Digital Sovereignty and Governance of Technological Dependence

Theme 2: Governance of IT and IT Management

1 WHAT IS DIGITAL SOVEREIGNTY

Digital sovereignty refers to the ability of an organisation—or a state—to exert effective control over its digital infrastructure, data, and the technologies it depends on. This includes operational control, legal jurisdiction, and strategic autonomy. As organisations increasingly depend on cloud services, foreign platforms, and complex digital ecosystems, the question of who holds that control becomes central to IT governance.

Originally a concept grounded in geopolitics, sovereignty now finds relevance in IT decision-making, risk management, and institutional governance. It is not just about technological independence—it is about ensuring that an institution retains the ability to make informed, compliant, and resilient choices in the digital sphere.

2 LAYERS OF CONTROL AND EXPOSURE

Digital sovereignty spans multiple domains within the IT landscape:

- **Infrastructure Layer:** Concerns over where data is hosted, under what jurisdiction, and who has physical or logical access.
- **Application and Platform Layer:** Reliance on proprietary software, vendor ecosystems, and opaque service models raise risks of lock-in and auditability loss.
- **Governance and Policy Layer:** Compliance with laws such as the GDPR, national security regulations, or EU directives like the Digital Markets Act influences how sovereignty is interpreted and enforced.

This means that sovereignty is not a binary condition but a gradient of control, risk, and governance maturity.

3 INSTITUTIONAL IMPLICATIONS AND SECTORAL RISKS

In the **public sector**, sovereignty relates to democratic legitimacy and accountability. Governments delivering digital services on infrastructures they don't fully control may struggle to guarantee citizen rights and transparency. Outsourcing becomes a political and governance decision.

In the **private sector**, dependency on a few hyperscalers (e.g., AWS, Azure, Google Cloud) introduces concentration risk. Firms face cost increases, integration barriers, and innovation limits due to lock-in. In regulated sectors like banking or pharma, sovereign misalignment can become a compliance issue.

4 GOVERNANCE RESPONSES AND MITIGATION STRATEGIES

Sovereignty-aware governance doesn't mean full self-sufficiency. Instead, it means identifying dependencies, assessing strategic relevance, and establishing governance to manage them. Common strategies include:

- **Contractual safeguards**, such as exit clauses and portability rights.
- **Adoption of open standards and architectures**, reducing interoperability risks.
- **Investment in hybrid or multi-cloud models**, supporting flexibility.
- **Alignment with regulatory frameworks**, including EU initiatives like GAIA-X and the Cybersecurity Act.

These responses mark a shift from reactive IT governance to proactive capability stewardship—treating technology choices as long-term governance decisions.

5 FROM COMPLIANCE TO STRATEGIC AUTONOMY

Digital sovereignty reframes compliance and risk. Instead of seeing regulation as constraint, institutions can use it as a compass for strategic alignment. Governance choices—platforms, data location, system design—are no longer just operational but expressions of institutional identity, responsibility, and resilience.

CxOs like CIOs, CISOs, and architects must interpret and communicate sovereignty trade-offs to boards and regulators. Their roles now intersect with ethics, law, and public accountability—areas once outside "IT governance".

6 CONCLUSION

Digital sovereignty is no longer optional—it defines responsible, strategic IT governance. Whether public institutions uphold legal and democratic mandates or private firms navigate market dependencies and regulations, governing digital infrastructures with awareness and agency is essential.

This sheet presents sovereignty not as technological isolation but as structured management of technological dependence. It highlights layered governance—legal, technical, strategic—and the need to build capabilities for foresight and autonomy in a fast-evolving digital world.

For professionals and students, digital sovereignty encourages shifting from viewing IT systems as operational to understanding them as embedded in power, control, ethics, and institutional purpose. As digital infrastructures become vital to society, their governance becomes inseparable from that of organisations.