Nordcloud
an IBM Company

Digital sovereignty roadmap: From uncertainty to control.

A best-practice approach to planning your digital sovereignty journey

Brought to you by Nordcloud an IBM Company

The board is talking about sovereignty… and you need a solution

The conversation around digital sovereignty is heating up across organisations in Europe. Questions around control, compliance and vendor dependency are no longer abstract – they're shaping cloud, AI and data strategies right now.

Sovereignty refers to your ability to ensure that your organisation's data, workloads and digital operations remain under your control and comply with local laws and regulations.

The topic is front of centre because of rising geopolitical tensions, evolving EU regulations, growing scrutiny of foreign infrastructure/service providers and massive data processing through AI.

Sovereignty is a challenge, but also an opportunity

Sovereignty isn't a temporary trending topic that will disappear with the next US election cycle. It's part of an emerging awareness at the highest levels of governments and enterprises that there's too much dependence on non-EU services and tech.

This guide will help you strike the right balance and capitalise on the opportunity.

Sovereignty can be a catalyst for building trust, resilience and agility in a rapidly evolving digital economy.

But to get there, you need a clear, actionable path – one that balances risks and regulatory demands with costs and agility to innovate.

Chapter 1

What should sovereignty do for you?

When we talk about framing a sovereignty strategy, you're essentially planning how you maintain (or regain) control of data and data processing.

That control is fundamental to your ability to run reliable processes (and, ultimately, your business). And, because it involves data at the most fundamental level, it affects your broader cloud and AI approaches.

Chapter 1

Ultimately, your sovereignty strategy must therefore be based around your ability to control 4 key areas:

Where data is located

Your location and the location where your data is stored/processed determine what legislation is applicable.

That legislation can be both restrictive (e.g. some data may not leave country borders) and protective (e.g. GDPR within EEA borders).

Who has access to data

Key to addressing sovereignty concerns is determining who has the ability to access your data, including:

- The owner of your infrastructure (e.g. Microsoft, AWS, Google)
- The partner managing your infrastructure (e.g. your managed services partner)
- Your organisation (through access management)
- Regulatory/government organisations that have legal means to request your data through the above parties

What security you need

You can protect your data through security measures, for example to ensure reliable processing or confidentiality.

This can be done by your infrastructure provider (evidenced through certificates) and/or implemented by you or your infrastructure vendor (e.g. using data encryption or implementing disaster recovery).

How you make it work

Additional aspects like **technical capabilities, costs, standardisation and sustainability** determine how you can run your cloud/AI/data services in line with your business values and requirements, alongside your sovereignty needs.

Chapter 2

A best-practice approach to planning your sovereignty strategy

In order to keep or regain control of your data, processes and therefore your business, we recommend our 5-step process

Step 1	Demystify sovereignty and align stakeholders
Step 2	Identify your sovereignty risks
Step 3	Strategise and blueprint sovereignty solutions
Step 4	Take an architecture-led approach to implementation and/or migration
Step 5	Monitor and maintain sovereignty

Let's look at each step...

Nordcloud
an IBM Company

Step 1

Demystify sovereignty and align stakeholders

There are lots of rumours, LinkedIn conversations and hyperscaler marketing materials around sovereignty. But what does it actually mean? What do you need cope with? What do the hyperscalers and EU sovereign organisations actually offer?

You need to gain a common understanding around terminology, business needs and available options, aligning stakeholders from across IT and business. Structured workshops are the most effective approach, in our experience.

Sample sovereignty workshop agenda

Sovereignty concerns and drivers

- US and EU policies and regulations affecting public cloud
- Organisational concerns from IT, security, compliance, risk and privacy stakeholders, e.g. cloud product owners, security team, compliance officers, risk managers, architects, IT managers

Organisational readiness for sovereignty

- What sovereignty is
- Why sovereignty matters
- How sovereignty fits into the organisation's existing IT and data strategy

Understanding sovereignty solutions

- What the hyperscalers offer (Microsoft, AWS, Google)
- What independent providers offer (with hyperscaler tech, open source, proprietary)
- What factors should shape the organisation's approach to selecting a solution pathway

