IDC

September 2023 | InfoBrief, sponsored by:

Red Hat | accenture

Cloud Sovereignty in the Banking Sector

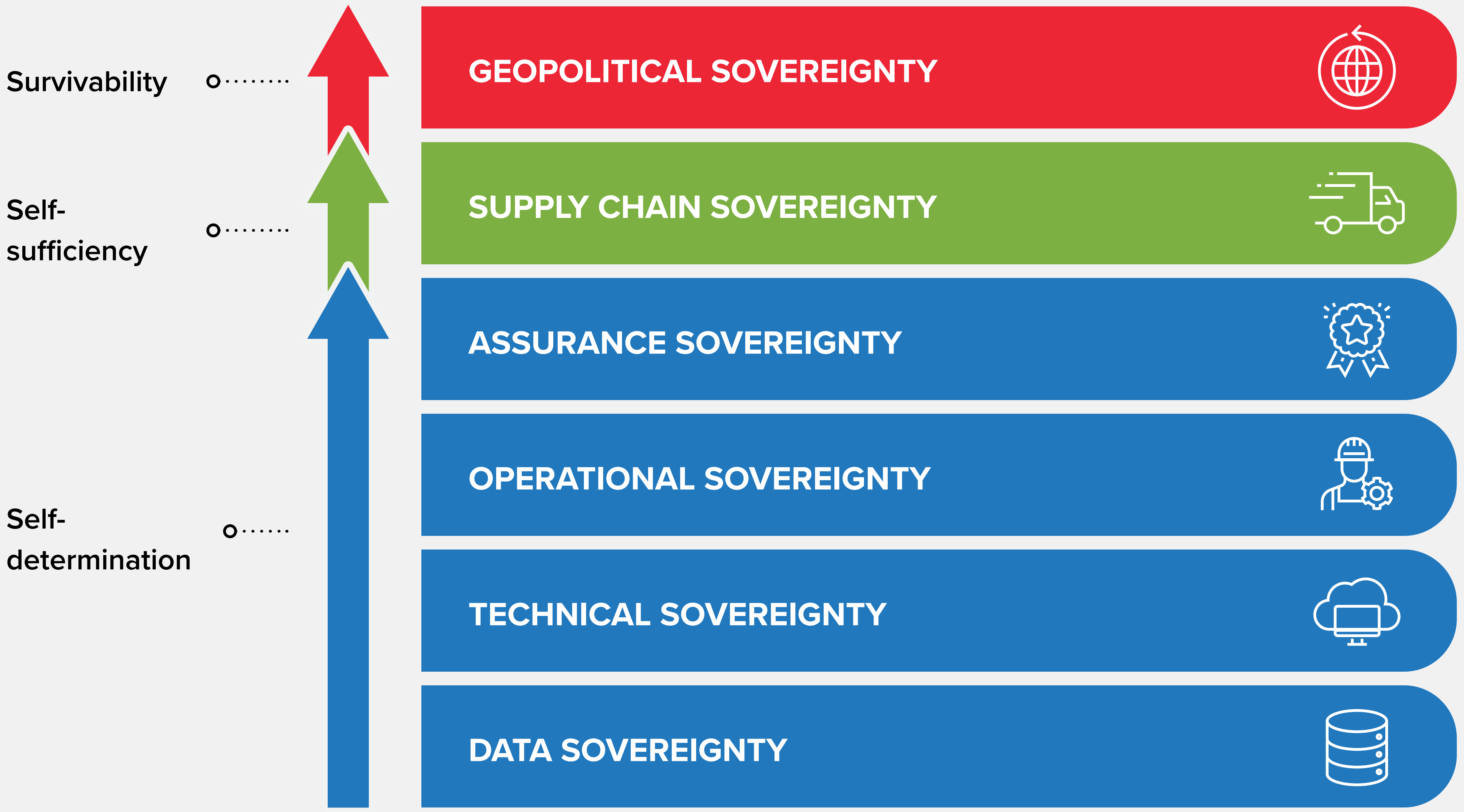
Rahiel Nasir,
Associate Research
Director, European Cloud

Maria Adele Di Comite,
Research Director, Financial Insights,
Corporate and Retail Banking

Executive summary

- **Greater business resilience** is an aspect of digital sovereignty. The EU's Digital Operational Resilience Act (DORA), which applies to financial institutions, suggests a greater need for organisations in this sector to seek solutions for digital sovereignty.
- **IDC defines digital sovereignty** as "the capacity for digital self-determination by nations, companies or individuals". Data sovereignty and cloud sovereignty are subsets of digital sovereignty.
- **Digital legislation**, the need to comply with regulations and increasing cloud adoption are driving demand for sovereign solutions.
- **Complexity is the number 1 challenge** for those looking to deploy sovereign solutions. Costs are also a concern as sovereignty is likely to mean increased investments in IT platforms and services.
- **Other pitfalls to watch out** for include avoiding lock-in and balancing the need for sovereignty so as not to stifle cloud's potential.
- **When seeking sovereign solutions** organisations should look for trusted partners and providers that can help them begin the sovereignty journey which starts with a data review and classification. Sovereignty is not a "fit and forget" process, so organisations should work with partners and providers that are in it for the long haul.
- **Once successfully deployed**, solutions for digital sovereignty can lead to a number of strategic benefits for businesses, such as enhanced trust among customers, governments and stakeholders. This can help open access to new markets.

Defining digital sovereignty



IDC defines digital sovereignty as “the capacity for digital self-determination by nations, companies or individuals”. It is the response to an organisation’s desire for control, choice and autonomy over its data, systems and applications.

Ongoing geopolitical uncertainties, along with macroeconomic trends such as the ongoing threat of a new pandemic and inflationary fears, mean digital sovereignty is shifting gears and emphasis from **self-determination** to **self-sufficiency** and **survivability**. Each of these includes the following attributes of digital sovereignty.

