

OPEN
MAINFRAME
PROJECT

Modernization Working Group

Sovereign Mainframe

Executive summary

As global regulations like the EU's Digital Operational Resilience Act (DORA) tighten, balancing cloud innovation with digital sovereignty and operational independence is a critical C-suite imperative. Digital sovereignty is not an all-or-nothing choice between mainframe and cloud. Rather, it requires retaining control over mission-critical data and infrastructure. When integrated into a sovereign hybrid architecture, on-premises mainframes provide an indispensable component for mitigating third-party concentration risks, ensuring strict data residency, and guaranteeing continuous operational resilience.

Introduction

Recent technological trends, including the growing use of big data analytics, the Internet of Things (IoT), artificial intelligence (AI), and cloud computing, have transformed enterprise architectures. However, mainframes continue to remain the cornerstone of mission-critical systems. Per the Arcati Mainframe Navigator 2026, 36% of surveyed organizations generate over half of their business revenue via mainframe applications, with 21% reporting that over 75% depends directly on IBM Z [1].

While multi-cloud strategies offer elasticity, over-reliance on public cloud introduces significant jurisdictional and operational risks. Navigating this requires evaluating enterprise platforms through two complementary lenses:

- **Digital Sovereignty**: The capacity to maintain legal, technical, and operational control over digital assets (hardware, software, algorithms, data) within local legal jurisdictions [2]. However, achieving this control becomes increasingly challenging when critical digital infrastructure depends heavily on foreign technology providers. For instance, US-based hyperscalers dominate over 70% of the European cloud market [3]. This structural imbalance creates significant provider concentration risk, where a single provider outage or geopolitical dispute could disrupt entire economic sectors.
- **Operational Resilience:** The ability of an organization to anticipate, absorb, adapt to, and rapidly recover from digital disruptions [4]. Regulators worldwide have shifted resilience from a best practice to a legal obligation through mandates like DORA and NIS2 (EU) [5], the Critical Third Parties framework (UK), and OCC/Fed guidance (US).

Figure 1 provides a macro view of regulatory initiatives governing sovereignty requirements, data localization, domestic platform adoption, and resilience mandates across global jurisdictions, underscoring that this is a shared international priority.

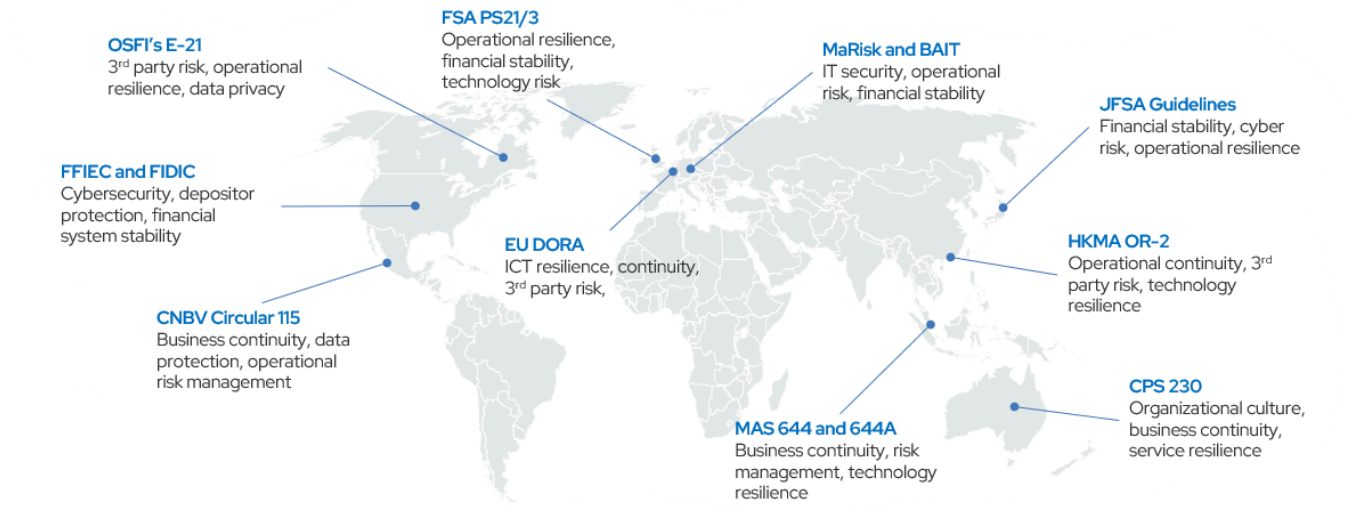


Fig 1. Global regulations on Digital Sovereignty and Data Localization [6]

By pairing native Reliability, Availability, and Serviceability (RAS) with open-hybrid integration, mainframes serve as proactive enforcement anchors for both digital sovereignty and regulatory compliance.

