Cloud Sovereignty for banks

Discover why cloud sovereignty is becoming paramount

The cloud sovereignty imperative for banks

Many banks are focusing their cloud strategy on sovereignty as an important need on top of the traditional drivers of financial savings, security, speed, and agility. It concerns control and survival in an intensely fractured world driven by protectionism. Many banks are also dependent on cloud vendors to deliver their critical services. This dependency has raised the stakes for both regulators and the companies that are being regulated. Cloud sovereignty focuses on jurisdictional control and operational autonomy, and it has become an important factor in how banks operate across the globe.

Banks are moving toward a sovereign cloud for 3 primary reasons.

1. **Changing regulatory landscape:** One-size-fits-all global cloud models have reached an end. Stricter, regional regulations like the European Union's (EU) General Data Protection Regulation (GDPR) and Digital Operational Resilience Act (DORA) as well as guidelines from national bodies such as the Reserve Bank of India India or the Federal Financial Supervisory Authority in Germany (BaFin) are adding increasingly divergent rules on governing cloud services within national or regional borders.
2. **Growing threat of extraterritorial interference:** Banks are a fundamental cornerstone to the economy and handle more than sensitive information. Yet, a service disruption can have a negative cascading effect across the economy. Foreign interference and surveillance are genuine concerns in a rapidly changing geopolitical environment.
3. **Surging operational risks:** Sovereign clouds aim to bolster operational resilience, a key focus for regulators. By using cloud architectures that are self-contained from global cloud services, banks can reduce the risk of a global service outage affecting their services.

Banks no longer have to be constrained by a general purpose approach to the cloud. These tailored clouds can reduce operating risks and costs. Importantly, emerging sovereign cloud architectures can help strengthen service continuity, reduce compliance costs, address security needs, and protect their customers from foreign interference.

The Red Hat approach to cloud sovereignty

A better way to protect the bank

Red Hat's approach to cloud sovereignty is built upon the core principles of control, transparency, and choice. This strategy minimizes complexity for Red Hat customers and partner ecosystem, providing the delivery of protected, sovereign solutions.

The value of this approach simplifies cloud operations with less risk and cost, which can be achieved by embracing these 3 pillars.

Uninterrupted software supply chain

A community-based approach to open source ensures supply chain continuity and on-demand auditability. It gives control over their technology stack, without foreign interference. The community-driven approach also fosters standardization and reduces the risk of malicious code. Red Hat delivers cryptographically signed software with verified provenance. This approach provides the auditable security and integrity that are essential for trust in business-critical infrastructure. It also prevents dependence on a single vendor—the core threat to technical independence.

Continuous compliance

Keeping the bank compliant.Red Hat focuses on strengthening organizational resilience to protect critical infrastructure from disruption and mitigate the risks by regulations such as DORA. Red Hat® OpenShift® facilitates integration with hardware security modules, allowing customers to maintain dedicated control over encryption keys—a critical defense against extraterritorial legal access. The platform ensures protection goes beyond data residency and provides tools for workload protection, including zero trust computing and advanced encryption. Furthermore, Red Hat OpenShift allows for rapid disaster recovery and business continuity through automated fail over and Recovery Point Objective (RPO) and Recovery Time Objective (RTO) improvements, fortifying the software supply chain against external threats.

Simplify resilience

Applying consistent operational policies across disparate cloud environments can be a costly challenge. Red Hat OpenShift provides a unified operating platform across on-premise, public, and hybrid cloud infrastructures. With this flexibility, workloads can be moved automatically across environments in response to regulatory or geopolitical changes. Red Hat Enterprise Linux® provides a consistent, security-focused operating foundation for national workloads, simplifying management across diverse locations. Red Hat Ansible® Automation Platform automates cloud operations, ensuring process control, and enforcing compliance at scale.

Cloud sovereignty is not limited to protecting an organization against geopolitical concerns; it includes being protected from state and non-state actor attacks, insulating it from global disruptions, and simplifying the complexity of meeting compliance obligations.

Meeting the range of sovereignty needs

Banks have a range of varied risk appetite and sovereignty needs. Red Hat approaches these different needs with a set of controls that are deployed on the same consistent foundation.

Data and AI sovereignty: Meet strict data regulations on how data is collected, classified, processed, and stored to ensure data regulations are met, including the legal control of AI models and training data.

Red Hat Advanced Cluster Management for Kubernetes and Red Hat Advanced Cluster Security support geo-fencing policies for data localization and granular tracking of workload locations. Banks can integrate External Key Management (EKM) to ensure encryption keys for sensitive customer data are stored and controlled by the bank itself or a trusted third party separate from the cloud provider.

Operational sovereignty: A focus on business continuity to make sure the people operating and supporting critical infrastructure are subject to the domestic jurisdiction (fulfilling DORA requirements).

Red Hat Confirmed Sovereign Support (e.g., for the EU): Dedicated technical support provided exclusively by staff who are citizens of the specific region, ensuring that operational control, monitoring, and privileged access are strictly localized and comply with regional staffing mandates.

A blueprint for cloud sovereignty

Not every sovereign cloud is identical. However, they are typically based on common patterns. Red Hat provides an opinionated reference architecture for building a sovereign cloud that offers a suite of Infrastructure-as-a-Service (IaaS), Platform-as-a-Service (PaaS), and artificial intelligence-as-a-Service (AIaaS) capabilities.

This architecture ensures consistency, control, and focused security measures across environments.

