



What is a Sovereign Cloud And Who Should Consider It?

Mark Sampson

SAP Sovereign Cloud
Lead, North & Central
Europe

October 2026

Public





Digital Sovereignty: from ~~compliance issue~~ to strategic imperative



Digital sovereignty challenges...



Growing Geo-Political Tension

Changes the risk profile of being dependent of other regions



External threats towards data

Risk of extraterritorial data access (e.g., CLOUD Act)



Internal Regulation rising

EUCS, GDPR, DORA, Compliance becomes more important



Critical Digital dependency

The majority of Cloud and software platforms are concentrated in only a few regions in the world



Shortage situations are rising

Need for Control increases (E.g., Electronic circuits, batteries, rare elements)

As political climates and technology strategies evolve, sovereignty becomes a foundational pillar for any organization with regulatory, operational, or strategic imperatives...applies to many Public, Defence and Regulated Industry clients

“Digital sovereignty is no longer just a policy issue. It is a core business imperative, shaping how organizations manage risk, safeguard operations, and compete in an increasingly interdependent digital world.”

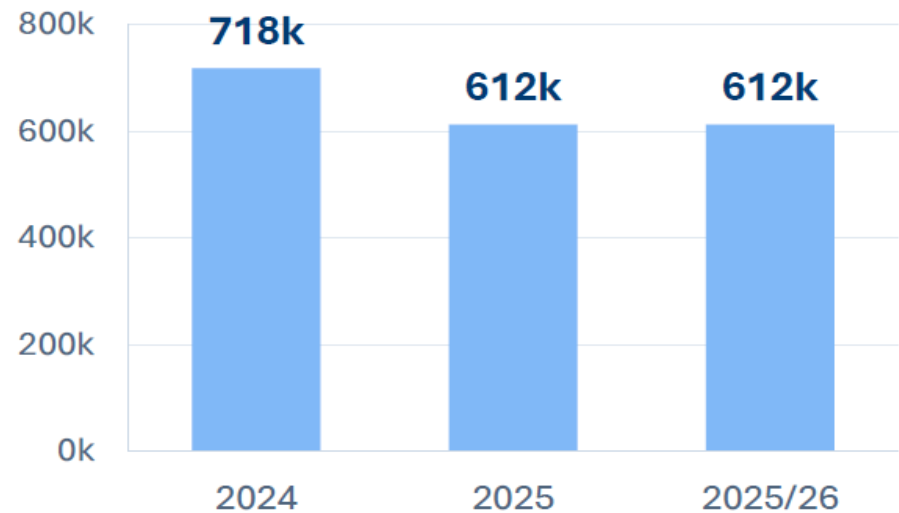
Fernando Alvarez

Chief Strategy and Development Officer, Capgemini.

UK Cyber Exposure and Rising Incident Severity

Businesses identifying a breach or attack

Estimated businesses, preceding 12 months



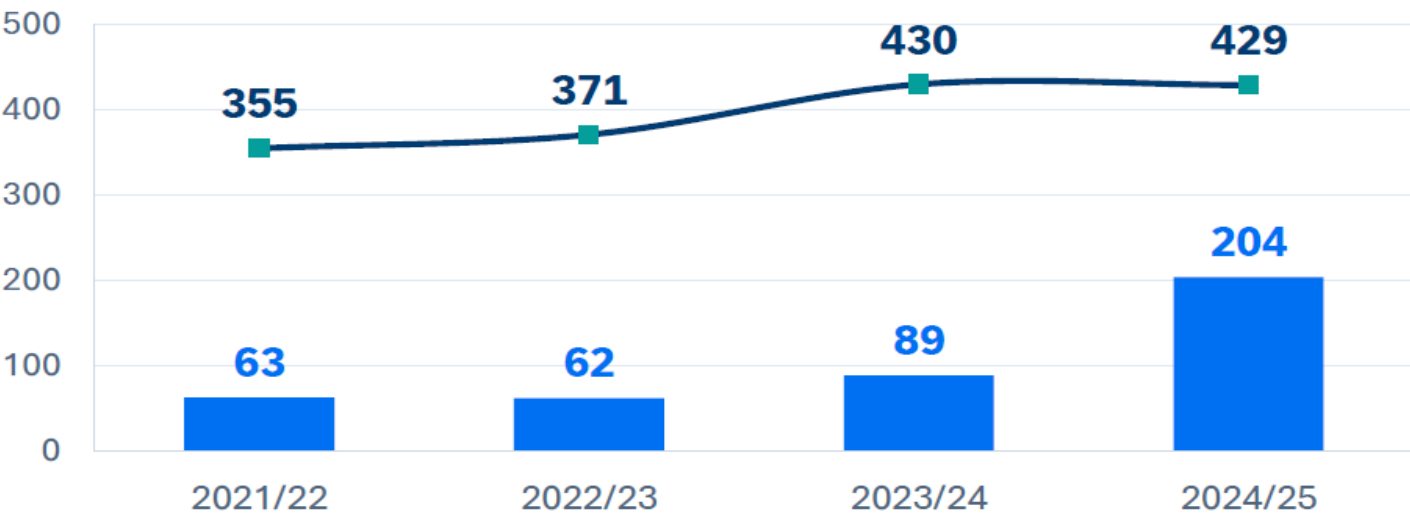
Reported exposure fell, then remained stable