Dimensions of Sovereignty & Resilience

Evaluating enterprise architecture through the lens of Sovereignty and Resilience requires analyzing how on-premises mainframes and public cloud environments support them.

SOVEREIGN HYBRID ENTERPRISE	
ON-PREM MAINFRAME (System of Record & Critical)	PUBLIC CLOUD (Elastic & Global)
• On-premises Data Residency • Pervasive & Quantum-safe Encryption • Zero Third-Party Cloud Risk • Built-In Hardware Redundancy	• Rapid Horizontal Elasticity • Easy consumption through APIs • Distributed Geographic Replication • Redundancy through Cloud-Native patterns

Table 1. Comparison of the Mainframe and the Cloud forces

3.1 Data Sovereignty

Data sovereignty requires that sensitive data remain under the control of the jurisdiction in which it is subject to applicable laws and regulations. Mainframes support this objective by allowing organizations to maintain core systems of record on-premises, behind organizational firewalls, while protecting sensitive data through pervasive encryption and quantum-safe cryptographic capabilities [7]. Beyond data protection, the latest IBM z17 mainframe version can support data sovereignty through localized AI processing, reducing the need to transfer it to third-party cloud platforms for inference and processing purposes [8].

For organizations permitted to use external environments, hyperscalers offer dedicated sovereign cloud regions [11]. However, data residency alone does not guarantee data sovereignty. Even when co-locating mainframe capacity in third-party data centers, extraterritorial laws like the US CLOUD Act [9] may allow foreign authorities to compel disclosure [10]. True data sovereignty therefore requires evaluating both physical residency and ultimate legal jurisdiction.

3.2 Operational Sovereignty & Concentration Risk

Operational sovereignty ensures service survivability even if an external vendor ceases support or suffers an outage. On-premises mainframes provide operational independence from foreign cloud provider outages, geopolitical conflicts, or administrative overreach. While sovereign public clouds aim to mitigate these risks, they still rely on shared responsibility frameworks and third-party infrastructure [14]. While sovereign public clouds offer sufficient autonomy for many workloads, for critical core operations they often leave an unacceptably high residual risk. In such cases, by maintaining critical transaction processing on-premises, enterprises avoid exceeding DORA's threshold for critical third-party service provider (CTP) dependence on public cloud hyperscalers.

3.3 Technical Sovereignty & Architectural Openness

Technical sovereignty requires the ability to evolve, modify, and replace systems without being hindered by vendor lock-in. Neither mainframes nor public clouds are inherently technically sovereign. Legacy mainframe applications can complicate modernization [12, 15], and because IBM Z hardware is engineered by a US-headquartered vendor, organizations face potential hardware supply-chain and export-control dependencies. Conversely, heavy reliance on proprietary hyperscaler services creates acute vendor lock-in and heightened exposure to abrupt service suspension or cross-border access restrictions. Organizations must therefore adopt two complementary approaches to minimize lock-in risks:

- **Mainframe Modernization:** Historical mainframe lock-in is increasingly overcome via open standards. Linux on IBM Z [16], z/OS Container Extensions (zCX) [17], and

open-source frameworks like Zowe enable enterprises to run Docker containers and modern cloud-native tools directly on mainframe hardware.

- **Hybrid Abstraction:** API abstraction layers shield enterprises from both mainframe and hyperscaler lock-in simultaneously. By decoupling modern applications from underlying databases, APIs allow cloud applications to interact with mainframe capabilities without demanding the immediate replacement of legacy systems.

