schwarz digits

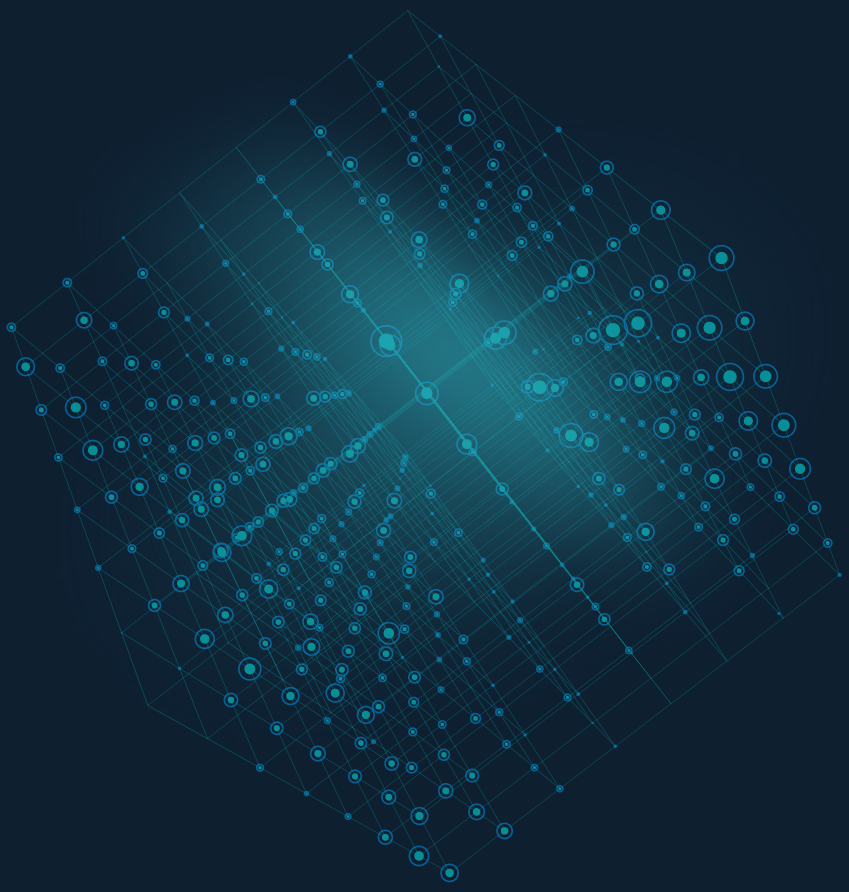
STACKIT

Framework and Criteria Specification

THE OPERATIONAL ENGINE: MAKING DIGITAL SOVEREIGNTY MEASURABLE, COMPARABLE AND MANAGEABLE.

www.stackit.com/en/es3

Table of Contents



1. Objectives and Guiding Principles

The Sovereignty Maturity Level (SML) Framework is an auditable assessment framework designed to assess the digital sovereignty of IT services.
In this context, digital sovereignty is understood as the "ability to walk away from the table at any time" – meaning the ability to terminate or migrate the use of a service without unacceptable dependencies and risks (e.g., legal, technical, operational, or within the supply chain).

The framework follows three guiding principles:

- **Auditability:** Assessments must be evidence-based, comprehensible, and reproducible.
- **SML classification:** SMLs are assigned based on defined mandatory controls per level.
- **Comparability:** Results should be comparable between services/providers and over time.

The SML Framework encompasses the structure of the assessment (Divisions, Control Objectives, Controls, Questions, Evidence) as well as the basic logic of the evidence-based evaluation. The concrete SML classification logic, particularly the assignment of controls to SMLs (Initial, Managed, Advanced, Future-Proof), takes place outside the framework via a separate mapping structure.

2. Scope and Object of Assessment

The SML Framework assesses a specific IT service within a defined context (e.g., service type, deployment model, utilized platforms, jurisdictions, contractual and operational models). The object of assessment is therefore always a combination of the client-facing service and the service provider.
Not within the scope of this document:

- The complete definition of all controls and questions per division. These are available in separate documentation.
- The formal attestation model, as well as liability and independence regulations, are not within the scope of this document. However, the basic logic of the SML classification is described; the concrete allocation of controls to SMLs takes place in a separate mapping table outside the framework.
- Technical automation (e.g., continuous assessment), unless described as a future option. Although it is not within the scope of this document, it will be implemented in the form of a dedicated SML tool.