Data sovereignty: This should include solutions that provide a holistic view of how data is collected, classified, processed, transferred and stored to ensure that data legislation and rules around data localisation are being met. Sensitive and confidential data must be safeguarded for use in both sovereign and non-sovereign jurisdictions. All this requires the constant monitoring of how digital regulations and laws continue to evolve.

Technical sovereignty: This refers to digital infrastructure located in a sovereign environment. It includes the data centers plus all the servers, IT hardware, software, and everything as a service (XaaS) used for cloud-based data and workloads. All this infrastructure should be shielded from non-sovereign digital infrastructure, as well as protected from all extra-territorial interference and scrutiny. Technical sovereignty gives users the ability to run specific workloads without continuous dependence on a specific provider’s cloud infrastructure, software or services. Adopting open-source architecture can help support and achieve this ability.

Operational sovereignty: This includes solutions that offer cloud capabilities that enable transparency in controlling operations, from provisioning and performance management, to monitoring of physical and digital access to the infrastructure. Open source solutions are recommended here as these lend themselves well to interoperability, portability and transferability. This “cloud reversibility” is essential as organisations cannot afford to lock themselves into custom-built solutions that become legacy systems in their own right.

Assurance sovereignty: This focuses on data availability and is essentially all about resilience. For example, in Europe, this is mandated by rules such as the EU Cybersecurity Strategy, Network and Information Systems directive (NIS 2), and the Digital Operational Resilience Act (DORA), which define the principles to ensure that digital infrastructure across the continent’s financial sector is always available to provide critical services.

Supply chain sovereignty: Aside from reinforcing digital supply chain resilience, the aim here is to strengthen the digital economy’s competitiveness, its capacity to innovate, and ability to create jobs. Skills sovereignty can also be considered as a part of this layer.

Geopolitical sovereignty: This takes the idea of digital sovereignty level to a macro level. With IT and digital technologies now at the heart of a nation’s critical infrastructure, governments want to use technology solutions to help deal with the strategic weaknesses, vulnerabilities, and high-risk dependencies of an increasingly volatile geopolitical environment.

Demand for cloud sovereignty

- 75% of organisations in Europe's financial sector currently use cloud computing technologies and services. 25% have cloud migration plans for various applications.**
- As the foundation for digital business innovation, cloud will be at the core of digital sovereignty developments.
- IDC considers cloud sovereignty to be a subset of digital sovereignty. Cloud sovereignty is an approach to ensure an organisation's hybrid cloud environment is owned, deployed, governed and managed locally or regionally within an entity or jurisdiction.
- A sovereign cloud should be subject to all relevant data laws and regulations. It is defined by who the platform provider is, who owns all the underlying infrastructure, where that's all located and who can access it.

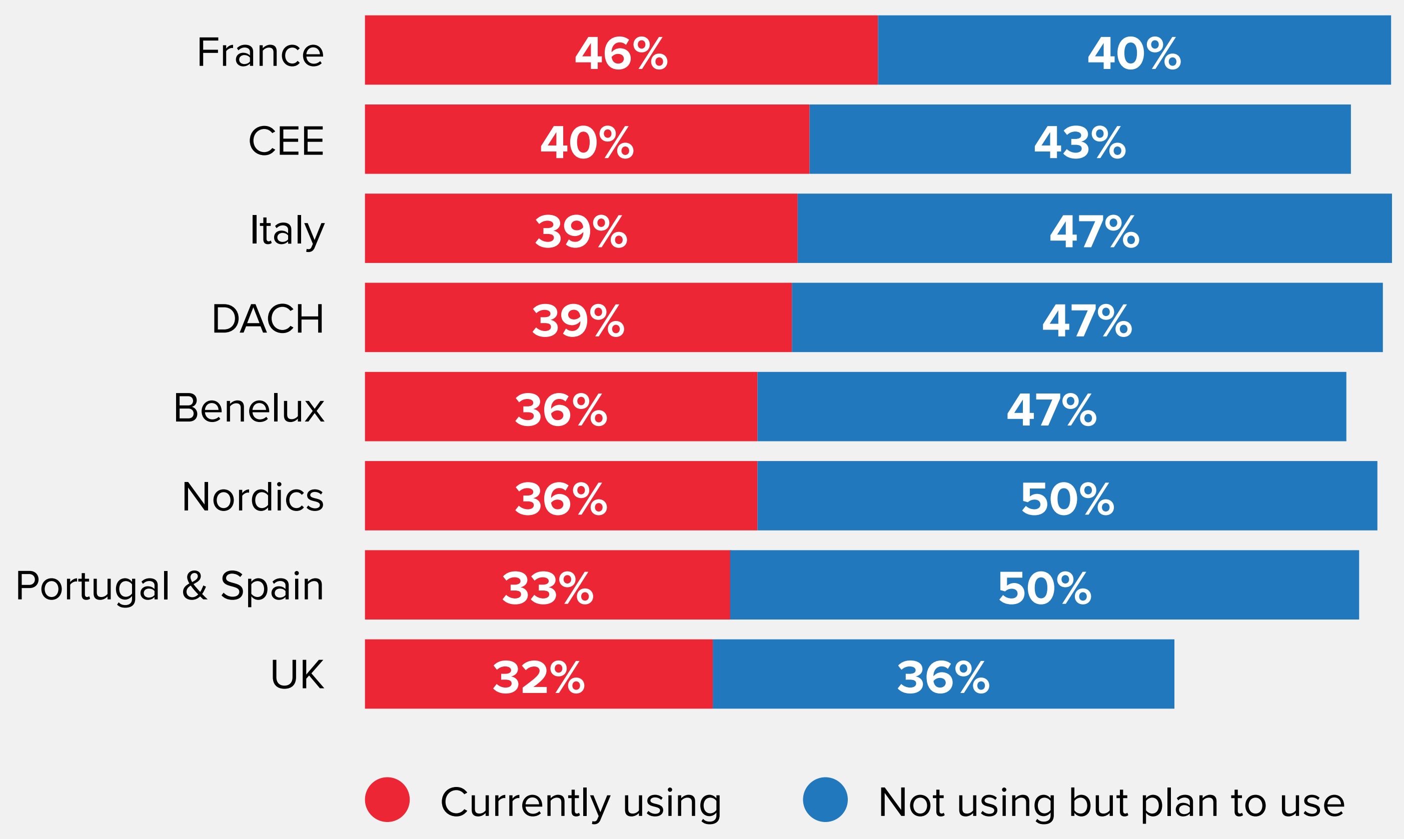
75% * of organisations in Europe now consider digital sovereignty to be a more important **business and technology concern** due to recent economic and geopolitical events.

