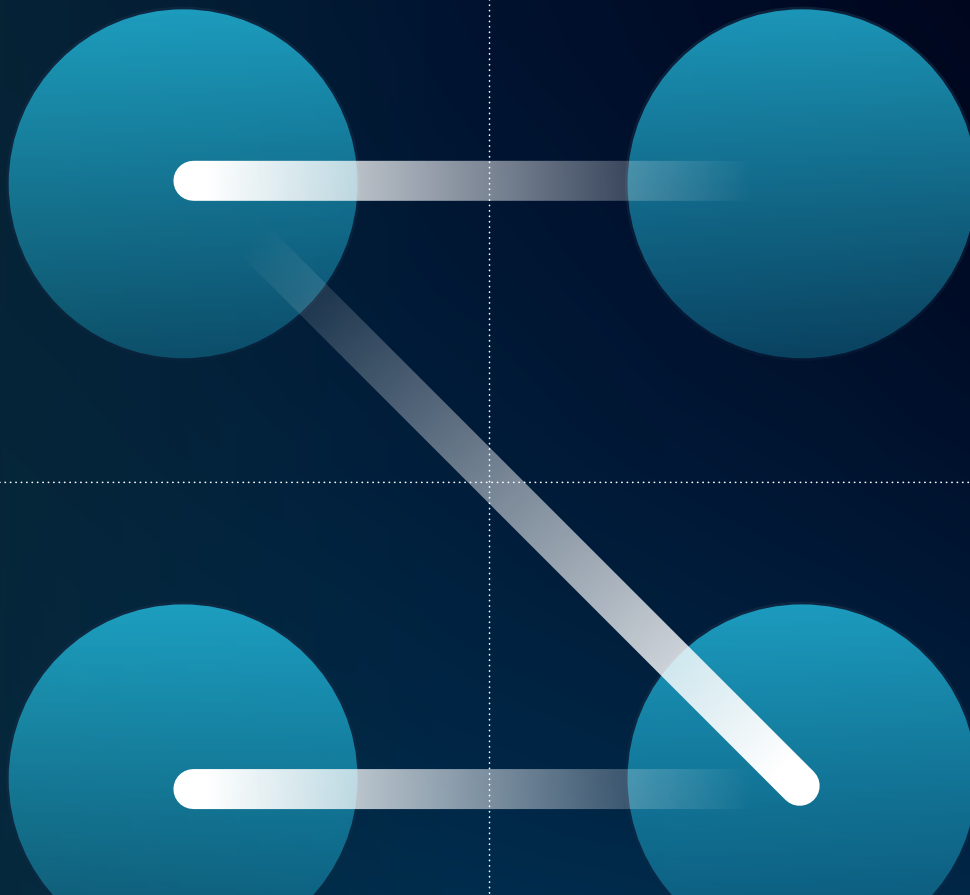




FACT SHEET

Strategic guide for critical infrastructure: how to systematically prioritize your digital sovereignty initiatives

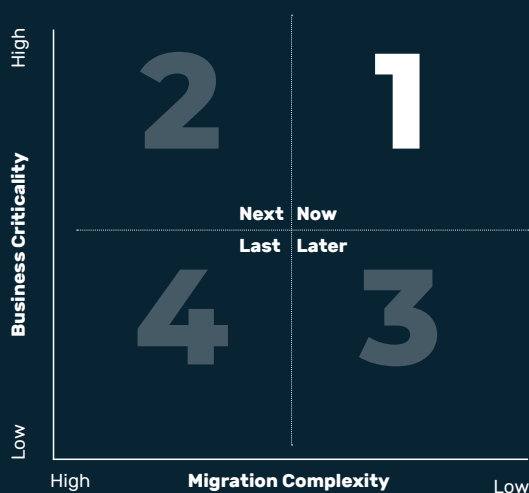


Strategic guide for critical infrastructure: how to systematically prioritize your digital sovereignty initiatives

Against a backdrop of geopolitical uncertainty, growing regulatory requirements, and increased cyber risks, digital sovereignty is becoming a strategic imperative for operators of critical infrastructure and NIS-2-regulated organizations. Digital dependencies in cloud, network, and security services create significant risks for business continuity, compliance, and resilience – especially when key components are operated outside the European legal framework or are dominated by a small number of non-European hyperscalers. Gradually transitioning to European alternatives is therefore not merely a technical measure, but a fundamental decision in favor of greater control, legal certainty, and crisis resilience.

This paper provides a concise strategic guide for efficiently migrating to European solutions, along with practical insights to help you prioritize your sovereignty initiatives. At its core is a decision guideline designed to support executives as a compass and thought starter, highlighting at a glance where sovereignty projects will have the greatest strategic impact.