In addition to the service and the service provider, the assessment also includes the relevant underlying services upon which the service is based. Before an assessment begins, the service to be evaluated must be clearly classified.
The classification comprises:

- Service Name
- Service Provider
- Service Type

The Service Type must be defined and determines the applicability of the controls. The classification is binding for the entire assessment. The goal is a consistent, comprehensible, and comparable assessment of services.

2.1 Service Types

The Service Type describes the nature of the service under consideration (e.g., IaaS, PaaS, SaaS, Managed Service, AI Service). The Service Type serves exclusively to determine the applicability of controls and questions. Depending on the Service Type, a control can be:

- Applicable (to be assessed)
- Not applicable (N/A)

The Service Type has no influence on the assignment of a control to the Control Scope, the assessment of dependencies, or the calculation of SMLs or maturity ceilings.

2.2 Control Scope

The Control Scope describes the level at which a control is implemented and assessed. The SML distinguishes between three levels:

Scope	Abbreviation	Description
Underlying Service	US	External cloud or platform services (e.g., STACKIT) on which the service is based..
Service Provider	SP	Organization that develops, operates, and is responsible for the service.
Client-facing Service	CFS	The specific service that is provided to the customer.

Design principles:

- Controls are assigned to exactly one of these levels.
- A Control Objective can contain controls across multiple levels.
- The Control Scope defines responsibilities exclusively and is independent of the Service Type.

The aim of this differentiation is to provide clear responsibilities, prevent duplicate audits, transparently map dependencies, and enable an auditable assessment of inherited capabilities.

To reduce redundant assessments and ensure a consistent evaluation, the SML framework utilizes an inheritance principle.

Controls are treated differently depending on their Control Scope:

- Controls at the Service Provider (SP) level can be assessed once and inherited across multiple services.
- Controls at the Underlying Service (US) level are not implemented by the service providers themselves, but are covered via suitable evidence (e.g., certificates, audit reports). These controls are considered "inherited" provided that corresponding evidence is available.

3. Framework Components and Terms

The framework is hierarchically structured and follows a clear logical progression:
Dimension → Control Objective → Control → Question → Evidence

3.1 Division

A Dimension describes a thematic area of digital sovereignty. It forms the highest structural level of the framework and groups multiple Control Objectives.

ID	Properties	Examples
SML x	■ Strategic thematic area ■ Stable over a long period of time ■ Contains multiple Control Objectives	**SML 3: Data Sovereignty** Description: Data sovereignty measures the control parameters established over data assets throughout their lifecycle.

3.1.1 SML Dimensions

The SML dimensions are based on the eight sovereignty objectives of the EU Cloud Sovereignty Framework. Each dimension consists of multiple Control Objectives to define the goals within that dimension.

ID	Dimension	Description
SML 1	Strategic	Strategic sovereignty evaluates the corporate governance architecture, ownership dependencies, and long-term continuity planning of the service provider. This dimension covers criteria assessing the explicit designation of governance authority, the transparency of corporate ownership structures to identify potential foreign influence, formal corporate commitments to localized control, and executive-level oversight regarding service substitution and exit readiness.
SML 2	Legal & Jurisdictional	Legal and jurisdictional sovereignty evaluates the legal frameworks, geographic processing boundaries, and regulatory environments governing the services. This dimension covers criteria assessing the corporate bodies and data processing locations, contractual clarity regarding applicable laws, and legal protection mechanisms against extraterritorial third-party claims or conflicting access requests.
SML 3	Data	Data sovereignty measures the control parameters established over data assets throughout their lifecycle. This dimension covers criteria assessing customer-controlled access management models, cross-environment data portability, purpose-bound usage constraints, and structural configurations for data integrity and long-term cryptographic resilience.
SML 4	Operational	Operational sovereignty evaluates the capacity to run, maintain, and support services independently of external or unilateral provider controls. This dimension covers criteria assessing the structural allocation of day-to-day operational responsibilities, the restriction and auditing of privileged administrative access, autonomous incident response and disaster recovery architectures, and collaborative change management procedures.
SML 5	Supply Chain	Supply chain sovereignty measures the geographic composition, component tracking, and systemic resilience of the third-party ecosystem supporting the service. This dimension covers criteria assessing the transparency of subprocessors and software components (SBOM), vendor risk governance frameworks, critical dependency mitigation strategies, the downstream flow-down of sovereignty criteria to subcontractors, and the viability of alternative vendor substitution workflows.