In separate research conducted by Accenture, the vast majority of those surveyed said that the Russia-Ukraine War **had strengthened their focus on sovereign cloud**.

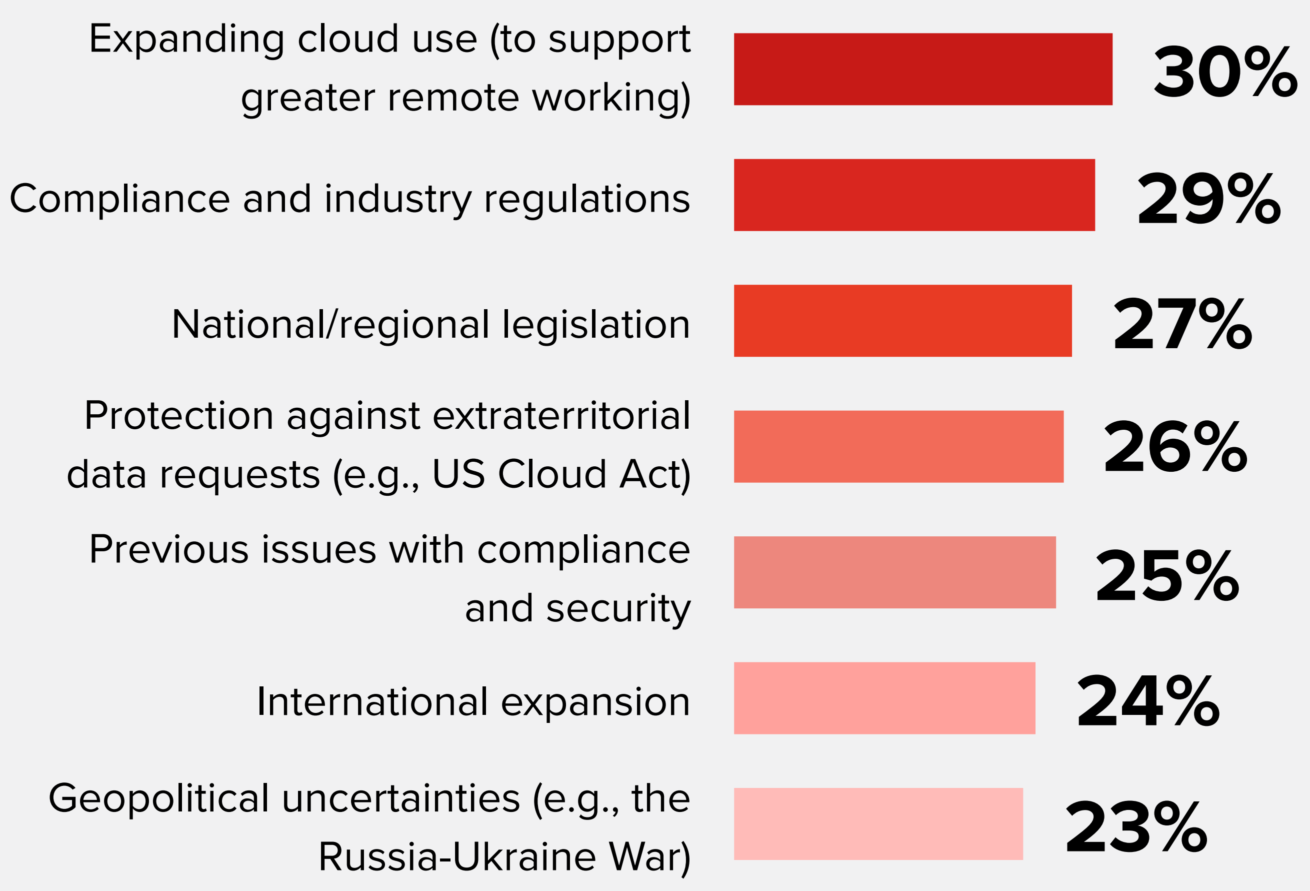
According to IDC, a combined **82%**** of organisations in Europe are either currently using sovereign cloud solutions or plan to do so during the coming years.

While geopolitical uncertainties remain a major concern, when asked what their **specific drivers** were, expanding cloud usage and compliance are the top answers.

Top European markets for sovereign cloud usage**



Main drivers for using sovereign cloud**



*Source: IDC EMEA, Future Enterprise Resilience Survey 2022, Internal, Wave 4, May 10–25, 2022; n = 340
**Source: IDC EMEA, Multicloud Survey 2022, September, August 2022; n = 1,077 (unweighted)

