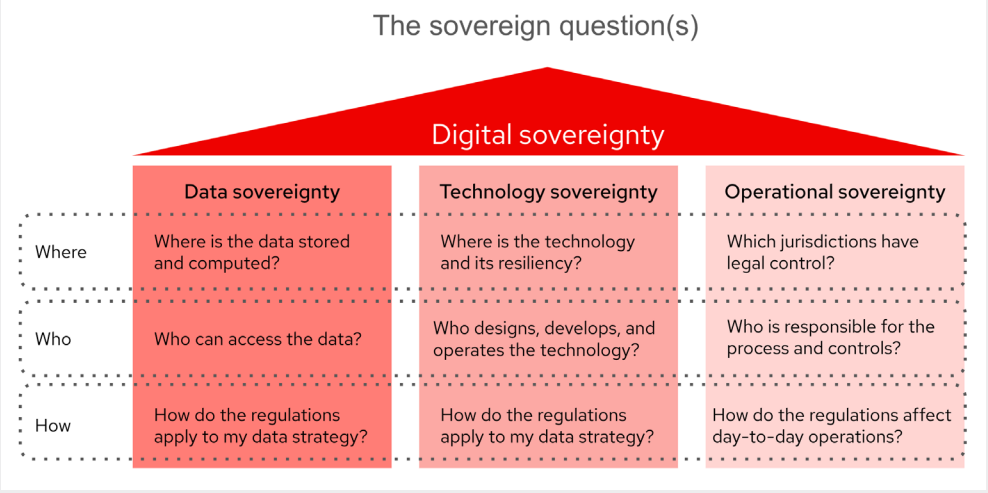

Figure 1. FAQs about digital sovereignty

A sovereign cloud provides the nimbleness, innovation, and cost savings of a traditional cloud environment while addressing concerns about data extraterritoriality, foreign government access, and control over critical national infrastructure.

The boundaries between data, technology, and operational sovereignty are not hard lines; in fact, they are actually intertwined. For example, data sovereignty focuses on data location and access, while technology sovereignty broadens the scope to encompass the entire technology stack, including hardware, software, and services.

Data sovereignty

While data sovereignty is, at times, defined as solely a nationalistic concern influenced by the need to prioritize products and services made in a country, it can also be viewed as a requirement for control, specifically over data sharing, where data is located, transmitted, and used. This necessitates that data and support personnel be located within specific national or regional boundaries. Additionally, operational independence, continuity in disconnected environments, and trusted software provenance are key customer expectations for data sovereignty.

Technology sovereignty

Technology sovereignty is predicated on the application of key control requirements. Nearly every organization is already taking advantage of some level of access management and security protocols, and the requirements for technology sovereignty stress how these controls interact with critical technologies and data, extending beyond traditional authentication to ensure verifiable trust in code artifacts and reproducible builds. The aim is to protect organizations against hidden backdoors or vulnerabilities that could be exploited by external actors.

Operational sovereignty

Technology sovereignty necessitates operational independence and continuity, even in the face of geopolitical instability or restrictions. It may include running systems in disconnected or air-gapped environments to keep critical services available regardless of internet access or supply chain issues. It also involves localized support and guarantees operational continuity, allowing organizations to maintain activities and deliver services without relying on external, potentially compromised entities.

Model for sovereign cloud

There are numerous potential architectures for addressing the sovereignty requirements of a nation or organization's infrastructure. Simply put, a sovereign architecture must provide control and transparency over core services, such as networking, fleet management, automation, and key management, while also ensuring control and isolation. The diagram below provides a high-level view of the key elements required when architecting a sovereign cloud.