Planning a sovereignty roadmap

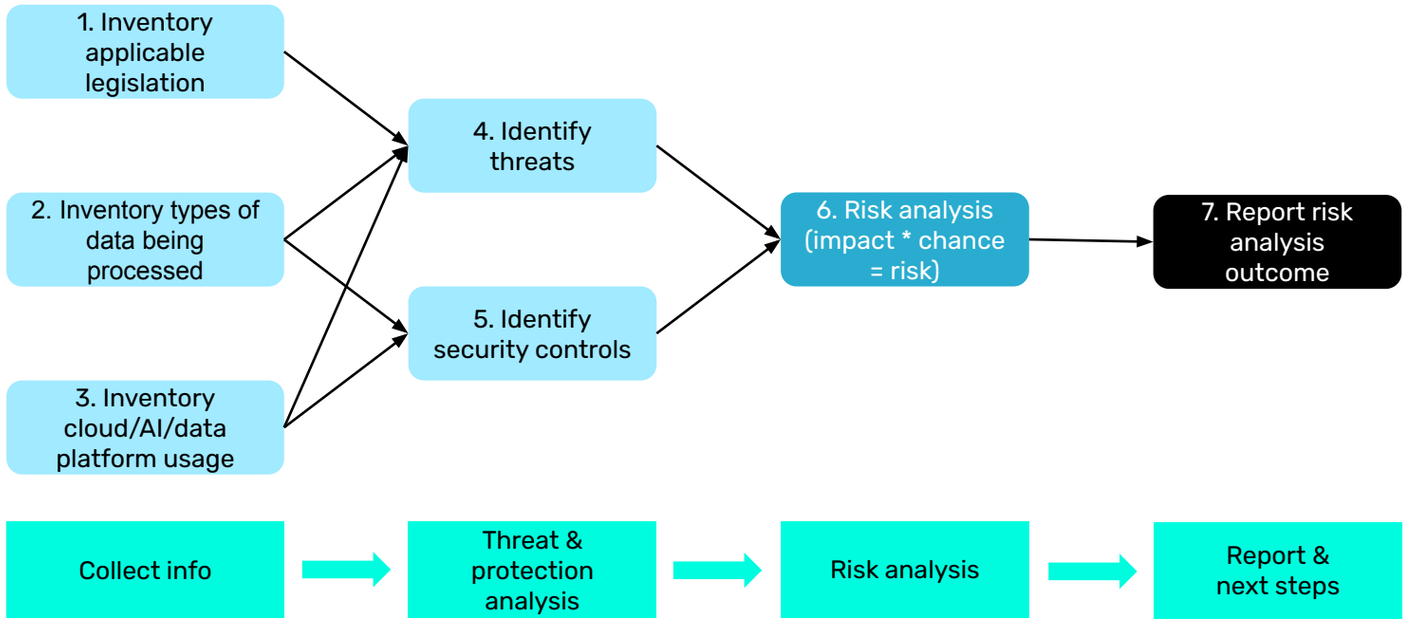
- Assessing risks
- Considering architectural approaches

Step 2

Identify your sovereignty risks

We often see customers jump to conclusions about how to solve their sovereignty concerns. Instead, we recommend taking a step back and conducting an objective risk assessment. Use a structured approach to analyse sovereignty-related risks, while also considering aspects like costs and innovation.

Risk assessment process



Step 3

Strategise and blueprint sovereignty solutions

The workshop and risk assessment provide a common language and evidence base for planning the most appropriate sovereignty solution for the organisation. We also have standardised sovereignty blueprints (see more on this in Chapter 3) to help integrate best practices and expedite this solutioning. And as a premium partner of the hyperscalers, we always account for their latest sovereignty offerings (which is a fast-moving area that's hard to keep up with) – while maintaining an independent and objective approach.

Step 4

Take an architecture-led approach to implementation and/or migration

This is where you implement your chosen solution, including enhancing security measures and/or migrating data or workloads to more sovereign infrastructures.

Based on your chosen blueprint, it could mean moving your public hyperscaler cloud environment to physical data centres in the EU. It could also mean implementing a hybrid cloud solution where certain high-risk workloads are migrated from public hyperscaler cloud to a private cloud, local cloud or EU sovereign cloud provider.

We have a set of standardised roadmaps and solutions at the ready, all based on our vast experience in a hybrid cloud context, which also enhance your security and compliance monitoring capabilities.

Step 5

Monitor and maintain sovereignty

Becoming more sovereign is only part of the challenge. Maintaining sovereignty is another part. To monitor your sovereignty state, you must be continually aware of what's happing in your environments – and integrate that with IT management processes and organisational/market developments.

The aim is to remain up to date and in control of sovereignty and associated compliance and security. For example, we support enterprises here by combining advisory and Security Operations Centre (SOC) services. And we provide automated audits and dashboards to streamline oversight and reporting.

Chapter 3

Using sovereignty blueprints as a strategy shortcut

As mentioned above, we have standardised sovereignty blueprints that help our customers integrate best practices into their strategy and solutioning. After all, you don't know what you don't know – and this is a rapidly-evolving area.