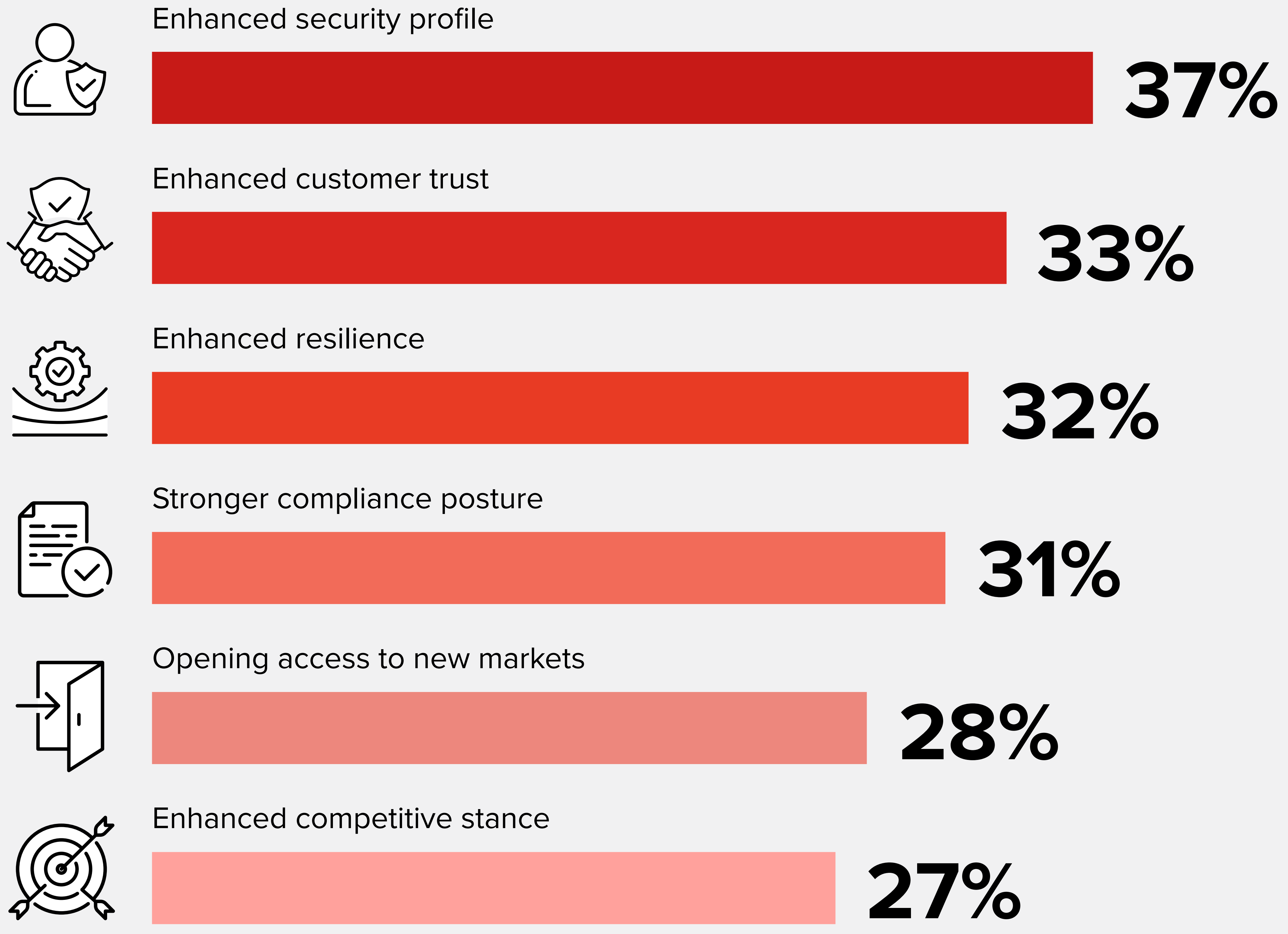
Advantages of digital sovereignty

- Implementing sovereign solutions gives businesses certain advantages. The top 3 benefits cited are about **enhancing security, trust and resilience**.
- Sovereign solutions enable organisations and governments to assert control their over digital infrastructure and data to protect themselves and their critical information infrastructure providers against cyberthreats, espionage and other types of digital attacks from foreign actors.
- This in turn makes organisations that use sovereign solutions more trusted by customers, governments and other stakeholders, boosting their competitive stance and helping them to gain access to new markets.

Digital sovereignty is ultimately about making organisations more resilient as it involves solutions for data backup, data assurance, business continuity and supply chain resilience, among others.

This has become particularly significant in Europe's financial sector, where the Digital Operational Resilience Act (DORA) is now due to come into force.

Main business benefits of using sovereign solutions



Source: IDC EMEA, Multicloud Survey 2022, September, August 2022; n = 1,077 (unweighted)

Assurance sovereignty: The Digital Operational Resilience Act (DORA)

Why have a Digital Operational Resilience Act?

- Financial entities operate in an augmented space, relying on ICT providers. Digital transformation has led to a highly interconnected and interdependent ecosystem, generating many benefits and raising concerns around systemic risk.
- DORA aims to **mitigate systemic risk** by addressing operational resilience with an end-to-end, holistic approach.
- Each critical ICT third-party provider will undergo the direct scrutiny of one of the European Financial Supervisory Authorities, i.e., lead overseer.
- A lead overseer will be appointed for each critical ICT third-party service provider.
- DORA is a “lex specialis” and has priority over other regulations and laws (e.g., NIS, eIDAs, PSD2).

For the first time ever, DORA brings critical ICT service providers and cloud providers under the direct supervision of the European financial supervisory authorities (EBA, EIOPA and ESMA).

DORA timeline and next steps

- DORA’s final text was published on December 27, 2022, and became applicable in January 2023. Full implementation is targeted for December 2024.
- Regulatory Technical Standards (RTS) will be published in 4Q23 and 2Q24; financial entities and ICT providers cannot wait till then to move ahead to comply with DORA, but will have to finetune their approach upon RTS availability.
- Financial entities and ICT service providers will need to implement tools and procedure to fulfil the regulatory requirements.

There is not too much time considering the impact and the activities that financial entities and critical ICT third-party providers need to undertake. Wait and see is not the best approach, neither for ICT providers nor for financial entities. Active programmes should be launched and thereafter finetuned against the regulatory technical standards. There could be severe fines, and non-compliance could mean financial entities might have to replace the ICT service provider.