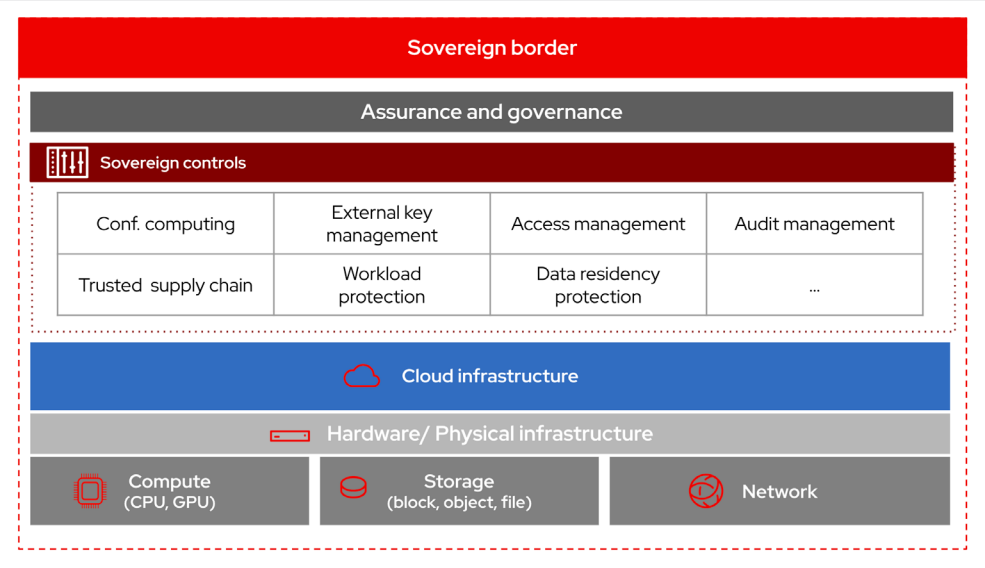

Figure 2. Key requirements for sovereign cloud

Let us look a little deeper into the key areas influencing the need for a sovereign cloud and how Red Hat is helping our customers meet sovereign requirements.

Inside the sovereign border

At the heart of a sovereignty cloud is the notion of autonomy, where all or nearly all technology elements reside inside the organization's or nation's borders. To put it simply, cloud sovereignty requires that foundational infrastructure, including storage, compute, network, hardware, and supporting operations, be physically located in the country or region of residence.

Cloud infrastructure

Cloud infrastructure is paramount to sovereignty, influenced by the need for data and operational control. Due to data residency requirements, organizations will seek to choose cloud providers with datacenters in specific jurisdictions, whether they are global giants like Amazon Web Services (AWS), Azure, and Google Cloud, or specialized local providers.

Deciding between single and multitenancy models impacts sovereignty. Single-tenancy, preferred for strict needs, offers more isolation with dedicated resources. Multitenancy is cost-effective, but it raises concerns about shared infrastructure. The choice depends on an organization's needs for data location, access, independence, and trust in the software supply chain, all of which are crucial for true cloud sovereignty.

Sovereign controls

A set of sovereign controls can be applied at the organizational level. These controls are requirements that all sovereign clouds use. Organizations need the ability to make precise decisions regarding the physical location of their infrastructure and to control who can access their systems and data. This

level of control extends to operational processes like disaster recovery (DR), incident management, data retention, and auditing. While certainly not an exhaustive list, these sovereign controls can include:

- *Data encryption.* This ensures data remains encrypted and protected even while in use by isolating it from the underlying infrastructure (i.e., confidential computing).
- *External key management.* Helps organizations maintain full control over encryption keys, which are often stored on their own hardware or with a trusted third party, separate from the cloud provider.
- *Access and identity management.* Provides granular control over who can access systems and data, including specific national or regional personnel requirements.
- *Audit management.* Allows comprehensive logging and monitoring of all activities, ensuring transparency and accountability for data access and system changes.
- *Software supply chain security.* This ensures the integrity and provenance of all software components, preventing hidden backdoors or vulnerabilities through measures like reproducible builds and geographic signing.
- *Workload protection.* Secures applications and data throughout their lifecycle, including in disconnected environments, ensuring operational independence and continuity.
- *Data residency protection.* Mandates that data is stored and processed within specific national or regional geographic boundaries, adhering to local laws and jurisdictional requirements.

Who is involved, and what steps are needed to deliver sovereign controls

The infrastructure and tools needed to deliver a business function, while remaining compliant with sovereign regulations, require collaboration across the organization. For platform engineering teams seeking to design and implement a comprehensive range of sovereign controls, the work begins with understanding and documenting the various requirements. Information security (Infosec) teams, along with risk and compliance, are a critical component to building this understanding, defining the security policies and controls that platform teams will build.