3.4 Operational Resilience in Practice

When looking at the four core pillars of operational resilience for mainframes, we get:

1. **Prevention:** Mainframes integrate hardware-level redundancy, such as Redundant Array of Independent Memory (RAIM) and hot-swappable components, eliminating single points of failure[19]. The recent IBM Z systems meet NEBS Zone 4 seismic standards, providing resilience against severe physical shocks such as earthquakes [18]. Additionally, IBM Z's **Safeguarded Copy** / Cyber Vault capability provides immutable, isolated, logical air-gapped snapshots that prevent ransomware corruption from replicating to backup storage.
2. **Detection:** z/OS provides extensive built-in observability through System Management Facilities (SMF) and Resource Measurement Facility (RMF), which collect system events and performance metrics. These capabilities support continuous monitoring, while AI-driven anomaly detection can help identify emerging performance bottlenecks before they cause downtime. According to the Arcati Mainframe Navigator 2026, anomaly detection is the most frequently reported AI use case on the mainframe [1].
3. **Adaptation**: Servers can scale vertically on demand through On/Off Capacity on Demand, or horizontally across up to 32 nodes using Parallel Sysplex [20]. However, some legacy mainframe applications have architectural constraints, such as hard-coded parameters and memory restrictions, or may not be configured to operate across multiple LPARs [12].
4. **Recovery:** Mainframes have recoverability built into the OS, with a rich set of error recovery and serviceability features. Near-zero recovery metrics (Recovery Time Objective/Recovery Point Objective) are achieved through HyperSwap and Geographically Dispersed Parallel Sysplex (GDPS) [22]. However, the retirement of experienced mainframe SMEs creates an operational risk, particularly for organizations that rely on specialized skills to maintain and recover critical systems [12]. This aligns with DORA's emphasis on managing operational and third-party dependencies.

In contrast, public cloud architectures distribute these four resilience pillars across decentralized, software-defined environments:

1. **Prevention:** Cloud platforms achieve resilience through geographic distribution, replicating data and workloads across multiple regions to absorb localized failures. For cyber resilience, cloud-native services can approximate capabilities like IBM Z's Safeguarded Copy. However, this requires complex coordination across backups,

isolated account structures, and key management to prevent primary account compromises from propagating into backup storage.

2. **Detection:** Cloud platforms deliver resilience through distributed observability, aggregating telemetry, logs, and traces across decentralized components rather than relying on a single, unified hardware footprint.
3. **Adaptation:** Cloud environments excel at dynamic horizontal elasticity, allowing organizations to scale compute resources dynamically with virtually no physical ceiling [20].
4. **Recovery:** Cloud recovery relies on automated failover and multi-region routing. However, applications must be explicitly re-architected to leverage these primitives and keep Recovery Time Objectives (RTOs) low [12].

Strategic Options for Sovereignty

A sovereign hybrid architecture eliminates the binary choice between on-premises mainframes and public cloud environments. By strategically placing workloads based on data sensitivity, latency, regulatory mandates, and business value, organizations are able to achieve operational agility without sacrificing legal control.

The following table summarizes three strategic approaches to balancing sovereignty and resilience:

Strategic option	Approach / what it means	Primary Sovereignty & Resilience Benefit	Key Considerations
Mainframe and Private Cloud first, extending to public for non-critical workloads	Keep critical systems and sensitive data on the mainframe and/or private cloud, while using public cloud for non-sensitive, high-scale, or elastic workloads such as analytics, AI, and APIs applications.	Maximum control over critical data and workloads while still benefiting from public-cloud scalability. Limits exposure of sensitive workloads to external cloud providers and reduces dependence on public infrastructure for essential operations.	Requires good understanding of workload and data classification before cloud ingestion. Maintaining mainframe, private cloud, and public cloud environments can increase operational and integration complexity.