This table gives you a high-level overview of the sovereignty blueprint levels we use, scoring key characteristics from 1 to 5.

1. **Sovereignty:** How independent the blueprint is
2. **Costs:** Generic cost level for the blueprint
3. **Flexibility:** How usable and deployable the blueprint is
4. **Resilience:** How well the blueprint copes with calamities and disasters

Chapter 3

Which level is right for you?

This depends on the outcomes of your workshop and risk assessment, but here are the trends we see:

- **Levels 1-3 provide cost-efficiency and high technical agility but come with sovereignty trade-offs**

  These levels would be most appropriate for processing less sensitive data in less regulated industries or, for example, agile start-ups that favour flexibility above sovereignty.

- **Levels 4-6 offer the best of both worlds, providing more control either via local infrastructure or local operators at the expense of higher complexity and cost**

  They're best suited for more regulated industries and organisations that process (EU) special personal data or run AI services with confidential data.

- **Levels 7-9 maximise independence but generally lag in scale and features**

  Typically, these infrastructures serve governments running judicial or defence services, as well as corporates with highly sensitive (trade, design, research) secrets.

Blueprint level	Description	Sovereignty (5=most sovereign)	Costs (1=lowest cost)	Flexibility (5=most flexible)	Resilience (5=most robust)
L1: Hyperscaler global cloud	Standard hyperscaler global cloud solutions	1	1	5	5
L2: Hyperscaler EU cloud	Localised hyperscaler cloud usage, with legal guarantees on (meta)data and operations	2	1-2	5	5
L3: Hyperscaler EU sovereign solution	Specific hyperscaler sovereign solutions	3	2-3	4	4-5
L4: Local hyperscaler cloud	Running hyperscaler technologies in a local data centre, connected to hyperscaler public cloud	2-3	3	3	2-4
L5: Hybrid cloud	Combination of local dat centre and hyperscaler public cloud	3	3	2-4	2-4
L6: Licenced hyperscaler cloud	Hyperscaler tech with local EU sovereign partners, not connected to hyperscaler public cloud	4	3-4	3-4	2-3
L7: EU native cloud	Running non-hyperscaler tech via EU sovereign partners	4-5	3-4	3-4	1-3
L8: EU open source cloud	Running non-hyperscaler open source tech via EU sovereign partners	5	4	2-3	1-2
L9: Data centre in the basement	L9: Running all workloads in local data centres, managed by your organisation	5	5	1	1

Chapter 4

Immediate actions to kick-start your sovereignty journey

So where should you start? What information should you have in place to hit the ground running with your sovereignty workshop and risk assessment?

We recommend starting with these 5 actions to provide the right baseline for ongoing discussion and planning.

01.

Check your data types and locations

You can't decide on sovereignty solutions without knowing:

- What data types the organisation has (e.g. public, personal, financial, confidential)
- Where that data is physically processed

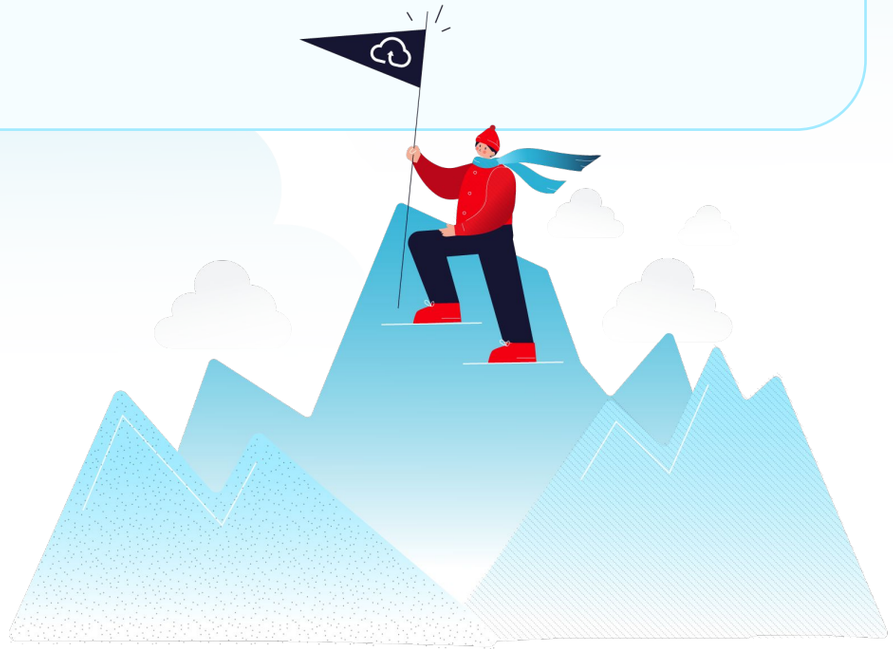
Many organisations know this on a high level, but is that complete and accurate enough? A first step in addressing your sovereignty challenges is having an actual and complete overview of where you process what type of data.