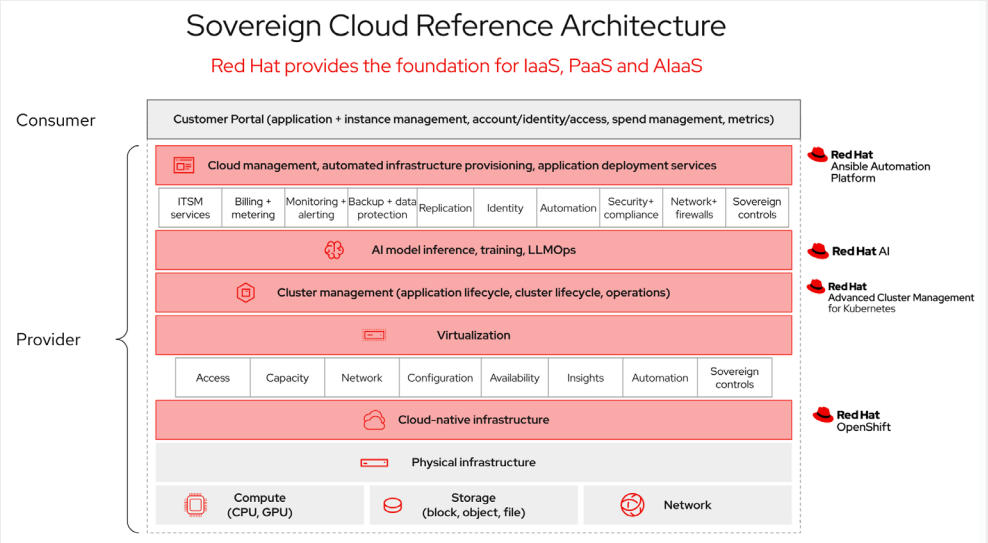

Figure 1: The reference architecture for sovereign cloud

The architecture is built on a layered model with Red Hat core products providing specific functions:

- The foundation is a layer of cloud-native infrastructure built on Red Hat OpenShift. As a prominent enterprise Kubernetes platform, Red Hat OpenShift provides a consistent, reliable, and scalable foundation for running both modern and traditional applications across physical, virtual, private, or public infrastructure.

- To deliver on the promise of sovereign AIaaS, integrate Red Hat AI. This component provides a comprehensive toolkit for data scientists and developers to build, train, and deploy AI models and applications directly on the platform. By providing a consistent environment for the entire AI/ML lifecycle, Red Hat AI makes certain that organizations can develop their own sovereign intelligence, keeping sensitive models and training data within their control and aligned with local governance.
- The management and automation layer sits at this level. Ansible Automation Platform is used for automated infrastructure provisioning, configuration management, and application deployment, ensuring that processes are repeatable and codified. For multicluster environments, Red Hat Advanced Cluster Management provides centralized cluster lifecycle management, application deployment and, crucially, policy-based governance to enforce security and compliance settings consistently across the estate.

This architecture explicitly supports running both virtual machines (VMs) and containers on a single, unified platform. This capability is critical for workload portability, allowing organizations to modernize at their own pace and avoid being locked into a single virtualization or containerization technology.

The ecosystem approach

Partners play a vital role in helping Red Hat meet the market's sovereignty needs. These ecosystem partners provide essential capabilities such as, in-country datacenters, compliance expertise, and staffing. Collaboration allows banks to use global innovation while meeting specific national mandates.

Red Hat technology is a trusted, portable middle layer, giving banks and their services the control, flexibility, and transparency needed to comply with sovereignty requirements, avoid vendor lock-in, and deploy advanced AI services with trustworthiness.

The era of strategic cloud autonomy

Cloud computing has delivered immense speed and efficiency, but at a hidden cost: the systemic surrender of control over critical operational capabilities and sensitive customer data. The increasing requirements of intensifying regulations, the accelerating friction from geopolitical parties, and the demands for operational resilience have fundamentally changed the risk calculus of many banks, and the financial market infrastructure that supports them. Cloud sovereignty is the resulting, necessary architectural paradigm shift.

Cloud sovereignty goes far beyond simple data residency. It brings new capabilities encompassing data, operations, and technology, and it is this confidence that helps organizations to:

- **Increase survivability.** Sovereignty is the strongest defense against the dual threat of expensive regulatory fines and the forced surrender of data fewer than foreign extraterritorial laws. It provides shareholders and regulators with confidence that the bank's core operations are insulated from escalating global instability.
- **Increase transparency.** In financial services, trust is an ultimate asset. By demonstrating control over data and adhering strictly to national mandates, firms can avoid sanctions from regulators and increase the trust relationship with their clients. Transparency is crucial, especially as global concerns over data privacy proliferate.

- **Protect AI.** The next wave of AI is important to the future of financial services, but it also brings with it a new set of risks. A sovereign cloud provides the auditable and compliant foundation with trustworthiness required for artificial intelligence.

Get started

The 1st step toward building your sovereign strategy is straightforward. Discover more about how Red Hat supports the provisions of sovereignty in the banking industry.

- **Engage with our experts:** Contact Red Hat to schedule a discussion about your organization's sovereignty challenges and goals. The Red Hat Account Executive team can help map a journey to digital autonomy.
- **Explore Red Hat's partner ecosystem:** Connect with an extensive network of domestic and regional cloud service providers. These trusted companies offer a range of sovereign cloud solutions and collaborative services built on Red Hat open hybrid cloud technologies.
- **Review our technical resources:** Visit our architecture center to access in-depth resources, reference architectures, and whitepapers on building and managing sovereign cloud environments with Red Hat's product portfolio.

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
#3358916_0126