~75%

State-linked share of NCSC-managed CNI and supporting ecosystem incidents
June 2025–May 2026

NCSC incidents: severity and total caseload

Blue bars: nationally significant Dark line: total managed



Nationally significant incidents more than tripled

£14.7bn

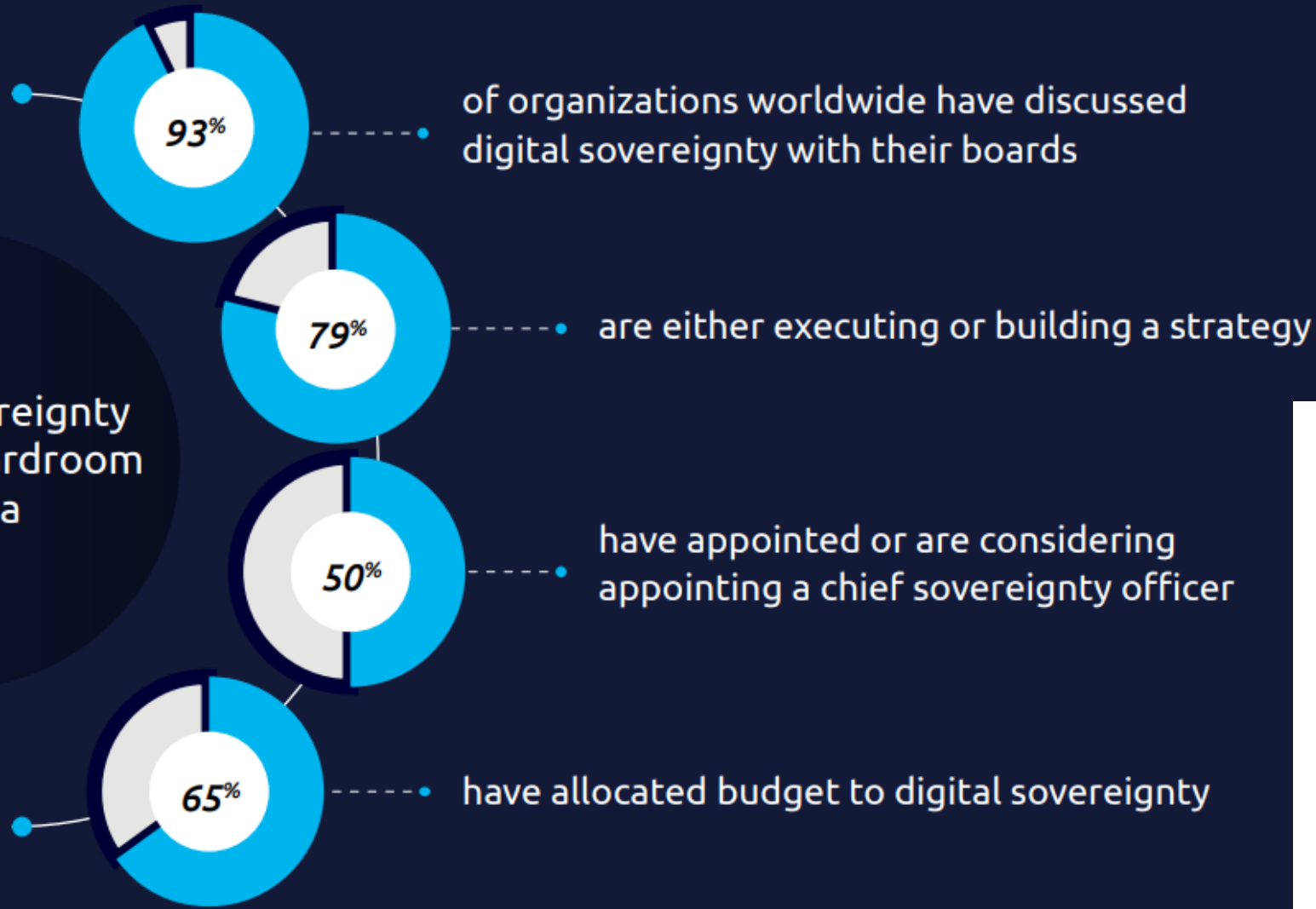
Modelled annual cost of significant cyber attacks to UK businesses
2024 estimate