02.

Review identity and access management

Hyperscalers offer a wide range of services to manage access, but you need to actually implement who has access to which (type of) data.

Make sure you have this in control and periodically review access rights, especially for privileged accounts (admin/root access) and vendor employees. This is the easiest part of controlling who has direct access to your data.



03.

Implement encryption and key management

To increase the level of protection your data has, you can and should use encryption – when storing, transporting and maybe even when processing data.

Make sure you not only implement encryption but also implement proper key management. And consider using customer managed keys for classified data.

04.

Reflect on your cloud strategy

Usually, our customers have a cloud-first strategy to help them leverage the agility, lower costs and robustness of public cloud.

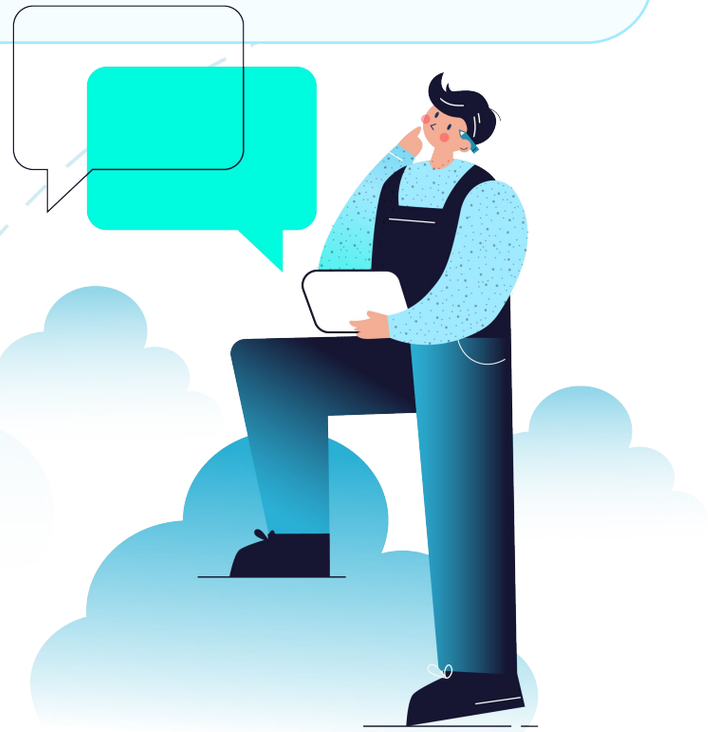
Now that sovereignty is coming into play, this strategy should be revisited and potentially changed. Examples we're seeing include refocusing to be container-first (to become less infrastructure independent) or being cloud-first only for public data processing workloads.

05.

Reflect on your data and AI approach

More than ever, data management is key. This isn't only because of sovereignty. It's also because laws and regulations like DORA, NIS2, the EU AI Act (and comparable legislation in the UK, Norway and Switzerland) are adopting risk-based approaches.

Plus, AI is processing data on a massive scale. At a minimum, ensure you have proper data owners who are responsible for data management and data security.



Strike the right balance with your sovereignty, cost, flexibility and resilience trade-offs

Enterprises tell us that one of their biggest sovereignty challenges is how fast everything is moving – regulation, hyperscaler offerings, AI tech... We help you keep on top of this fast-moving area, so you can plan and implement a sovereignty strategy that balances a range of complex needs.

Contact us to discuss how we can support your sovereignty journey

Contact us

Why Nordcloud?

Structured approach that delivers rapid results

We're known as the European cloud partner that gets difficult projects done, efficiently and cost-effectively. And we have that reputation because we have a structured methodology shaped by architecture approaches, best practices and tech capabilities like automation that pre-empt pitfalls and overcome blockers that would otherwise hold up results.

European cloud expertise

We're hybrid cloud experts and a leading partner for all 3 hyperscalers. For example, we're a launch partner for Microsoft Sovereign Cloud and AWS EU Sovereign Cloud – putting us at the cutting edge of developments and insight. At the same time, we're provider agnostic and independent, helping you create the optimal solution for your enterprise needs (even if that means migrating your workloads out of hyperscaler solutions).

Empowered teams

We're commercially focused, using proprietary tools and technologies that help you maximise value from your sovereignty approach. From technology to training, from solution design to DevOps, you get the support needed to (re)gain control of your cloud, AI and data.