DORA is a challenge but also an opportunity for critical ICT third-party service providers that will undertake appropriate actions in collaborating with their “financial entities” customers to identify a risk-based action programme and to elevate the relationship. DORA is by law a C-level responsibility.

Who will be subject to DORA?

Financial entities

Banking

Market trading

Insurance

Investment funds

Credit rating agencies Crowdfunding providers Statutory auditors

ICT third-party service providers

Cloud services

Datacen tres

Data analytics

The five pillars of DORA

DORA requirements are applicable to all financial entities and their critical ICT providers. The key regulatory requirements can be grouped under the following five pillars which all require a degree of the sovereign attributes as previously described (see slide 3):

Risk Management

Business continuity and disaster recovey plans a must

ICT Third Party Risk

ICT third parties subject to EU oversight

Digital Operational Resiliency Testing

Annually including remediation plan propotionality applies

Mandatory Incident Reporting

Mandatory major ICT-related incident reporting and voluntary for significant cyberthreats

Voluntary Information and Intelligence Sharing

FSI entities to share threat information and intelligence

The 5 DORA pillars impact sovereignty

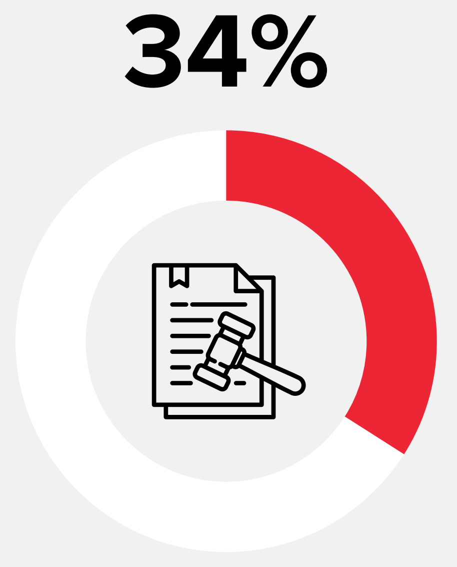
- Assurance sovereignty is all about greater business resilience.
- Financial sector organisations should seek BC/DR providers that offer sovereign solutions to maximise compliance with DORA.

- As part of its calls for digital sovereignty, the EU says all European data must be held by European providers on European soil.
- EU legislation such as GDPR protects European data against extraterritorial interference.

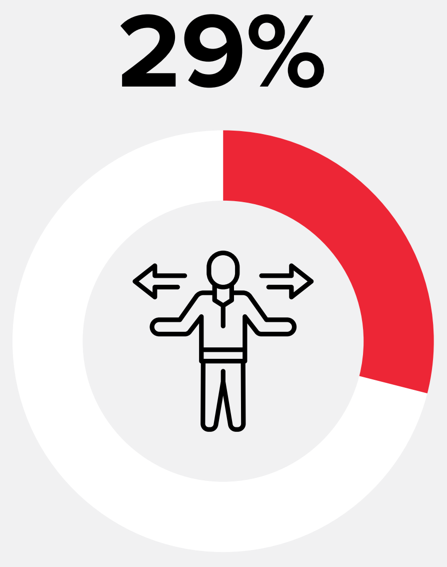
- All data related to testing, incident reporting and information sharing can be considered as sensitive or highly confidential.
- It may therefore need to be stored, processed and monitored in infrastructure that is operated according to sovereign principles.
- This includes the support and admin personnel from third-party or other providers that have access to that data and infrastructure. EU citizenship requirements and/or other identity safeguards may be required for such personnel.

Drivers, benefits and challenges of using sovereign clouds in the banking sector

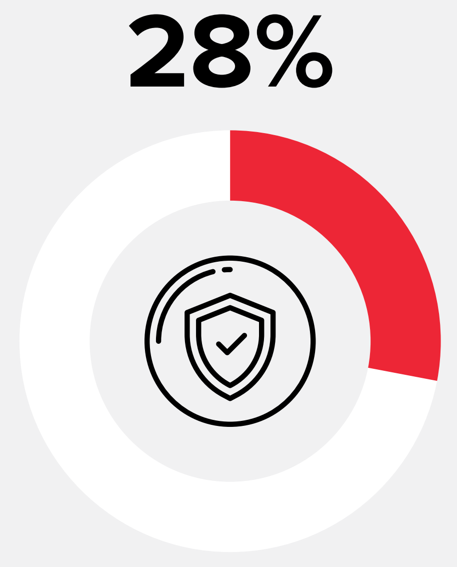
Top 3 drivers of using sovereign cloud in the financial sector



Compliance and industry regulations



Geopolitical uncertainties

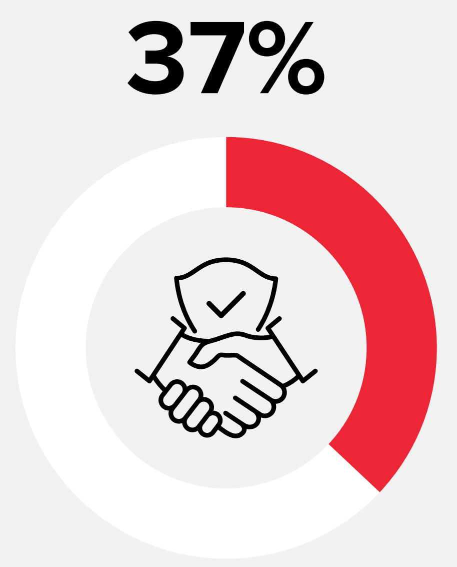


Protection against extraterritorial data requests

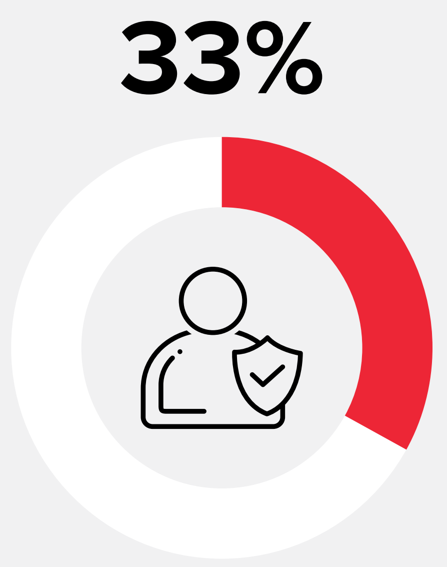
When asked to select the main drivers behind their decision to use sovereign cloud, the top answer for organisations in Europe's financial sector was the need to satisfy **compliance and industry regulations**.