Sources: UK Cyber Security Breaches Surveys 2024, 2025 and 2025/26; NCSC Annual Review 2025; Parliament; DSIT/KPMG.

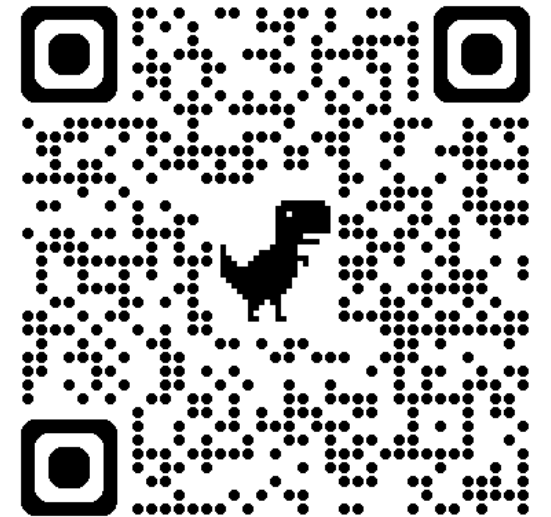
Capgemini Research Institute Report (released Sept 26)



Digital sovereignty
is on the boardroom
agenda



"Sovereignty is a balance between freedom of choice and control"
Martin Merz
SAP President Sovereign Cloud.



<https://www.capgemini.com/insights/research-library/digital-sovereignty/>

Digital Sovereignty

Balancing risks mitigation and strategic goals across the digital value chain



By 2028, over **50%*** of **multi-national enterprises** will have **digital sovereignty strategies**, up from less than 10% today.

Digital Sovereignty

is an organization's capability to be **resilient**, to have **strategic autonomy** and be **free from foreign interference** across the **digital value chain**



“Being sovereign means having the ability to choose your dependencies. For organizations – especially in Europe – the goal is not full autonomy, but a clear understanding of technological dependencies, so they can move from dependence to interdependence.”

Karine Brunet
Chief Operations and
Delivery Officer, Capgemini.

Full digital sovereignty across the entire value chain is usually **unrealistic**. The goal is to find the **right balance** between client's **risk tolerance and strategic goals** using **sovereignty not to constrain innovation**.

SAP's Sovereign Cloud Domains



DATA

All data (incl. telemetry) is stored within country or approved countries – preventing unauthorized cross-border transfers & adhering to critical infrastructure requirements.



LEGAL

Governance stays aligned. Legal entities are based locally or in approved countries, and ownership, control and influence risk by foreign authorities is mitigated.

Data sovereignty

Data residency:

Data storage is local or within an approved country.

Data compliance:

Adherence to critical infrastructure regulations.

Data flows:

Prevention of unauthorized data transfer across national borders.

Legal sovereignty

Location of legal entity:

Legal entities must be located within an approved country, with mitigated control influence from foreign ownership.¹

Operational sovereignty

Admin/maintenance nationality:

Personnel must be from an approved or local country.

