

AWS Sovereignty Assessment

Define sovereignty
before you architect it



Evolving regulatory requirements and new cloud models such as the AWS European Sovereign Cloud are raising the bar for digital sovereignty. The Skaylink AWS Sovereignty Assessment helps you identify your organization's needs, assess risks, and develop a well-founded sovereignty strategy for your AWS environment.

Why a Sovereignty Assessment?

Many organizations are facing the same questions:

- Which workloads are subject to regulatory requirements?
- What data must remain within the EU or even within Germany?
- Which requirements are driven by regulation, and which are defined by internal corporate policies?
- Which AWS infrastructure is the best fit for our requirements?

Without a clear requirements baseline, organizations risk either implementing unnecessary controls that increase costs or falling short of compliance due to insufficient safeguards.

What does the assessment include?

Expert review & consulting

Assessment by AWS and sovereignty experts

Executive report & roadmap

Prioritized recommendations and a target architecture for your AWS environment

Personal consultation with sovereignty scan

Analysis of your AWS landscape regarding data residency, governance, encryption, and compliance

Assessment results

- ✓ Sovereignty maturity assessment
- ✓ Risk and gap analysis
- ✓ Architecture/infrastructure recommendations
- ✓ Prioritized actions
- ✓ Executive-ready results report
- ✓ Readiness check for the AWS European Sovereign Cloud

AWS Sovereignty Assessment

Define sovereignty
before you architect it



Our 7-Domain Sovereignty Framework

The assessment is based on a structured framework that examines the three core pillars of digital sovereignty: compliance, control, and continuity.

Understanding the context

D1 – Business objectives & requirements

- Strategic drivers
- Critical business processes
- Non-negotiable requirements
- Stakeholders and responsibilities

D2 – Regulations & jurisdiction

- Industry-specific requirements
- Compliance and legal requirements
- Jurisdiction and data sovereignty

D3 – Data classification

- Data inventory
- Critical data sets
- AI and training data
- Data governance

Evaluating the pillars of sovereignty

D4 – Data sovereignty & protection

- Data residency
- Data transfers
- Encryption
- Encryption key management

D5 – Resilience & independence

- Disaster recovery
- Provider dependencies
- Exit strategies
- Operability in view of regulatory restrictions

D6 – Operational sovereignty & access

- Access models
- Roles and responsibilities
- Jurisdictional requirements
- Operating and support models

Sustainable governance

D7 – Continuous assurance

- Compliance monitoring
- Auditability
- Evidence management
- Drift detection
- KPIs and continuous improvement

Questions?

We're happy to help:

✉ awspartner@skaylink.com