When asked to choose the main business benefits of using sovereign cloud, the top answer selected was **enhanced customer trust**.

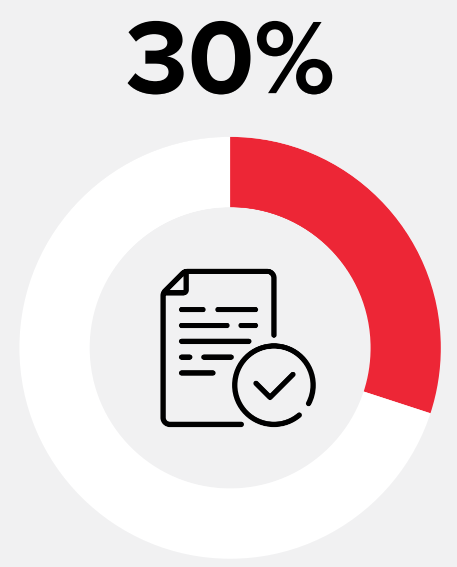
Top 3 business benefits of using sovereign cloud in the financial sector



Enhanced customer trust



Enhanced security profile

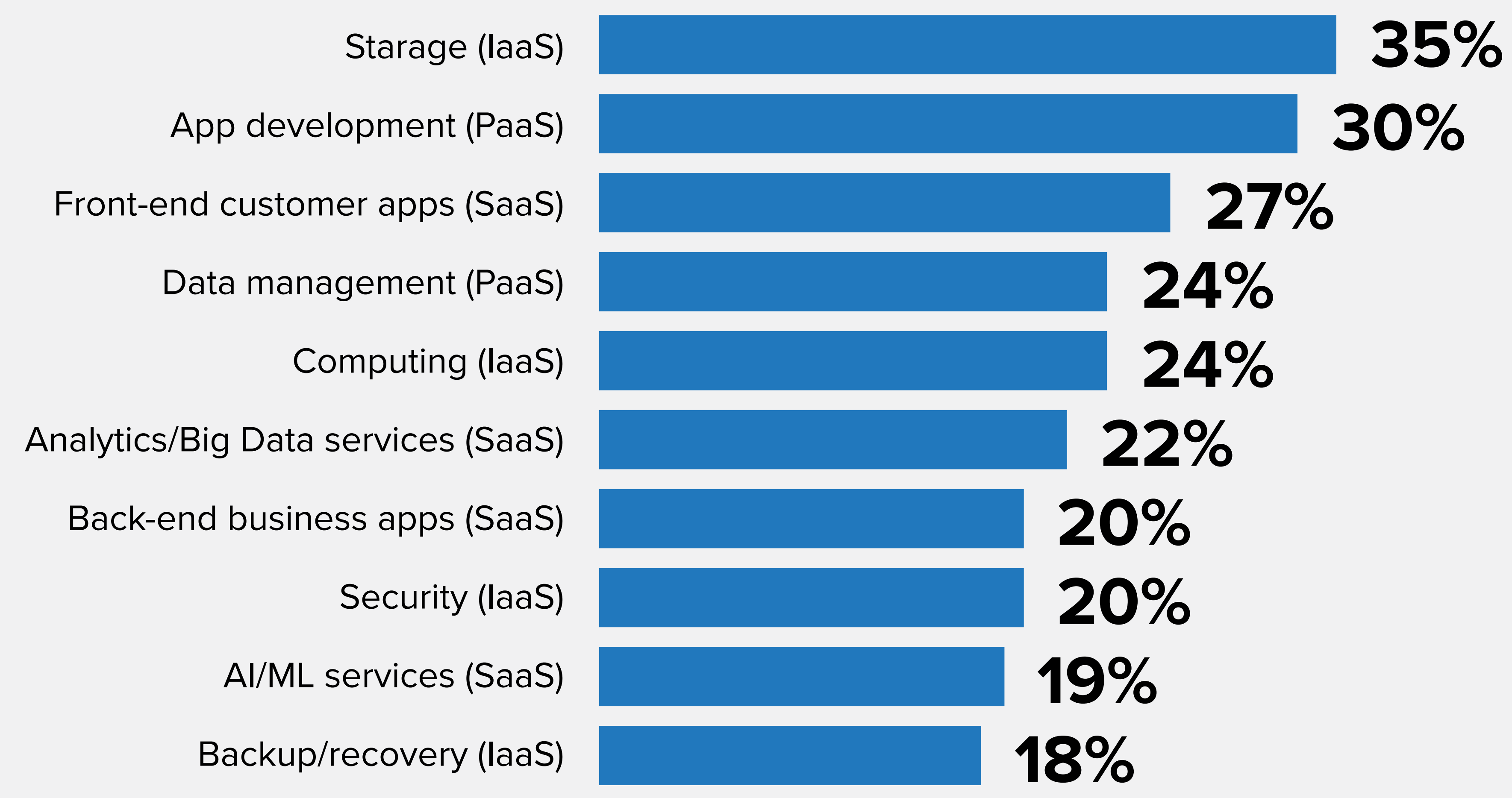


Stronger compliance posture

The challenges of adding a sovereign cloud to a multicloud, hybrid IT environment

The top 3 challenges for finance sector organisations implementing sovereignty solutions are **high complexity, high costs** and conducting a **data review and classification** to determine which workloads should be migrated to a sovereign cloud.