Decision Guideline: Sovereignty Switch



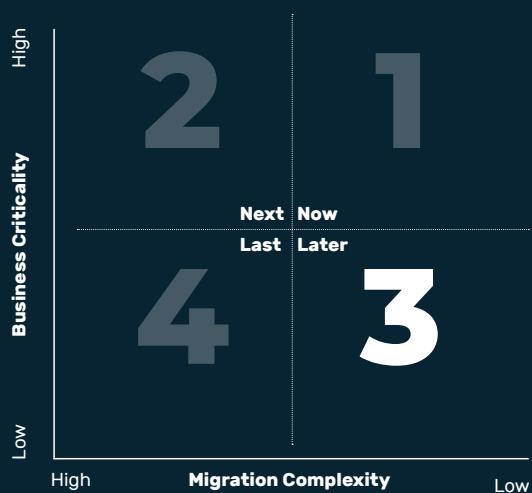
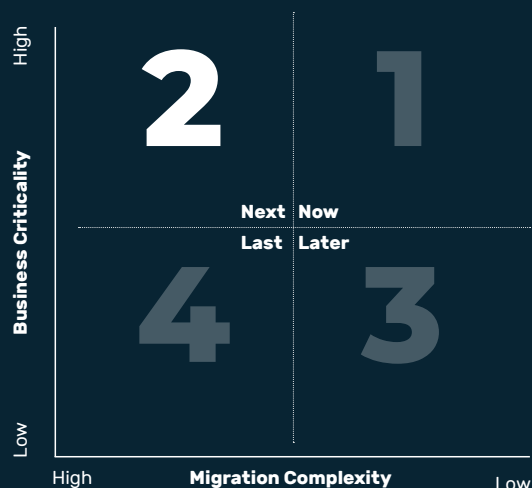
The combination of business criticality and migration effort creates four clear decision scenarios that enable targeted prioritization of all migration projects.

Priority 1 – Now (high criticality, low effort)

This is where sovereignty and compliance gains can be realized particularly quickly and visibly. Systems with high relevance and open interfaces, for which mature EU-based alternatives are available, should be prioritized and migrated as early as possible. The risk and effort remain manageable, while the benefits are substantial – especially where non-European services are currently in use. These projects are ideal lighthouse initiatives and should feature prominently in your roadmap and communication.

Priority 2 – Next (high criticality, high effort)

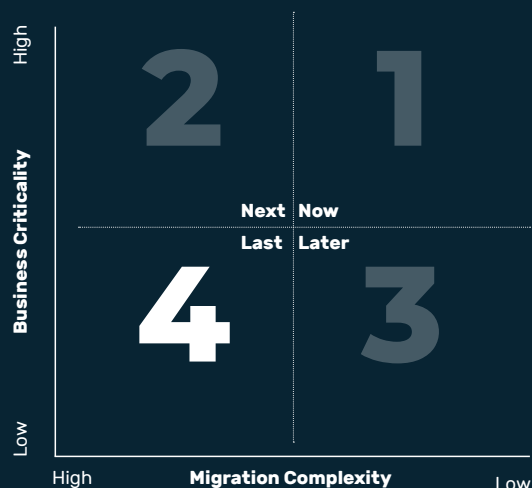
This category covers strategic large-scale projects: a transition is essential for sovereignty and resilience, but requires substantial investment and careful planning. European providers should be involved early through pilot phases and joint development projects to ensure market readiness and seamless integration.

**Priority 3 – Later (low criticality, low effort)**

This area is ideal for pilot projects and low-risk experiments with minimal effort. Less critical, easily replaceable systems allow you to test migration processes, governance, and change management. Successful initiatives build trust in European providers and pave the way for more demanding projects.

Priority 4 – Last (low criticality, high effort)

In this category, waiting is the rational strategy: the migration effort is not proportionate to the expected benefits or sovereignty gains. A transition only becomes relevant when the system needs to be renewed, reaches the end of its lifecycle, or new regulatory requirements arise. Until then, the focus should be on monitoring, evaluating options, and concentrating resources on higher-priority areas.



Criticality and effort: the key factors for migration decisions

The following section outlines the assessment dimensions and success factors that are essential for systematically evaluating the transition to digitally sovereign solutions.



Business criticality

Business-critical solutions and processes must be consistently prioritized and secured based on their impact on core business, revenue, compliance, and resilience. The following are typical drivers of high or very high business criticality; the more strongly these factors apply, the higher the criticality:

- Direct impact on revenue, value creation, or production (e.g. core banking systems, payment transactions, ERP, manufacturing execution).
- Control or protection of business-critical digital processes such as online portals, web applications, and APIs through application security.
- Relevance for reporting and supervisory obligations (e.g., NIS-2, DORA, KRITIS, as well as regulatory and reporting duties towards authorities and supervisory bodies).
- Processing of highly sensitive or personal data with significant regulatory and reputational risk (GDPR, sector-specific frameworks such as B3S).
- Direct importance for security of supply, public services, or critical infrastructure (e.g. energy, healthcare, public administration, financial markets).
- Low substitutability and long recovery times in the event of failure (monolithic systems, proprietary SaaS platforms, complex migration paths).

