Open Source and Digital Sovereignty: Two Sides of the Same Coin

How Open-Source Software Will Empower the Public Sector to Self-Determine their path to Digital Transformation

The public sector is betting the farm on digital transformation to deliver on the promises of competitive net-zero economies and places, high-performing public administrations, and people inclusion and well-being.

Successful public sector leaders aim to realize the benefits of technology innovation to:

- Deliver empathic customer experiences that make bureaucracy invisible
- Enable intelligent automation and collaboration that make civil servants productive
- Foster trusted data sharing to make evidence-based policy and operational decisions

IDC defines digital sovereignty as

THE CAPACITY FOR DIGITAL SELF-DETERMINATION BY NATIONS, COMPANIES, OR INDIVIDUALS

Public sector leaders want to achieve these strategic digital transformation goals, while protecting digital sovereignty. For instance, through its "Cloud at the center" doctrine, the French government "... encourages all public actors to seize its (of the cloud) potential in order to develop a new generation of high-quality digital services, while protecting the data of businesses and citizens".

Digital sovereignty can enable governments to choose how they deploy and manage infrastructure, data and software that they rely upon to realize the benefits of digital transformation. In essence, digital sovereignty is more than just data localization. It also includes cloud platforms, workload software, datacenter assets, and communications infrastructure. More importantly, it entails processes and operations used to control and manage infrastructure and digital services.

Digital sovereignty is about the entire digital architecture and ecosystem that underpins a digital-first Europe where senior public sector leaders have genuine choice.

European public sector leaders are leading the way in embracing digital sovereignty. 28% of those polled expect that Digital Sovereignty principles and policies will be a key element of executing digital trust and resilience programs. The percentage of public sector leaders that prioritize digital sovereignty is even higher in France, Germany and the U.K.

European governments that will invest significantly in these three areas - over the next two years - to ensure long-term resilience

57%
Digital trust programs (to safeguard people, information, systems, and technology)

57%
Operational resilience programs (e.g., automating processes)

47%
IT architecture resilience (e.g., cloud migration, interoperability)

To execute Digital Trust programs **28%** will invest in **"Digital sovereignty principles and guidelines"**

Source: IDC Europe, Government Insights Survey, August 2022 – N = 230

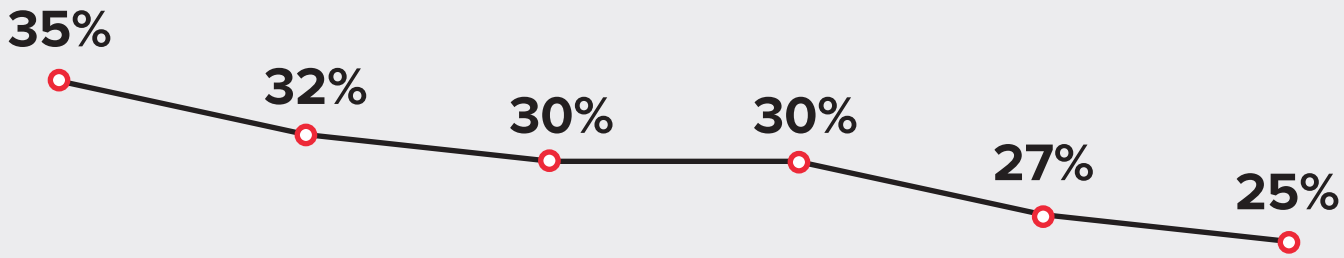
The key attributes of digital sovereignty for the European public sector

European public sector executives are not only ahead of the game in the digital sovereignty journey, compared with other industries and regions, they are also more demanding of specific elements of digital sovereignty, because they understand that digital sovereignty is underpinning trusted digital services and usage of data. For them, the most critical elements of digital sovereignty can be clustered into six key goals that public sector leaders are aiming to self-determine:

- Compliant and trusted **data** collection, governance and processing capabilities that can scale data sharing, while addressing legitimate concerns related to privacy and security in cross-border data flows
- **Technical** architectures that enable digital development teams to seamlessly integrate digital services end-to-end, incrementally migrate from legacy in an agile and affordable manner, and freely reverse their choices when appropriate.
- Granular, easy-to-use, and certified **operational** controls and processes, to automate provisioning, performance management and monitoring of physical and digital access to the infrastructure.
- **Assurance** against cyber incidents and attacks that could negatively impact the continuity of critical services.
- A level playing field for the local ICT **supply chain** to empower local companies to nurture talent and become world-leading innovators.
- Bolstering resilience with better processes to identify vulnerabilities and high-risk dependencies in an increasingly volatile **geopolitical** environment.

European governments want the full breadth of genuine choices across these six elements. They want digital sovereignty to empower them to achieve digital transformation outcomes; for some use cases they will have to comply with strict rules for data localization and certification of operational personnel for reasons of national security, while for other use cases they will want to be able to promote better societal outcomes through data spaces that span across borders, while still self-determining technical and operational capabilities.

