Re-thinking IT Strategies for Digital Sovereignty

Sovereign Cloud Summit 2022, Barcelona

Rahiel Nasir,
Associate Research Director, European Cloud,
7 November 2022
Agenda

- Sovereignty as an Enterprise Security Concern
- Impact of Recent Economic and Geopolitical Upheavals
- How Organizations Are Reacting
- Planning For Sovereignty
- Challenges and Pitfalls
- Future Sovereignty
- Advice For Sovereign Solution Customers & Providers
- Recommendations
- Further information
What are your organization’s biggest security, compliance or trust challenges when it comes to cloud?

- Cloud security skills: 32%
- Visibility, security, and recovery of data: 29%
- Identity and access management: 27%
- Cloud governance and regulatory compliance: 24%
- Managing encryption keys across multiple cloud environments: 24%
- Data sovereignty concerns (e.g., Schrems II, US CLOUD Act): 23%
- Application and API security and DevOps: 21%
- Lack of clarity on who has responsibility for security (shared responsibility model): 20%
- Security-by-design enforcement: 20%
- Multi-tenancy of cloud: 16%
- Misconfiguration of cloud services: 16%

Source: IDC’s European Multicloud Survey, 2022 (N=1077)
Who cares about digital sovereignty in Europe?

When asked what top attributes they considered when choosing a partner for a cloud project, 21% of European organizations look for digital sovereignty capabilities.

Who are the 21%?
Most of these organizations are in the Czech Republic, Spain and Portugal, and from the following sectors:

- Czech Republic: 31%
- Spain: 29%
- Portugal: 26%
- Germany: 25%
- France: 24%
- Benelux: 21%
- Austria: 20%
- Nordics: 20%
- Italy: 19%
- Switzerland: 18%
- Poland: 16%
- Hungary: 15%
- UK: 11%

Source: IDC’s European Multicloud Survey, 2022 (N=1077)
Which of the following best reflects your organization’s view of the importance of digital sovereignty as a business and technology concern due to recent economic and geopolitical events?

**Much more important** – we are changing our business and IT strategy as a result of current events

**Somewhat more important** – we are adjusting our day-to-day operations as needed, but not making major changes

**Neither more nor less important** – we have no plans to change our operations at the moment, but are following the news

**Not at all important** – we do not think the current situation will change our way of running business and using technology

Due to your increased digital sovereignty concerns, which of the following actions is your business and IT leadership prioritizing?

- Improve integrated risk management process to include geographic parameters
- Improve privacy measures and implementation
- Improve supply chain management and transparency
- Improve organizational and regulatory compliance
- Adopt or enhance geopolitical resiliency plans
- Work with our ICT suppliers more closely to mitigate third party risk
- Review current SLAs and force majeure clauses in IT contracts
- Put in place software escrow agreements

### Deploying Digital Sovereignty

<table>
<thead>
<tr>
<th>IS DIGITAL SOVEREIGNTY A STRATEGIC PRIORITY?</th>
<th>REVIEW</th>
<th>CLASSIFY</th>
<th>APPLY SOVEREIGNTY CONTROLS TO THOSE DATA &amp; APPS (&amp; AS PER REGULATIONS)</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>YES</strong></td>
<td>YOUR SECURITY &amp; COMPLIANCE PROCESSES, TOOLS &amp; SKILLS</td>
<td>YOUR DATA &amp; APPS BY SOVEREIGNTY REQUIREMENTS &amp; WORKLOADS</td>
<td>ered to those data &amp; apps (&amp; as per regulations)</td>
</tr>
<tr>
<td><strong>NO</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>IS IT A REGULATORY REQUIREMENT?</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>IF YES, MOVE BACK TO GO</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>NO</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>IS IT VITAL FOR YOUR PARTNER ECOSYSTEM?</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>IF YES, MOVE BACK TO GO</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>NO</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>IS IT IMPORTANT TO YOUR CUSTOMERS?</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>IF YES, MOVE BACK TO GO</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

#### HIGHEST PRIORITY

80% of European organizations consider digital sovereignty to be their highest priority over the coming years, ranking alongside diversity & inclusion.

IDC’s Worldwide CEO Survey, Dec 2021 (n=103 European respondents)
Challenges and Concerns:

What are your organization's main challenges regarding data sovereignty needs?

- **Regulations (Schrems II, Privacy Law, EDPB Ruling)**: 45%
- **Mitigation of risks related to extra territorial legislation (e.g., CLOUD Act)**: 37%
- **Data residency**: 34%
- **Data classification**: 33%
- **Existing vendor lock-in**: 31%
- **Increased costs**: 30%
- **Proprietary environments**: 28%
- **Lack of data mobility/portability**: 27%
- **Data mobility**: 25%

Source: IDC Sovereign Cloud, VMware, September 2022 (N=600)
Challenges and Concerns:

Which of the following are your organization’s main concerns regarding implementing a sovereign cloud strategy?

- High complexity: 49%
- High implementation costs: 48%
- Limited choice of sovereign cloud partner: 41%
- Lack of skills to integrate with existing hybrid and multicloud environments: 39%
- Lack of management buy-in: 36%
- Limited or lack of required cloud features: 35%
- Push back over fears of reduced speed of innovation: 34%
- Lack of knowhow: 31%
What do you think are the main skills required to manage a sovereign cloud?

