

Digital sovereignty is about being smart

Most CIOs know the feeling of being tied too closely to external vendors. Contract renewals become harder. Licensing costs increase. And systems that once felt flexible and valuable can gradually start to feel like a liability.

That concern is not new. What is new is the growing focus on digital sovereignty. In recent years, digital sovereignty has moved from being a political discussion to becoming a very real concern for CIOs: the risk that dependency on specific vendors can expose the business to geopolitical instability, regulatory uncertainty and reduced strategic freedom.

The question many CIOs are now asking is simple: How do we continue to benefit from cloud platforms, SaaS ecosystems and AI services while still maintaining digital sovereignty?

The answer is more practical than ideological. Digital sovereignty is not about rejecting technology. It is about making conscious architectural decisions that preserve flexibility, resilience and strategic freedom over time.

It Is Not About Getting Rid of US Technology only

The debate around digital sovereignty often becomes emotional and ideological. It quickly turns into a discussion about getting rid of US software, avoiding dependency altogether, hosting everything internally or building everything from scratch.

In reality, most CIOs know that these extreme positions are not realistic — at least not in the short or medium term. US-based cloud platforms, SaaS ecosystems, AI services and technology partnerships create too much value. In many areas, there are currently no fully comparable European alternatives. Avoiding these technologies entirely would often hurt competitiveness far more than it would increase independence.

Digital sovereignty, therefore, cannot be about avoiding certain technologies altogether. It has to be about maintaining enough strategic control to make technology decisions freely. In short: preserving room to manoeuvre.

Building an exit-driven strategy

The digital sovereignty discussion becomes much more useful when it is translated into a practical architectural question:

“Is our ability to replace core platforms operationally viable — or merely theoretical?”

Exit planning is not a new concept. Organisations subject to DORA or NIS2 are already required to consider how critical technologies and vendors can be replaced if necessary. But if these plans exist only to satisfy auditors and regulators, they provide very little strategic value.

Strong enterprise architecture teams make exit planning a living part of IT strategy. More importantly, they stop treating exit plans as documentation exercises and start treating them as real operational capabilities that must be prioritised, tested and validated.

Planning and testing for a potential exit is one of the most powerful first steps an organisation can take towards digital sovereignty.

Planning for exit is planning for stability

A useful exit strategy is not about preparing to leave every vendor relationship. It is about ensuring that you can leave if circumstances change.

Modern IT landscapes will always depend on external platforms and ecosystems. Those dependencies are not the problem. The problem arises when they become so deeply embedded that the organisation loses its ability to change course.

Digital sovereignty is therefore not about reducing dependencies to zero. It is about understanding them, managing them and ensuring that they can be changed when business conditions require it.

When organisations know they can migrate data, replace integrations, retrain users and transition critical capabilities within an acceptable timeframe and cost, they operate from a position of strength. They are better prepared for regulatory change, more resilient in the face of geopolitical uncertainty and better positioned in contract renewals.

Enterprise architecture teams have a critical role to play in this effort. By making exit planning a core architectural discipline rather than a compliance exercise, they can turn dependencies from strategic vulnerabilities into calculated risks with realistic mitigation options.

Digital sovereignty is not achieved through isolation. It is achieved through preparation.

The organisations that maintain the greatest freedom to act tomorrow are the ones that deliberately design for change today. Because the true measure of digital sovereignty is not whether you depend on others. It is whether you can change direction when circumstances demand it.