Key goals that European governments are pursuing regarding digital sovereignty



Operational sovereignty — to control operations, from provisioning and performance management to monitoring physical access to infrastructure

Assurance — to ensure protection against cyberattacks and black swan events

Supply chain resilience — to enable SMBs to harness the value of cloud as a foundation to develop their own product and service innovation and nurture local talent

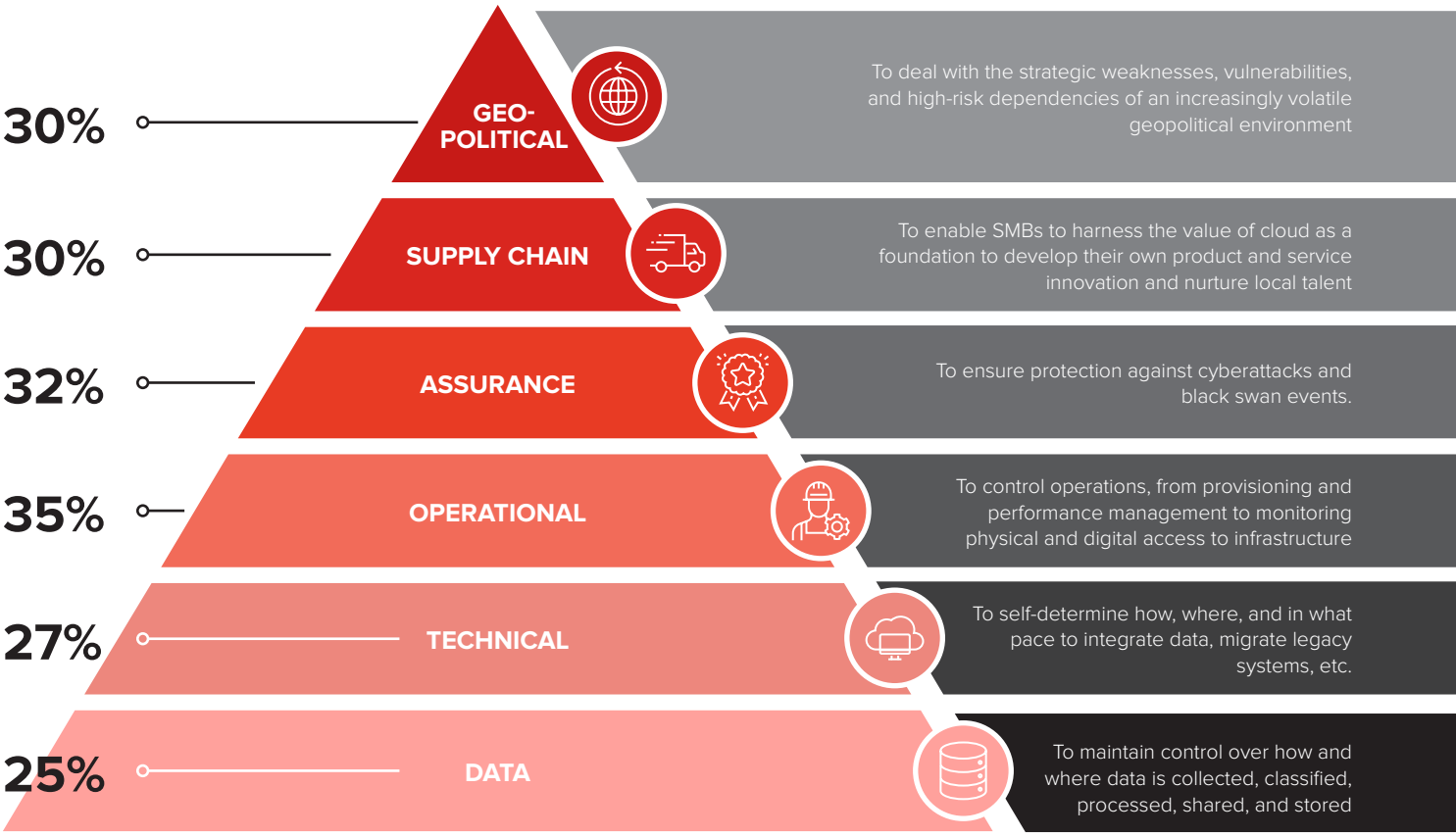
Geopolitical survivability — to deal with the strategic weaknesses, vulnerabilities, and high-risk dependencies of an increasingly volatile geopolitical environment

Data sovereignty — to maintain control over how and where data is collected, classified, processed, shared, and stored

Technical sovereignty — to self-determine how, where, and at what pace to integrate data, migrate legacy systems, etc.