Full hybrid (Mainframe/Private Cloud and Public Cloud host critical workloads)	Distribute critical workloads across the mainframe/private cloud and public cloud, using APIs, replication, or tightly integrated hybrid architectures to allow workloads and data to operate across environments.	Greater flexibility and resilience through workload distribution. Critical services can potentially continue operating if one environment becomes unavailable, while organizations can use cloud elasticity and specialized capabilities.	Latency and Synchronization increase complexity and can become an issue for highly interactive workloads [12]. Critical data and workloads may become subject to security concerns, external provider dependencies and jurisdictional constraints.
Multi-cloud (different public cloud / sovereign cloud providers)	Use multiple cloud providers, potentially combining public hyperscalers with sovereign/regional cloud providers, to distribute workloads and avoid reliance on a single provider [21].	Reduces provider concentration and lock-in, while sovereign clouds can provide greater control over regulated data. Multiple providers can also provide additional redundancy and reduce dependence on a single infrastructure provider.	Increases architectural and operational complexity, while data portability, interoperability, synchronization, and security must be carefully managed. Cross-provider data transfers may also incur significant egress costs [13].

Table 2. Strategic options for Sovereignty and Resilience

The main point to keep in mind is that there is no right strategy, only trade-offs. The industry domain, local regulatory regime and even organizational risk appetite will make one of the strategies a better fit than the others.

Conclusion

Mainframes continue to play a vital role in enabling digital sovereignty and operational resilience as they have in the past. Their ability to deliver total control over critical infrastructure, enforce strict access governance, protect sensitive data on-premises, and guarantee zero-downtime operations makes them uniquely suited for sovereignty-sensitive enterprise environments. However, digital sovereignty does not mean keeping every workload on the mainframe. Rather, organizations should retain workloads on the mainframe where its control, security, availability, and regulatory advantages provide meaningful value, while using private, sovereign, or public cloud environments where they are better suited to the workload's requirements.

To optimize this value within a modern IT strategy, enterprise leaders should consider five key actions:

1. Classify Workloads: Categorize applications and data by sovereignty requirements, regulatory exposure, and business criticality.
2. Anchor Core Systems: Reserve mainframes for mission-critical, high-resilience workloads requiring absolute operational independence.
3. Control Infrastructure: Maintain direct governance over core assets to eliminate third-party concentration and supply-chain risks.
4. Embrace Open Standards: Utilize Linux, containers, and modern open API frameworks to prevent vendor lock-in and enhance technical sovereignty.
5. Deploy Sovereign Hybrid Models: Treat hybrid architecture as a strategic asset, distributing workloads between mainframe stability and cloud elasticity based on workload need.

Rather than competing with cloud platforms, mainframes are the cornerstone of the sovereign hybrid architecture, the modern standard for enterprise computing. Far from obsolete, the IBM Z Mainframe platform continues to evolve through Linux, open-source integration, and containerization. By pairing native mainframe resilience with cloud-native flexibility, organizations achieve long-term digital sovereignty without sacrificing innovation or agility.

References

[1] Planet Mainframe (2026). Arcati Mainframe Navigator 2026.

https://planetmainframe.com/arcati-2026/

[2] Bridson, B. (2026, March 25). What is digital sovereignty and why does it matter? Uncover IE.

https://www.ie.edu/uncover-ie/digital-sovereignty-master-in-public-policy/

[3] Wrede, Insa (2021). Gaia-X cloud: A safe haven for Europe's data?. Deutsche Welle.

https://www.dw.com/en/gaia-x-cloud-a-safe-haven-for-europes-data/a-59724779.

[4] Bigelow, S. J. (2025, August 21). What is digital resilience? Definition, strategy and use cases. Search Data Backup.

https://www.techtarget.com/searchdatabackup/definition/What-is-digital-resilience

[5] EU NIS 2 Directive: Expanded Cybersecurity obligations for key sectors | Insights | Greenberg Traurig LLP. (n.d.).

https://www.gtlaw.com/en/insights/2025/8/eu-nis-2-directive-expanded-cybersecurity-obligations-for-key-sectors.

[6] Resolver Inc. (2025, November 27). Global Operational Resilience Compliance & Regulations | Resolver. Resolver. https://www.resolver.com/blog/global-operational-resilience-compliance/

[7] Mainframe advanced security - IBM Z. (2025, June 23).

https://www.ibm.com/products/z/security

[8] IBM's z17 Mainframe: Data Sovereignty Reinvented. (2025, August 16). StorageTech.

https://storagetech.news/recent-data-breaches/ibms-z17-mainframe-data-sovereignty-reinvented/

[9] Wikipedia contributors. (2026, August 6). CLOUD Act. Wikipedia.

https://en.wikipedia.org/wiki/CLOUD_Act

[10] Anonymous industry expert. (2026). Interview conducted by the author with a senior mainframe strategy leader at a Canadian financial institution, [July 7, 2026].