Most affected workloads impacted by digital sovereignty priorities in the financial sector:



Source: IDC EMEA, Multicloud Survey 2022, September, August 2022; n = 1,077 (unweighted)

Any IT transformation initiative requires the involvement of all stakeholders across an organisation to agree and achieve the required business outcomes.

Implementing a **cloud centre of excellence (CCoE)** can prove vital to help drive cultural change across an organisation and win buy-in from all users impacted by the new IT practices and processes that come with migrating to cloud.

Source: IDC EMEA, Multicloud Survey 2022, September, August 2022; n = 1,077 (unweighted)

A potential use case example: migrating from mainframes

Moving apps and workloads to cloud

When asked about their plans regarding mainframe applications, 23% of finance sector organisations in Europe said they will move to public cloud.

- Companies need to look at cloud deployments from an individual workload perspective and decide which cloud model is the best fit. They can then create a hybrid and/or multicloud environment that benefits the organisation's business and IT functions.
- When asked which application they plan to migrate first, the top answer for finance sector organisations was **finance and accounting**.
- When asked which cloud migration strategy they plan to take for these workloads, **18%** will modernise the apps for public cloud IaaS (replatform), **13%** will rearchitect to PaaS and **12%** will replace with SaaS. However, **18%** will retain these workloads on premises.

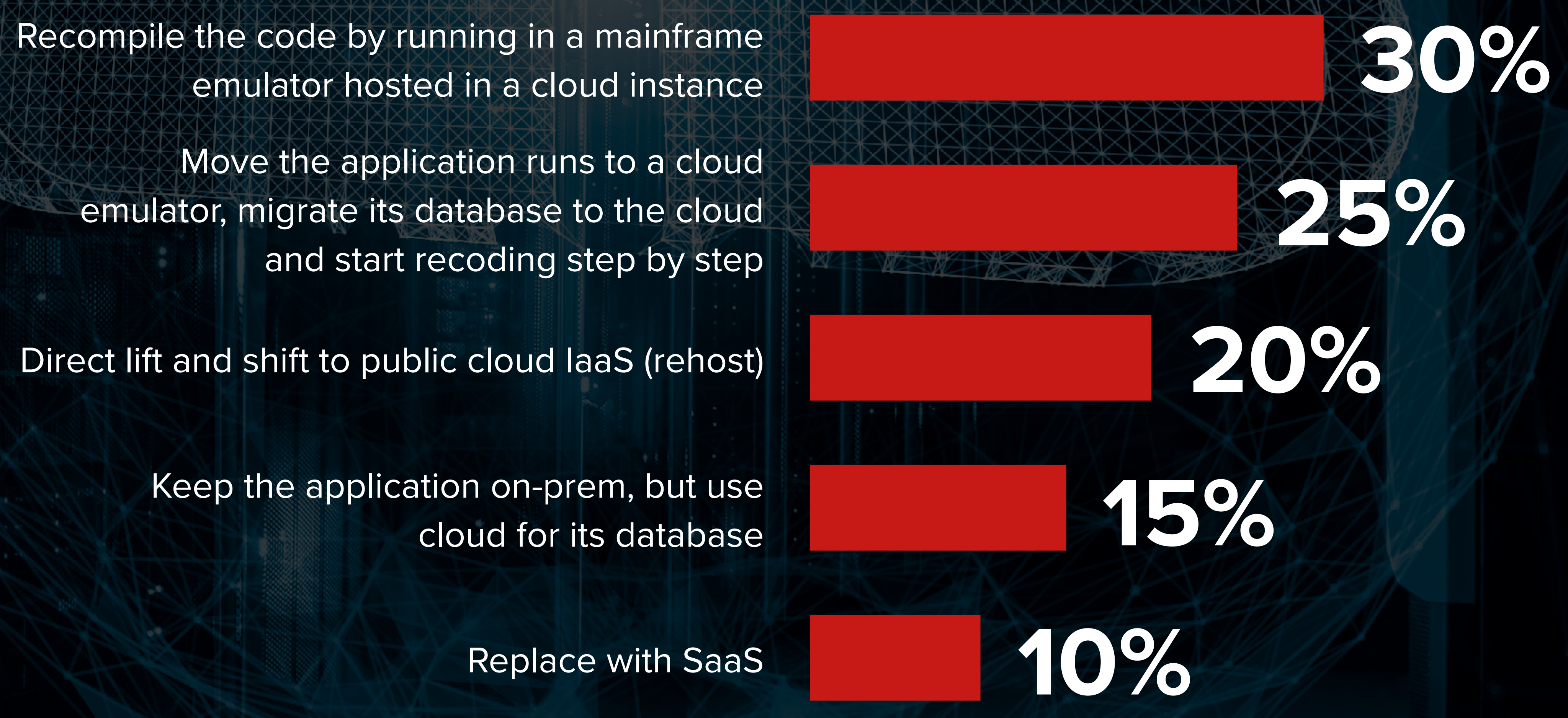
When asked which area they will need to most focus on in terms of skills acquisition and training to address emerging digital sovereignty requirements, the top answer for 41% of organisations was data management (source: Future Enterprise Resiliency & Spending Survey - Wave 4, IDC, May 2022. N=825). Data management includes reviewing and classifying data, and this is part of the challenge of high complexity that many organisations face as they start to implement solutions for data and cloud sovereignty.

Why cloud may not always be the answer

When asked about their plans regarding mainframe applications, 44% of finance sector organisations in Europe said they will retain their mainframe apps on premises.

- The top reasons for finance sector organisations choosing to keep their mainframe apps on premises are lack of in-house cloud skills to migrate; not having the developers who know the applications and can ensure they will still work in the cloud; and concerns about the migration costs being too expensive.
- There also other challenges to consider. When asked what their biggest obstacles were when it comes to app modernisation, the top answers for organisations in the finance sector were assessing and classifying all applications; finding out where to start the modernisation and migration process; and the need to modernise infrastructure first.

