IT-GOVERNANCE.NET RESEARCH
FIELD PAPER 01 / JULY 2026

THE EXECUTIVE GUIDE TO DIGITAL SOVEREIGNTY

A practical control framework for critical digital capabilities

Published by it-governance.net, a BusinessFragen OG service
Austria · Germany · Switzerland

EXECUTIVE SUMMARY

Digital sovereignty is the organizational ability to understand, operate, change, move, and if necessary replace critical digital capabilities on acceptable terms. It is not a requirement to avoid cloud services or commercial software. It is a requirement to preserve meaningful choices.

Executives should examine sovereignty across five control domains: data, identity, integration, deployment, and operational knowledge. A platform can be technically modern and still create material dependency when exports are incomplete, interfaces are proprietary, administrators lack access, or the operating model depends on one supplier's undocumented knowledge.

THE FIVE CONTROL DOMAINS

1. DATA CONTROL

The organization knows where material data is stored, how it is classified, which jurisdictions and subprocessors apply, and how complete exports can be produced and verified. Retention, deletion, backup, and recovery obligations are explicit and testable.

2. IDENTITY CONTROL

Critical services integrate with an organization-controlled identity layer. Privileged access, emergency access, role design, logging, and revocation are not dependent on an individual supplier account.

3. INTEGRATION CONTROL

Interfaces are documented, monitored, and governed as products. Business logic does not disappear into opaque point-to-point connections. The cost and technical feasibility of replacing a component are understood before the component becomes operationally critical.

4. DEPLOYMENT AND PORTABILITY

The organization understands where software can run, what infrastructure it requires, and which contractual or technical barriers constrain mig

ration.
Portability is demonstrated with evidence rather than assumed from a product
label or licensing model.

5. OPERATIONAL KNOWLEDGE
Architecture decisions, configurations, runbooks, dependencies, recovery
procedures, and ownership are documented. Internal teams retain enough
knowledge to govern suppliers and make informed decisions.

A PRACTICAL ASSESSMENT

For every critical capability, ask:

- Can we obtain a complete, usable export within an agreed period?
- Can another qualified party operate or migrate the capability?
- Are interfaces, configurations, and decision logic documented?
- Do contracts define transition assistance and deletion evidence?
- Can we recover service without relying on one named individual?
- Do we know the cost, duration, and principal risks of an exit?

RED FLAGS

Warning signals include undefined data extraction costs, supplier-only
administrator access, undocumented integrations, proprietary workflow logic,
missing transition obligations, and architecture decisions justified only by
short-term implementation speed.

GOVERNANCE MODEL

Assign an accountable business owner and a technical owner to every critical
capability. Review dependency risk at architecture, procurement, contract,
release, and renewal gates. Record accepted dependencies explicitly; not all
dependencies are wrong, but material dependencies should be conscious,
priced, and governed.

90-DAY ACTION PLAN

Days 1–30: identify critical capabilities, suppliers, data flows, and owners.
Days 31–60: score the five control domains and test the highest-risk claims.
Days 61–90: agree remediation priorities, contract actions, architecture
changes, and capability-building measures.

THE DECISION PRINCIPLE

Sovereignty is achieved when the organization has credible options and the
capability to exercise them. The objective is not theoretical independence.

It is operational freedom under realistic commercial and technical conditions.