Determining criticality

A robust information security management system (ISMS) – for example, in accordance with ISO 27001 based on the BSI IT-Grundschutz framework – forms the foundation for a transparent and audit-proof assessment of system criticality. Key elements include the systematic recording and evaluation of all IT systems, services, and software solutions in use, the analysis of their impact on operations, availability, data protection, and statutory reporting obligations, as well as their classification into protection requirement categories based on business impact. The higher the criticality, the stricter the requirements for technical safeguards, documentation, and contingency planning – in particular, digital resilience against supply chain risks and service outages must be ensured on a permanent basis.



Migration complexity

Whether European solutions can be introduced quickly or require a longer transformation project depends primarily on a few key factors.

Data structure and integration with other systems

The more open and accessible a solution is – meaning the easier it is to export data and process it in other systems – the simpler and faster the transition will be. Challenges arise where large, historical datasets with legal retention requirements exist, or where an application is deeply embedded into multiple other systems, workflows, and automations. Standardized formats and interfaces are crucial for an efficient migration. For decision-makers, the following guiding questions are particularly important:

- How is the data structured (formats, tenants, history), and which datasets must be migrated for legal or business reasons?
- Which applications, processes, identity systems, logs/monitoring tools, and data platforms are connected via interfaces?
- Which downstream systems depend on this data, and which upstream systems feed data into the legacy environment?
- Are there standardized export/import mechanisms (APIs, established formats), or are proprietary mechanisms in use?
- What availability and recovery objectives apply, and how long is a parallel operation of legacy and new systems acceptable in terms of data consistency and compliance?

Process and organizational dependencies

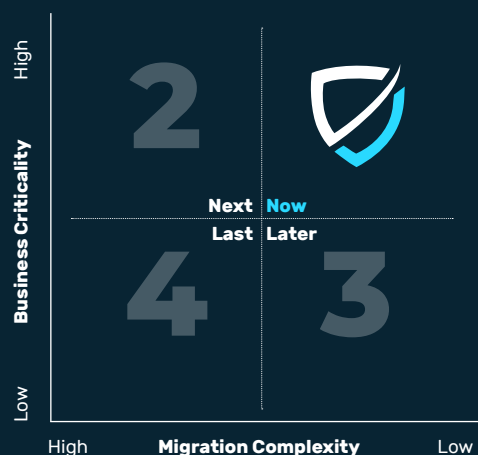
Systems that are closely tied to established workflows, policies, or reporting procedures cannot simply be replaced “on the side”. A transition affects training, roles, responsibilities, and often also audit and reporting obligations. For planning purposes, this means: the more deeply a system is embedded in day-to-day operations or compliance processes, the higher the migration effort. The following guiding questions help to assess this dimension:

- How many employees use the service?
- How frequently is the service used by staff?
- Does the use of the service require dedicated training or enablement?
- Which role and authorization models are currently in place, and which of them would need to be adapted in case of a migration?
- Which specific audit, reporting, or evidence obligations depend on this system (e.g., towards regulatory authorities or external auditors)?



Special case: application and network security

Services such as DDoS protection, CDN, WAF, and bot management are business-critical for the availability and performance of online services. Because they are typically integrated via standardized configurations and delivered as cloud-based solutions that do not require additional hardware or software, switching to European providers can be achieved with comparatively little effort. In most cases, it is sufficient to route traffic through the respective service provider. Despite their high importance, these services therefore enable a rapid and low-risk transition.



Availability of sovereign alternatives

The availability of sovereign, European alternatives determines whether digital sovereignty can be implemented in practice. When selecting and deploying such solutions, what matters is not only the strategic ambition, but also whether these solutions can be used without restriction from both a functional and regulatory perspective. IT decision-makers must therefore consider not only technical capabilities, but also the effort and risk associated with a transition. Where the following criteria are met, a migration to EU-based solutions is realistically achievable in practice:

- **Technical equivalence:** functionality, performance, scalability, quality
- **Price equivalence:** costs for hardware, software, and licensing
- **Service equivalence:** availability (24/7), quality (expert support), SLAs
- **Open standards:** compatibility, open APIs, no lock-in barriers
- **Existing ecosystem:** documentation, native integrations
- **Compliance level:** certifications and audits (GDPR, DORA, NIS-2)

Outlook

The transition to European software solutions is not just a technical migration, but a strategic decision. Digital resilience and sovereignty do not result from symbolic provider changes, but from structured portfolio management: understanding the greatest dependencies, addressing them consistently along the four priority levels, and adopting European alternatives wherever they are already viable today and will secure strategic room for maneuver tomorrow.

Made in Germany



Myra protects what matters. In the digital world.

Would you like to learn more about how our sovereign solutions can strengthen your digital independence, reduce costs, and protect your web applications against malicious attacks? Our experts will be happy to provide individual guidance and develop a tailored solution for your organization. Schedule a non-binding consultation today.

**Cyberattacks are costly.
A conversation with us is not.**

Myra Security GmbH



+49 89 414141 - 345



www.myrasecurity.com



info@myrasecurity.com