ID	Dimension	Description
SML 6	Technology	Technology sovereignty assesses the openness, auditability, and physical or logical layout of the underlying technical stack. This dimension covers criteria assessing the deployment of virtual and physical infrastructure within approved geographic boundaries, the adoption of open standards to mitigate proprietary vendor lock-in, architectural transparency for security auditing, and cross-platform component portability.
SML 7	Security & Compliance	Security & compliance sovereignty evaluates the isolation, administrative control, and auditability of security configurations and compliance mechanisms. This dimension covers criteria assessing least-privilege identity and access control architectures, lifecycle data encryption implementations, customer visibility into security logs or event monitors, and technical isolation workflows for high-risk or sensitive operational tasks.
SML 8	Environmental Sustainability	Environmental sustainability evaluates the long-term operational resilience, resource dependency profiles, and metric transparency of the service regarding environmental constraints. This dimension covers criteria assessing infrastructure energy dependency profiles, critical hardware and cooling supply chain exposures, architectural planning for environmental risk factors, and the tracking and disclosure of sustainability indicators.
SML 9	AI	This dimension evaluates the organizational oversight, system clarity, and independent control of artificial intelligence solutions. It covers criteria assessing corporate accountability models, system explainability, operational reliance on external software providers, and the protection of training data and internal model components against unauthorized access.

3.2 Control Objective

A Control Objective describes a goal within a dimension that must be achieved to ensure digital sovereignty.

ID	Properties	Examples
SML x.CO y	■ Describes a target state ■ Technology-neutral ■ Implemented through multiple controls	**SML 3.CO 1** Customers retain sovereign control over access to their data.

3.3 Control

To ensure a structured and comprehensive implementation of Control Objectives, Controls are organized along three implementation levels:

- **Level 1: Contractual** – Contractual regulations and assurances, e.g., service agreements, SLAs, legal arrangements.
- **Level 2: Governance & Operations** – Organizational, procedural, and operational implementation, e.g., organizational responsibilities, policies and procedures, operational processes and controls.
- **Level 3: Technical** – Technical implementation and system configuration, e.g., technical security measures, system configurations, automation.

The following design principles apply:

- Each control is assigned to exactly one implementation level (Contractual, Governance & Operations, or Technical). A mixture of multiple levels within a single control is not permitted. If a requirement affects multiple levels, it is split into separate controls. The goal is clear auditability, unique assignment, and consistent evaluation.
- Application is optional: Not every level must be mapped for every Control Objective. Controls should only be defined where they make functional sense; individual levels can be omitted (e.g., no technical controls).

ID	Properties	Examples
SML x.CO y.C z	■ Concrete measure ■ Implementable ■ Auditable	**SML 3.CO 1.C 11** Contracts ensure that the customer retains sole authority to define, grant, modify, and revoke access rights to their data.

3.4 Questions

Questions are binary audit questions ("Yes," "No," or "N/A") used to verify the implementation of a control. Each question addresses exactly one concrete requirement and is formulated in a way that is uniquely verifiable and derives a specific piece of evidence.Different variations of implementation are mapped either through multiple questions or through separate controls. The goal is a clear, objective, and auditable assessment based on individual, clearly verifiable criteria.

Design principles for Questions:

- **Uniqueness:** Each question tests exactly one fact.
- **Binary Assessment:** Questions must be phrased so they can only be answered with "Yes," "No," or "N/A".
- **Auditability:** Each question must be verifiable through concrete evidence.
- **Selectivity:** Questions must not overlap.
- **Minimalist Principle:** Only as many questions are defined as necessary.

Questions are used exclusively for the evidence-based assessment of individual controls. They are not assigned directly to SMLs.

3.5 Evidence

Evidence is the proof used to substantiate an answer to a question. It must be specific, verifiable, and directly assignable to the control. General statements such as "documentation available" or "process exists" are insufficient.
Permissible evidence types include:

- Contracts or legal agreements
- Policies and procedural documentation
- Technical configurations or system extracts
- Audit reports or certifications
- Architecture diagrams

The evidence must enable an independent third party to fully comprehend the assessment.