Admin location:

Administrators are required to operate from approved or local locations.

Security clearance:

Security clearance is mandatory for personnel handling sensitive government data.

Technical sovereignty

Physical security:

Data centers must implement enhanced security protocols.

Control plane (incl. all tooling):

The control plane must be locally deployed & managed.

Tenant separation:

Logical separation through encryption or physical separation.



OPERATIONAL

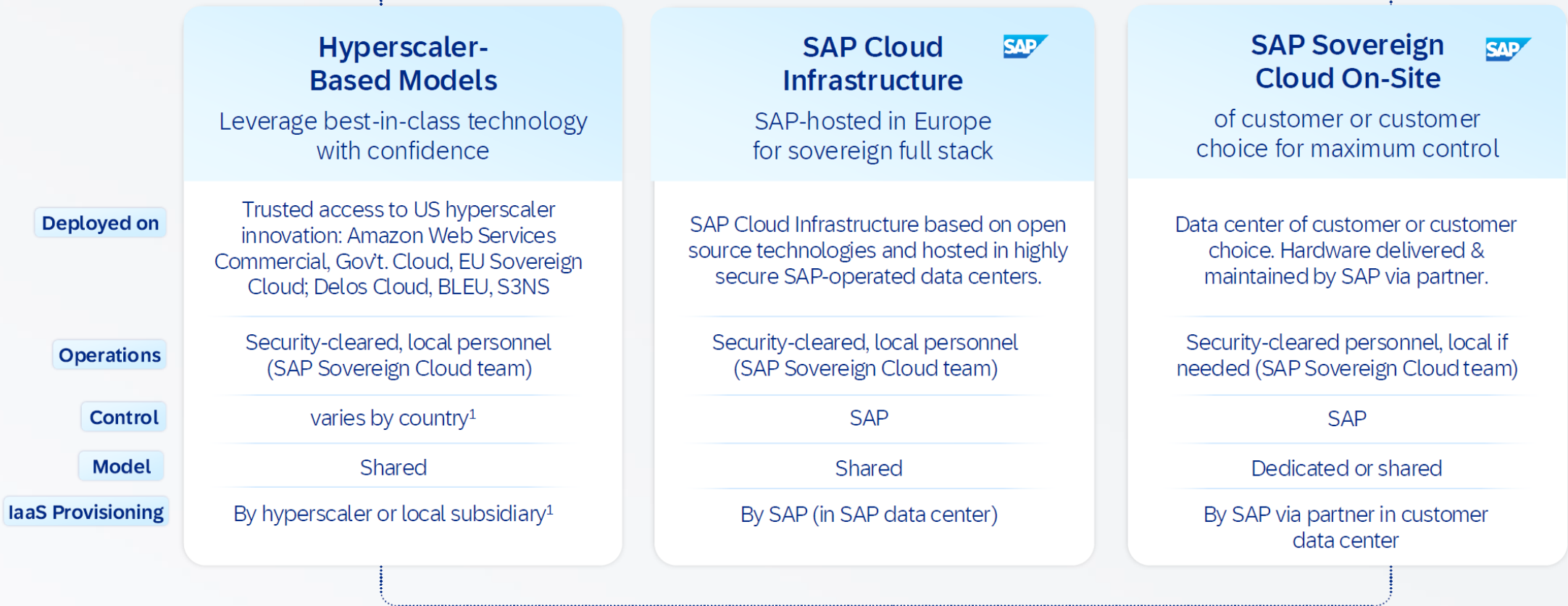
Operations stay local. Only approved personnel, local nationals or those from trusted countries, handle administration & maintenance. Mandatory security clearance for personnel handling classified data.



TECHNICAL

Control planes (incl. all tooling) are locally deployed & managed. Logical separation of tenants through encryption, or physical separation. Data centers must implement enhanced security protocols.