[11] Research, E. M. (2026, July 20). Top companies in the Sovereign Cloud: leaders, trends, and regional outlook. Econ Market Research. https://www.econmarketresearch.com/blog/top-sovereign-cloud-companies

[12] Joan Reester (2026). Interview conducted by the author with a Mainframe Consultant (previously with IBM and AWS) [August 5, 2026].

[13] Johnson, D. (2026, January 7). Cloud Egress fees: What they are and how to reduce them. Backblaze Blog | Cloud Storage & Cloud Backup. https://www.backblaze.com/blog/cloud-101-data-egress-fees-explained/

[14] What is sovereign cloud? (2026, April 8). Cisco. https://www.cisco.com/site/us/en/learn/topics/computing/what-is-sovereign-cloud.html

[15] Keizer, J. (2024). Mainframe Software Price Increases are Giving IT Leaders Heartache. CPT Global. https://cptglobal.com/resources/cpt-insights/mainframe-software-price-increases-are-giving-it-leaders-heartache

[16] Linux OS on IBM Z Mainframe. (2025, June 23). https://www.ibm.com/products/z/linux

[17] z/OS Container Extensions (zCX) content solution. (2018, July 16). https://www.ibm.com/support/z-content-solutions/container-extensions/

[18] Dickens, S. (2024, April 12). Enhancing infrastructure resilience: IBM Mainframe's Approach - Futurum. Futurum. https://futurumgroup.com/insights/enhancing-critical-infrastructure-resilience-ibm-mainframes-approach/

[19] Ijraset. (n.d.). The RAS Paradigm in Mainframe Systems: A Comprehensive analysis of design principles and operational benefits. IJRASET.

https://www.ijraset.com/research-paper/comprehensive-analysis-of-design-principles-and-operational-benefits

[20] Everyone said the mainframe couldn't scale. then we looked at the data | LinkedIn. (2026, April 13). https://www.linkedin.com/pulse/everyone-said-mainframe-couldnt-scale-we-looked-data-thirumala-4hzlc/

[21] Ahmed, S., & Ahmed, S. (2026, May 17). Cloud 3.0: Hybrid, Multi-Cloud & Sovereign Architecture Guide. The Developer Space. https://thedeveloperspace.com/cloud-3-0-hybrid-multi-cloud-sovereign-architecture/#Part_4_AI_Cloud_30_%E2%80%93_The_Accelerator

[22] Server and cyber resiliency with IBM Z. (2026, September 28). https://www.ibm.com/products/z/resiliency#footnote

About this paper

Our authors

This document was developed under the Open Mainframe Project's Summer 2026 Mentorship program and sponsored by the Mainframe Modernization Working Group.



Junior Tadiffo is a final-year Computer Science student at the University at Buffalo, USA. He is an IBM Z Student Ambassador and the founder of the "UB IBM Z Club."

He has experience in Software Engineering, AI, and Systems, with a strong passion for sports and hardware projects. He is passionate about developing innovative applications and creating solutions for the mainframe.



Swathi is currently working as a Technology Consultant at KPMG, where she works with organizations to build and implement cybersecurity frameworks that are secure, practical and scalable. She is passionate about open source, spanning both its technical and governance aspects. She previously served as the release communications lead of Kubernetes v1.37 and was an LFX Mentee in 2024 under the Open Mainframe Project.

Special thanks

This work would not be possible without the useful suggestions and feedback of members of the Mainframe Modernization Working Group, part of the Open Mainframe Project. Special thanks to **Joan Reester** (previously with IBM and AWS), **Joe Gentile** (IBM), and **Steven Dickens** (HyperFrame Research) for their insightful perspectives on the industry.

About the Modernization Working Group

The Modernization Working Group, part of the Open Mainframe Project, intends to be a focal point for thought leadership around what it means to modernize mainframe applications.
We are an open group passionate about knowledge sharing, leading constructive discussions, challenging status quo, exploring creative solutions, and generating contents that will help the community in their journey.
Learn more about the working group at:
https://openmainframeproject.org/our-projects/working-groups/modernization-working-group/

Appendix I - Operational Resilience Frameworks

The figure below shows the 5 pillars of Operational Resilience Framework and the DORA (the Digital Operational Resilience Act) pillars side by side.