Properties	Examples
■ Always 1:1 to a question ■ Document-based or technical ■ Auditable	■ Architecture diagram ■ Configuration extract ■ Policy document ■ Audit report ■ Certification

3.6 Four Sovereignty Maturity Levels

An SML is assigned based on a control-level mapping table to the four Sovereignty Maturity Levels Initial, Managed, Advance, and Future-Proof. This mapping table defines which controls must be fulfilled for a specific SML. The SML mapping is thus not a component of the list of criteria itself, but a component of the SML classification logic. Classification is based on the principle that an SML is only achieved when all of its required controls are fulfilled. The lowest-level unfulfilled mandatory control dictates the maximum level that can be achieved.

SML	Description
Initial	**Non-standardized; strong dependencies and limited verifiability.** High dependency on external actors cannot be ruled out for the organization and its services. Strategic actions evidence low awareness of digital sovereignty. Business continuity and service restoration following geopolitical disruptions are reactive and not formalized. Digital dependencies are not managed and are not embedded in risk management.

SML	Description
Managed	**Basic capability present; partially documented/rule-based; verification generally possible.** The organization has developed a basic awareness of digital dependencies and is beginning to systematically record them. Critical dependencies on external actors are identified and documented in risk management, but only some are actively managed. Initial contingency and restoration plans exist for the most important services, enabling a structured, though not yet fully tested, response in the event of geopolitical disruptions. Strategic considerations regarding digital sovereignty selectively influence procurement and architecture decisions, but are not yet consistently embedded in corporate governance.
Advanced	**Structured implementation; processes/mechanisms established; consistent and verifiable; low dependencies.** Digital sovereignty is anchored as a strategic objective in corporate management and is systematically implemented across procurement, architecture, and operations. The organization possesses active dependency management that continuously evaluates external providers and maintains at least one alternative sourcing option or a documented migration path for all business-critical services. Restoration and continuity plans are formalized, regularly tested, and explicitly account for geopolitical and regulatory scenarios. Data is predominantly processed within the EU/EEA.
Future-Proof	**Optimized/industrialized; high level of standardization and automation where applicable; robust exit and control capabilities** The organization has achieved near-complete digital autonomy. Core processes and business-critical services run on self-operated or sovereign-controlled infrastructure based on open standards, open-source components, and trustworthy European supply chains. Remaining external dependencies are deliberate strategic choices, fully transparent, and substitutable at any time with proven alternatives. The organization is capable of maintaining the operation of all critical services without significant restriction, even during severe geopolitical disruptions, sanction regimes, or the loss of individual providers. Digital sovereignty is an integral part of corporate culture, governance structures, and innovation strategy, and the organization actively drives the development of sovereign digital ecosystems in Europe.

3.7 Approved Jurisdictions List (AJL)

Approved Jurisdictions List is maintained based on the STACKIT "Legal Assessment for third-party countries outside the EU", including Core Jurisdiction (EU/EEA and Switzerland) as well as Extended Jurisdiction (UK, Canada, Israel, Andorra, and Japan). This list is subject to future updates and expansions.

4. Assessment Logic

4.1 Assessment of Questions and Controls

The assessment is performed based on the provided evidence and answers to the associated questions.

- Questions are designed for binary assessment: "Yes," "No," or "N/A"
- A control is considered:
  - **Fulfilled:** When all questions relevant to the assessment are answered with "Yes".
  - **Not fulfilled:** When at least one question relevant to the assessment is answered with "No".
- Questions answered with "N/A" are only considered if they are objectively not applicable and appropriately justified. They must not result in a control being considered fulfilled without substantive proof.
- Individual questions or controls are not assigned numerical scores or weighted.

4.2 Assessment at Control Objective and Division Level

A Control Objective describes the functional goal to be achieved within the assessment. Whether a Control Objective is considered fulfilled or not fulfilled is determined based on those controls defined as required for the respective SML according to the separate mapping table.

The following rules apply to the assessment:

- A Control Objective is fulfilled for a specific SML if all of its required controls are fulfilled.
- A Control Objective is not fulfilled for a specific SML if at least one of its required controls is not fulfilled.
- Controls assigned to a Control Objective that are not defined as required for the respective level remain unconsidered for determining fulfillment of that level.