<table>
<thead>
<tr>
<th>Skill</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ensure and prove regulatory compliance</td>
<td>42%</td>
</tr>
<tr>
<td>Better visibility into current infrastructure, applications, and data environments</td>
<td>41%</td>
</tr>
<tr>
<td>Assess and define the scope of sovereign cloud strategy to win additional budgets</td>
<td>41%</td>
</tr>
<tr>
<td>Migrate and modernize on trusted cloud foundation</td>
<td>41%</td>
</tr>
<tr>
<td>Identify the full set of data and workloads that will be subject to sovereign requirements</td>
<td>40%</td>
</tr>
<tr>
<td>Develop new applications and digital services adhering to sovereign cloud standards</td>
<td>38%</td>
</tr>
<tr>
<td>Operate and govern cloud operations</td>
<td>38%</td>
</tr>
<tr>
<td>Data classification capability</td>
<td>37%</td>
</tr>
</tbody>
</table>

Source: IDC Sovereign Cloud, VMware, September 2022 (N=600)
How will your organization’s technology investment and partnership priorities related to digital sovereignty affect the use of different types of cloud partners in the following areas?

All industry sectors

- We will move more workloads to global cloud providers
- We will move more workloads to local cloud providers
- We will move more workloads from cloud providers to our own datacenters
- We will not change our current distribution of workloads

You indicated that your organization plans to shift some workloads based on its digital sovereignty priorities. Which of the following workloads will be most affected?

Building digital sovereignty

Digital sovereignty encompasses several layers of sovereignty, shifting gear and emphasis from **self-determination** to **self-sufficiency** to **survivability**.

- **GEOPOLITICAL**
  - Military; economic; trade dependence

- **SUPPLY CHAIN**
  - Chip manufacture; skills; raw materials; energy

- **ASSURANCE**
  - Assured workloads; business continuity & disaster recovery; redundancy; portability

- **OPERATIONAL**
  - Controls & stability; authorized key access for customer, admin & support

- **TECHNICAL**
  - Protectionism; interoperability; portability

- **DATA**
  - Regulation; portability; data transfers
Advice for sovereign solution customers and providers

<table>
<thead>
<tr>
<th>CUSTOMERS</th>
<th>PROVIDERS</th>
</tr>
</thead>
<tbody>
<tr>
<td>▪ Data discovery is foundational to any data governance, privacy, and</td>
<td>▪ Be prepared for greater customer and auditor scrutiny</td>
</tr>
<tr>
<td>security program</td>
<td>▪ Market education remains vital</td>
</tr>
<tr>
<td>▪ Look for cloud solutions that ensure protection against cyber-attacks</td>
<td>▪ If you want to be the go-to provider of sovereign solutions:</td>
</tr>
<tr>
<td>▪ Be prepared for complexities and extra costs</td>
<td>• Demonstrate key capabilities</td>
</tr>
<tr>
<td>▪ Using local cloud solutions can offer advantages. However…</td>
<td>• Offer a broad level of expertise and skill sets</td>
</tr>
<tr>
<td>▪ Use the jurisdiction that has the toughest regulations and laws as a</td>
<td>• Engage all lines of business and stakeholder departments</td>
</tr>
<tr>
<td>benchmark</td>
<td>▪ Maintain security and compliance on an ongoing basis, and as a shared</td>
</tr>
<tr>
<td>▪ Always watch out for new and upcoming legislation</td>
<td>responsibility</td>
</tr>
<tr>
<td>▪ Seek out partners and solutions that offer the greatest adaptability -</td>
<td></td>
</tr>
<tr>
<td>and avoid lock-in</td>
<td></td>
</tr>
</tbody>
</table>
# Recommendations

## CUSTOMERS

- Cloud sovereignty still in its early evolutionary stages
- Organizations should ultimately be guided by business outcomes
- Implementing sovereignty principles is a long-term process
- Risks of over-optimizing for local needs

## PROVIDERS

- Vendors should consider a number of baseline controls
- Data encryption as a minimum
- Handing customers their encryption keys
- Granular user access controls
- Digital sovereignty is all about helping organizations become more resilient
- Sovereignty success is based on working within an ecosystem
- An “ideal” sovereign cloud versus a “practical” sovereign cloud
Learn more

**Digital Sovereignty: Rethinking IT Strategies and Operations for Self-Determination**
Sep 2022 (#EUR149591322)

**Oracle Plants Big Sovereignty Flag in EU with Launch of Oracle Sovereign Cloud**
Jul 2022 (#lcEUR149505922)

**Sovereign Clouds and the Digital Sovereignty Imperative: Europe's Quest for Digital Independence**
May 2022 (#EUR149098122)

**EU Chips Act: The EU Strategy to Level the Semiconductor Playing Field and Safeguard its Digital Sovereignty**
May 2022 (IDC #EUR149008122)

**VMware on the Right Track as it Expands the Sovereign Cloud Initiative**
May 2022 (#lcEUR149094722)

**How the Russia-Ukraine War Is Impacting the European Cloud Market and Changing the Digital Sovereignty Paradigm**
Apr 2022 (#EUR249014922)

**Atos Aims to Protect Europe's Data with OneCloud Sovereign Shield** – Nov 2021 (#lcEUR148410021)

**OVHcloud: Putting the Final Pieces in Place for Europe's Digital Fortress?** – Nov 2021 (#lcEUR148397721)