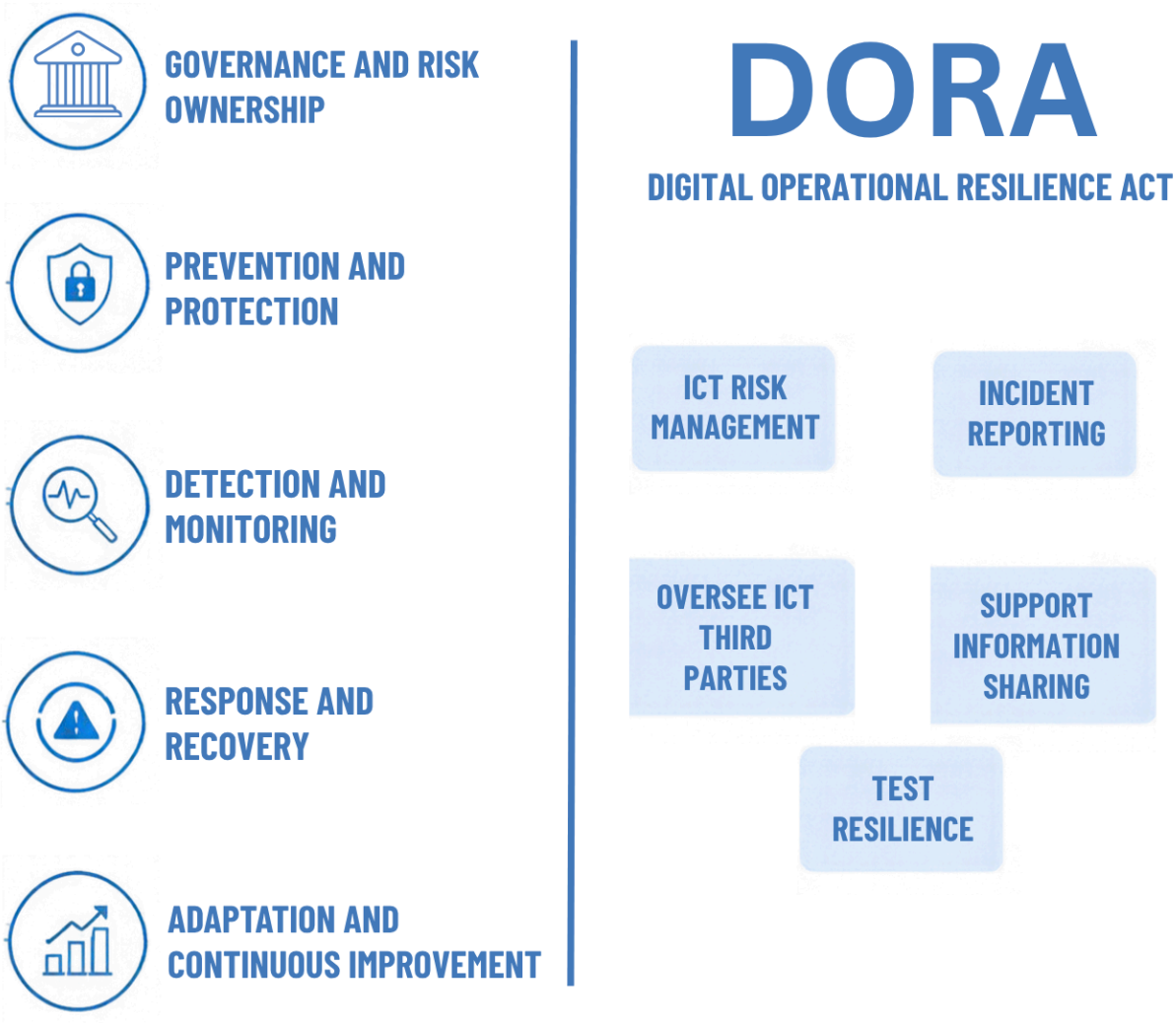


Fig 2. Pillars of Operational Resilience