A division can be viewed as fulfilled if all relevant Control Objectives of this division for the level under consideration are fulfilled. The division perspective serves primarily transparency purposes and the contextual classification of strengths and weaknesses.

4.3 Determining the SML

To achieve a specific SML, all controls defined as mandatory for that level must be fulfilled. The maximum achievable SML is determined by the lowest level at which Control Objectives are not fulfilled due to at least one required control being unfulfilled.

Fulfilling other controls cannot compensate for a missing requirement. This logic ensures that critical requirements cannot be offset by other strengths.

4.4 Limitation by Underlying Services

The Control Scope defines the level at which a control is implemented and assessed. Controls with the scope Underlying Service (US) are not fulfilled by the service providers themselves, but are factored in based on the assessment result of the underlying service. The result of a US control does not apply globally to other controls, but exclusively to the specific Control Objective to which the control is functionally assigned.
Therefore, the following applies with respect to the assessment:

- Each control is assessed independently of other controls.
- An unfulfilled control of a US does not automatically cause other controls to be considered unfulfilled.
- The impact of an unfulfilled US control lies exclusively in it being factored in as unfulfilled in the evaluation of its associated Control Objective.

Whether an unfulfilled US control causes a Control Objective to be unfulfilled for a specific SML is determined by the separate mapping table. What matters is whether this control is defined as required for the respective level. This logic ensures that controls are assessed independently of one another, the impact of underlying services is functionally correctly assigned to the respective Control Objective, and the SML classification remains comprehensible and auditable. The assessment result of a control with the scope “Underlying Service” is fully adopted from the assessment of the underlying service and is not influenced by the service provider.

5. SML Framework Catalogue

The framework catalogue is available for download at this link. Each row represents a single assessment question (Question) within a specific context (Dimension/Control/Service Type). In addition to the framework, a separate SML mapping table is maintained. This is used exclusively for the SML classification logic and defines which controls are mandatory or optional for specific SMLs. The mapping table is not part of the framework structure itself, but is an independent, versioned assignment table.

Column	Purpose/Content
Dimension ID	Unique identifier of the domain in the framework (e.g., SML 1). Used to group all Control Objectives within a domain.
Dimension	Name of the domain or sovereignty area (e.g., Strategic, Legal & Jurisdictional, Data & AI).
Dimension Description	Description of the functional scope of the division and which aspects of digital sovereignty are assessed.
Control Objective	Functional goal to be achieved within the division. Describes the desired state, but not the concrete implementation.
Sovereignty Contribution	Explanation of why this control contributes to digital sovereignty and what concrete effect it has.
Control ID	Unique identifier of a control (e.g., SML 1.CO 1.C 1). Uniquely assigns the control to a Control Objective.
Control	Description of the concrete organizational or technical measure by means of which the Control Objective is implemented.

Column	Purpose/Content
Control Scope	US/SP/CFS
Service Type	Indication of which service types the control is relevant for (e.g., IaaS, PaaS, SaaS, Managed Service, AI Service).
Underlying Service	Reference to the external service used (e.g., from STACKIT).
Question ID	Unique identifier of the assessment question (e.g., SML 1.CO 1.C 1.Q 1).
Question	Concrete assessment question to evaluate the control. Must be as clear as possible and structured for a binary response.
Evidence Type	Type of expected proof (e.g., documentation, architecture diagram, contract, configuration, interview).
Evidence Example	Example of potential evidence or expected artifact.
Answer	Result of the assessment (“Yes”, “No”, “N/A”).
N/A Reason	Justification for why a question is not applicable.
Evidence Provided	Reference, link, or ID to the evidence actually submitted.
Assessor Comment	Comment or justification by the assessor regarding the evaluation.

6. Revision and Versioning

A process has been defined for the creation, maintenance, and annual revision of the list of criteria and the SML mapping. The objective is to ensure the quality of the SML framework while simultaneously enabling a response to technological and regulatory changes. Feedback is collected throughout the year from marketplace partners and internal and external experts. The further development and versioning follows an annual cycle.

Versioning follows the pattern [YEAR].[RELEASE].[PATCH]:

- **Year:** Annual major update with potentially new requirements.
- **Release:** Intra-year functional additions (without increasing the audit burden).
- **Patch:** Correction of editorial errors.

To maintain continuity, existing certifications remain valid until their individual expiration date (usually 12 months).