Source: IDC Europe, Government Insights Survey, August 2022 – N = 63

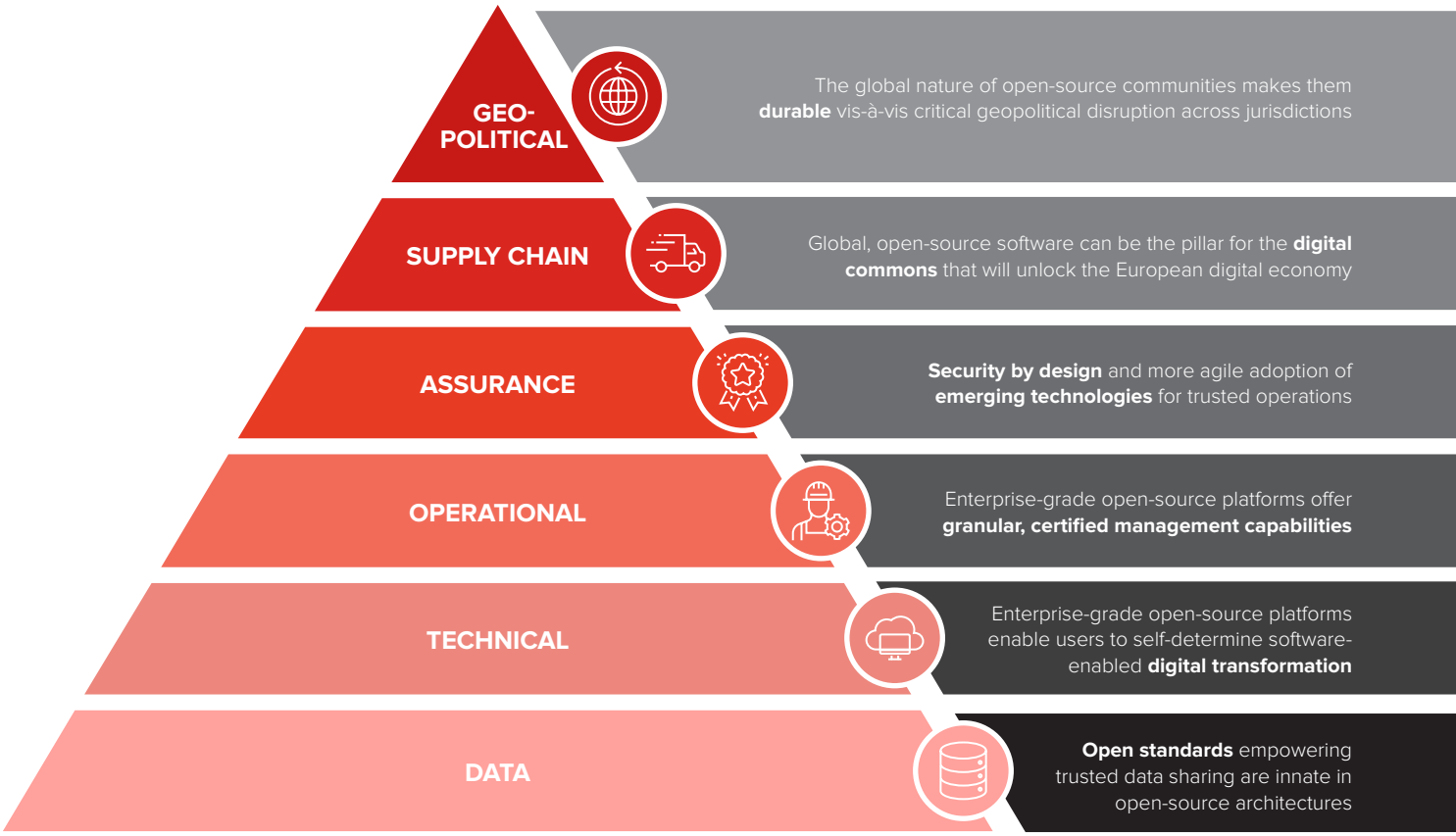
Six goals that European governments are pursuing regarding digital sovereignty



The value of open-source as an accelerator of digital sovereignty

European governments have invested in open source software (OSS means that the users can view the code that comprises the software and make any kind of changes to it they want and that anyone can take the source code and distribute their own program from it for many years) across many layers of the stack, from applications, to platforms, to data management and infrastructure software. Public sector executives that embrace open-source software should understand how they can accelerate their path to digital sovereignty through open source:

- **Open standards are innate in open-source architectures**, thus enabling public sector mission and data experts to share data across the public sector, with citizens and enterprises in a trusted manner.
- Enterprise grade **open-source platforms enable users and contributors to maintain full control** on the development, evolution and reversibility of cloud-native applications.
- Enterprise grade **open-source platforms offer granular, certified operational capabilities** that help to automate the deployment, orchestration, and management of heterogeneous environments.
- Enterprise **open source has a culture of** (and associated processes for) **security by design** and share responsibility that ensure resilient services, even for the more complex hybrid clouds. Also, openness empowers government IT executives to adopt in a more agile manner emerging technologies, such as secure hardware architectures, probabilistic computing, and fully homomorphic encryption, that in the near future will allow trusted operations even on non-trusted systems.
- **Open-source software can be the pillar** for the digital commons that will unlock the European **digital economy**.
- The **global nature of open-source** communities makes them resilient to geopolitical disruption across jurisdictions.



Message from Sponsor

Open Source is key to digital autonomy by the very nature of its open, collaborative development model, and guided by clear and trusted governance processes, open source is driving innovation and developing vital skills for European competitiveness, resilience and control, now and in the future.

For almost the last three decades Red Hat has been collaborating on community projects and protecting open source licenses so that we can continue to develop software that pushes the limits of technological capabilities, and create more reliable, stable, and innovative technologies.

Red Hat