SAP Sovereign Cloud Deployment Options



1 AWS for AWS Commercial (ANZ, UK, CAN), Government Cloud (US), EU Sovereign Cloud. National partner Clouds: SAP with Delos Cloud (SAP subsidiary), air-gapped (GER); Capgemini with BLEU (FRA); Thales with S3NS (FRA)

	USA ¹	AUS/NZ	UK	Canada	India	Europe	Europe	GER Federal	France ⁸	Global (excl. USA)
Infrastructure	AWS GovCloud	AWS				AWS ESC	SAP Cloud Infrastructure ⁵	Delos Cloud ⁷	SAP Cloud Infrastructure	SAP Sovereign Cloud On-Site

Capgemini's Sovereign Cloud Assessment for SAP

Areas of Focus

SAP Sovereign Cloud Domains



Capgemini Sovereign Cloud Assessment for SAP Dimensions



Our Sovereign Cloud Assessment for SAP approach includes detailed analysis of the Dimensions through surveys and interviews with key client stakeholders

Capgemini's Sovereign Cloud Assessment for SAP

* Standard Assessment based on a single SAP Platform Estate. Custom Assessment options are also available



Assessment Overview



Why is this important?

Rising regulatory, cybersecurity, jurisdictional and geopolitical pressures mean that organisations must ensure critical SAP systems and data are hosted, managed and secured compliantly. Failure to do so can have serious business, legal and financial implications.

Finding the right Sovereign solution, and defining the correct path to it, is imperative to enable organisations to make cloud and SAP deployment decisions that are **legally compliant, risk-aware, future-proof and defensible** - without unnecessarily sacrificing cost, agility or innovation.



What is it?

Tailored, structured evaluation that provides an **evidenced-based** approach to determine how an organization's data, systems and operations should be deployed to meet regulatory, cybersecurity and jurisdictional requirements. This Assessment is not a "technical nice-to-have"; it is a **risk, compliance and business-value decision tool** that analyses factors such as data residency, legal access, operational control requirements, mapping these to the most appropriate SAP deployment model, ensuring the chosen model is **compliant, proportionate, defensible and aligned to business objectives**.

1

2

3

4

5

Initiate Discover Evaluate Develop Present



What are the Deliverables?

- Assessing and qualifying Sovereign Hosting needs (Needs Analysis)
- Sovereign strategy assessment and alignment
- Sovereign Hosting Compliance validation (Fit Analysis)
- Identifying required enabling activities for Sovereign Hosting adoption (Gap Analysis)
- Detailing the path forward for the recommended Sovereign Hosting approach (Roadmap Definition)



Benefits



Clear, defensible deployment decisions



Reduced regulatory and compliance risk. Early risk identification



Stronger business case and investment confidence



Improved security and operational resilience



Business Outcomes

TAILORED, FOCUSED ASSESSMENT WHICH MINIMISE BUSINESS IMPACT AND DISRUPTION

ASSESS NEED, STRATEGY, FIT AND GAP TO ENABLE ADOPTION OF SOVEREIGN CLOUD

PROVIDES THE PATH TO ACCESS THE RANGE OF SAP'S SOLUTIONS IN A SOVEREIGN CLIENT MANNER

Capgemini SAP Sovereign Cloud Credentials/Capabilities



Selected Capgemini Credentials

SAP Sovereign Cloud Clients	Bleu in France (JV: MS Azure, Capgemini, Orange) provides Sovereign Cloud workloads which are also being made available for SAP
Greenfield scenarios: Defence Manufacturer Nuclear Enrichment Services Provider UK Public Sector Cluster (supporting) Defence Ministry (contracted via SAP)	CLOUD^{4C} Part of Capgemini
Brownfield/Hybrid scenarios: UK Tax Authority (CNI/40TB+ d/base) Space and Defence Manufacturer	Currently running RISE and Sov Infra (ME)
Sovereign Technology Partnership with SAP	SC Validated Partner Programme
Unique SAP-AWS-Capgemini Sovereign Delivery Collaboration Forum	SAP Sovereign Cloud PARTNER

Relevant Capgemini SC Services Portfolio Include



...rapid digital and SAP focused sovereignty assessments helping clients build their path to SAP Sovereign Cloud



...build, migrate, transform and operate solutions in SAP Sovereign Cloud



...data quality and migration services leveraging Syniti's leading data management platform



...continuously innovate and exploit new enhancements to SAP product suite incl Joule-powered AI use cases

Takeaways