Using the example in Figure 2, let us focus on the policy management control. In this control, the compliance and governance team begins by interpreting regulations and developing requirements and control recommendations to mitigate risk. The Infosec team defines the policy for data sovereignty, which includes data classification, access controls, and encryption requirements. The Platform team reviews the requirements and looks to acquire or build the appropriate tools to accommodate them. This is not a new process. However, with sovereign controls, the Platform and Infosec teams must apply this rigor across many controls, weaving sovereign and technical requirements into the platform without sacrificing control, transparency, or agility. Once the sovereign controls are built, a common control plane can be constructed.

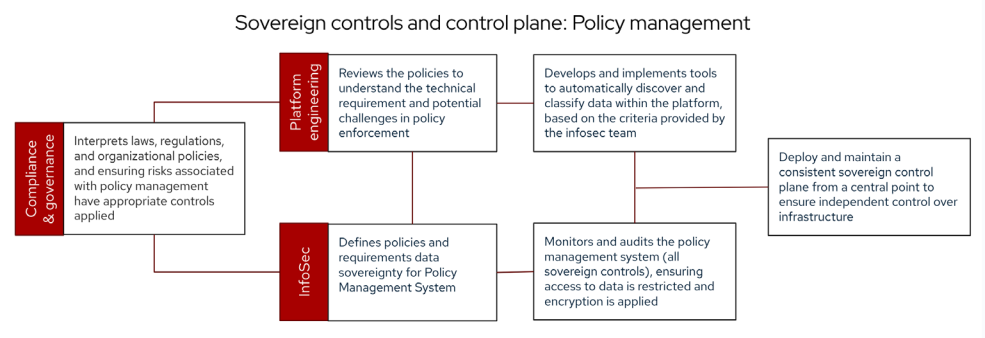

Figure 3. High-level workflow of sovereign control for policy management

How Red Hat can help

Red Hat empowers our customers to achieve resiliency, autonomy, and independence by providing:

- *Transparency.* Red Hat enterprise open source solutions build trust that is vital for digital sovereignty. Our open source model allows community contributions, ensuring Red Hat's transparency, security-focus, and reliability. An upstream-first policy develops changes for community use, enhancing security, compliance, and supply chain integrity. This model helps nations control digital assets by supporting software adaptation. Red Hat provides transparency with hardening, lifecycle management, and support for critical deployments, fostering trust for autonomy and resilience.
- *Control.* Red Hat's open hybrid cloud strategy offers organizations extensive deployment options—on-premise, cloud, or edge—supported by a global ecosystem of cloud service provider (CSP) partners. This supports choosing suitable technologies and local expertise to meet sovereignty needs now and in the future. Red Hat's open standards and consistent experience prevent vendor lock-in and make IT investments ready for the future, offering agility amid evolving regulations and tech. For example, running applications in Red Hat® OpenShift® allows smooth migration to different infrastructures if hyperscalers no longer meet sovereignty requirements.
- *Operational stability.* Red Hat technologies are vital for enhancing digital sovereignty and safeguarding critical infrastructure, addressing regulations like the European Union's (EU) Digital Operational Resilience Act (DORA). Our solutions, with partner support, protect sensitive data, improve backup and recovery, bolster business continuity, and enhance software supply chain security, improving resiliency in organizations. Red Hat's portfolio offers capabilities such as data snapshots, archiving, and improving Recovery Point Objective/Recovery Time Objective (RPO/RTO) through configuration management and automated failover. The products and services provide the flexibility necessary for sovereign solutions now and in the future.

Learn more

Discover how Red Hat's open hybrid cloud approach and robust security features can help your organization achieve true digital sovereignty. Explore the many ways Red Hat and our partner ecosystem can help you safeguard sensitive data, ensure operational independence, and maximize your business potential.

Visit digital sovereignty solutions from Red Hat to learn more.

About Red Hat

Red Hat helps customers standardize across environments, develop cloud-native applications, and integrate, automate, secure, and manage complex environments with award-winning support, training, and consulting services.

facebook.com/redhatinc
@RedHat
linkedin.com/company/red-hat

North America
1 888 REDHAT1
www.redhat.com

Europe, Middle East, and Africa
00800 7334 2835
europe@redhat.com

Asia Pacific
+65 6490 4200
apac@redhat.com

Latin America
+54 11 4329 7300
info-latam@redhat.com

redhat.com
#2464003_0725