Planned strategy for moving mainframe applications to the cloud in the finance sector:



Key takeaways and recommendations

1

Choose the right venue for the right workload

- Not all applications and workloads will need to be migrated to a sovereign cloud. Organisations will need to conduct a data discovery, review and classification exercise to identify which workloads should shift.
- Adding sovereign cloud options in multicloud or hybrid IT scenarios means further complexities and potential extra costs for organisations. The additional investments needed here will cover areas such as local infrastructure and platforms, new tools for data governance and management, and redesigning internal processes and mechanisms to ensure compliance. New skills to support all this may also be required.
- While the need for sovereign solutions will largely be driven by data privacy laws, regulatory needs and continued uncertainties regarding future legislation, all organisations should ultimately be guided by business outcomes when considering cloud. And here, including digital sovereignty in planning will make inevitable future adjustments easier.

2

Importance of gaining buy-in across all stakeholders when migrating

- Providers will need the in-house expertise to be able to talk about sovereignty at all levels within the customer's organisation. For instance, data sovereignty should not be the sole responsibility of the CIO, data protection officer, IT department or other infosec personnel.
- For effective compliance, all lines of business and stakeholder departments — such as legal, procurement, finance and audit teams — need to be a core part of the governance processes.

Key takeaways and recommendations

3 Think beyond day one

- Implementing sovereignty principles is a long-term process and involves adapting to new IT requirements in terms of infrastructure, strategy, governance framework and skills. All these therefore become key criteria for sovereign cloud evaluations.
- It's vital to maintain security and compliance on an ongoing basis, and this should be consistent across the entire IT estate to protect against operational risks. All of this must be a shared responsibility across all partners, so a close working relationship between provider and customer remains crucial. Tools will be needed to regularly manage and monitor.
- The idea of digital sovereignty applies not only right across the IT stack, but also to the partner ecosystem behind it. Vendors will need to constantly assure customers that the sovereign solutions they are leveraging today remain sovereign tomorrow, and that not only do their partners adhere to sovereign principles, but so do their partners' partners.

4 What to look for in a solution provider

- Organisations will seek partners, providers and solutions that offer the greatest adaptability and flexibility with their sovereign offerings. That also includes open source solutions that lend themselves well to interoperability, portability and transferability.
- By over-optimising for local needs, IT decision makers not only risk lock-in with local providers, but also jeopardise future opportunities in international markets where they will need to leverage more globalised IT resources and assets.
- While there are advantages to using cloud solutions hosted by in-country partners and providers, this can reduce the ability to realise public cloud's full benefits. As well as hampering scalability, it could also mean restricted services in terms of being able to leverage energy-efficient datacentres and best-in-class cybersecurity. Partnerships between local and global cloud providers offer a solution here.
- Customers that have a less-developed approach to DX and cloud will need to lean heavily on partners that can offer digital sovereignty expertise with, for example, greater guidance about classifying data and workloads.

Message from the sponsors

About Red Hat

Red Hat is the world's leading provider of enterprise open source software solutions, using a community-powered approach to deliver reliable and high-performing Linux, hybrid cloud, container, and Kubernetes technologies. Red Hat helps customers integrate new and existing IT applications, develop cloud-native applications, standardize on our industry-leading operating system, and automate, secure, and manage complex environments. **Award-winning** support, training, and consulting services make Red Hat a **trusted adviser to the Fortune 500.** As a strategic partner to cloud providers, system integrators, application vendors, customers, and open source communities, Red Hat can help organizations prepare for the digital future.

About Accenture

Accenture is a leading global professional services company that helps the world's leading businesses, governments and other organizations build their digital core, optimize their operations, accelerate revenue growth and enhance citizen services—creating tangible value at speed and scale. We are a talent and innovation led company with 732,000 people serving clients in more than 120 countries. Technology is at the core of change today, and we are one of the world's leaders in helping drive that change, with strong ecosystem relationships. We combine our strength in technology with unmatched industry experience, functional expertise and global delivery capability. We are uniquely able to deliver tangible outcomes because of our broad range of services, solutions and assets across Strategy & Consulting, Technology, Operations, Industry X and Accenture Song. These capabilities, together with our culture of shared success and commitment to creating 360° value, enable us to help our clients succeed and build trusted, lasting relationships. We measure our success by the 360° value we create for our clients, each other, our shareholders, partners and communities. **Visit us at www.accenture.com.**

Red Hat | accenture

About IDC

International Data Corporation (IDC) is the premier global provider of market intelligence, advisory services, and events for the information technology, telecommunications, and consumer technology markets.

With more than 1,300 analysts worldwide, IDC offers global, regional, and local expertise on technology and industry opportunities and trends in over 110 countries. IDC's analysis and insight helps IT professionals, business executives, and the investment community to make fact-based technology decisions and to achieve their key business objectives.

Founded in 1964, IDC is a wholly-owned subsidiary of International Data Group (IDG, Inc.), the world's leading tech media, data and marketing services company.

IDC Custom Solutions

This publication was produced by IDC Custom Solutions. As a premier global provider of market intelligence, advisory services, and events for the information technology, telecommunications, and consumer technology markets, IDC's Custom Solutions group helps clients plan, market, sell and succeed in the global marketplace. We create actionable market intelligence and influential content marketing programs that yield measurable results.

IDC

IDC UK
5th Floor, Ealing Cross, 85 Uxbridge Road, London, W5 5TH, United Kingdom
T 44.208.987.7100

@idc | @idc | idc.com

© 2023 IDC Research, Inc. IDC materials are licensed for external use, and in no way does the use or publication of IDC research indicate IDC's endorsement of the sponsor's or licensee's products or strategies.