

# SLA Governance Framework Playbook

for Multi-Provider Cloud-Edge Continuum  
Environments



**Version 1.0 (November 24th, 2025)**

ISBN: 978-3-9828074-0-9

**Published by**

eco – Association of the Internet Industry (eco – Verband der Internetwirtschaft e.V.) Lichtstrasse 43h, 50825 Cologne, Germany

**Copyright © eco Association on behalf of FACIS - funded by the German Federal Ministry for Economic Affairs and Energy (IPCEI-CIS)**

Image Source: Adobe Stock

This work is licensed under the Creative Commons Attribution 4.0 International License. To view a copy of this license, visit <http://creativecommons.org/licenses/by/4.0/> or send a letter to Creative Commons, PO Box 1866, Mountain View, CA 94042, USA



**Comissioned author:**

**Fieldfisher Partnerschaft von Rechtsanwälten mbB**

Amerigo-Vespucci-Platz 1

20457 Hamburg

Germany

Point of contact: Oliver Süme, Dr. Bahne Sievers & Melanie Ludolph

E-mail: [oliver.sueme@fieldfisher.com](mailto:oliver.sueme@fieldfisher.com)

Website: <https://www.fieldfisher.com/de-de/locations/germany>

**Peer reviewed by the following persons in October 2025:**

- Andreas Weiss, eco – Association of the Internet Industry
- Thomas Niessen
- Yannick Heß, Technical University of Munich
- Prof. Dr. Sebastian Lins, University of Kassel

## Executive Summary

This SLA Governance Framework Playbook (hereafter „Playbook“) provides a practical framework for designing, implementing, and enforcing Service Level Agreements (SLAs) in complex, multi-provider cloud and edge environments. Its goal is to enable consistent and transparent governance across digital ecosystems involving multiple providers, layered platforms, and diverse data and cloud services.

It serves as a toolkit for technical leads, legal advisors, service architects, and vendor managers by offering a shared reference to translate business needs into measurable service commitments.

The Playbook is aligned with the FACIS Taxonomy for SLAs, which defines the conceptual foundation for SLA design and governance. It builds on four main elements:

1. Foundation – establishes scope, terminology, and the relationship between actors;
2. Service Level Objectives (SLOs) – defines measurable commitments such as availability, performance, or support responsiveness;
3. Monitoring – specifies how SLOs are verified through Service Level Indicators (SLIs) and metrics;
4. Enforcement – describes remedies, escalation paths, and rights in case of SLA violations.

The modular architecture allows combining a stable base SLA with attachable annexes for services, sectors, or jurisdictions, thereby supporting both new procurements and modernization of existing contracts.

Within multi-provider environments, the Playbook addresses two main coordination approaches:

- Entangled Supply Chains – this is the traditional model, where a lead provider manages multiple sub-providers and must cascade obligations downward to avoid “blame chains”.
- Federated Ecosystems – this is the emerging model and the main focus of this Playbook, where independent providers interoperate and share data or services under harmonized, jointly governed SLAs.

Key challenges addressed include responsibility allocation, cross-provider risk management, and end-to-end observability of service guarantees.

This Playbook also promotes the automation and machine-readability of SLAs as a future direction for efficient governance and compliance.

# Table of Contents



<b>Executive Summary</b> .....	<b>1</b>
<b>1. Introduction</b> .....	<b>1</b>
1.1 What are we talking about? .....	1
1.2 The Playbook .....	1
<b>2. SLA Governance in a Federated, Multi-Provider Environment</b> .....	<b>2</b>
<b>3. Multi-Provider Governance Models</b> .....	<b>3</b>
3.1 Definition and Purpose .....	3
3.2 Overview of Governance Models .....	3
3.3 Lead Service Provider Model (hub-and-spoke) .....	3
3.4 Dedicated SLA Broker/Central SLA Manager Model .....	4
3.5 Decentralized/Peer-to-Peer Model .....	4
3.6 Implications for Transition and Continuity .....	5
<b>4. Roles and Responsibilities</b> .....	<b>6</b>
4.1 Context: Multi-Provider Provisioning Scenarios .....	6
4.2 Actors and Stakeholders .....	6
4.3 Cross Provider Coordination .....	7
4.4 Responsibility Allocation .....	7
4.5 Liability and Risk Allocation .....	8
<b>5. SLA Structure and Core Components</b> .....	<b>9</b>
5.1 Core Structure .....	9
5.2 Hierarchy of SLA Commitments .....	9
5.3 Design and Documentation Guidance .....	10
5.4 Practical Examples .....	10
5.5 Integration with Sector-Specific Annexes .....	10
<b>6. SLA Content and Design Guidance</b> .....	<b>11</b>
6.1 Purpose and Relation to the FACIS Taxonomy for SLAs .....	11
6.2 Design Approach .....	11
6.3 Example Service Level Objectives .....	11
6.3.1 Availability .....	11
6.3.2 Performance .....	12
6.3.3 Customer Support .....	12
6.3.4 Maintainability .....	13
6.3.5 Change Management .....	13
6.3.6 Data Protection and Privacy .....	13
6.3.7 Information Security .....	14
6.3.8 Reliability and Operational Resilience .....	14
6.4 Escalation Paths .....	14
6.5 Remedies and Penalties .....	14
6.6 Relationship to the General Terms and Complementary Agreements .....	14

<b>7. Monitoring and Reporting</b>	<b>15</b>
7.1 Purpose	15
7.2 Real-Time and Periodic Monitoring	15
7.3 Data Sources and Verification	15
7.4 Reporting Requirements	15
7.5 Dashboards and KPIs	15
7.6 Audit and Verification Rights	16
7.7 Governance Reviews	16
7.8 Integration with Other Frameworks	16
<b>8. Using This Playbook in Practice</b>	<b>17</b>
8.1 Purpose	17
8.2 Typical Use Cases	17
8.3 Implementation Steps	17
8.4 Governance Integration	17
8.5 Maintenance and Version Control	17
8.6 Continuous Improvement	18
8.7 Future Extension – SLA Repository	18
<b>9. Annexes</b>	<b>20</b>
Annex A: Generic SLA Templates	20
Annex B: Example Metrics and Dashboards	31
Annex C: Glossary of Terms	33
Annex D: Legal and Regulatory Frameworks	36
Annex E: Sector-Specific SLA Adaptation – Methodology and Example	37

## List of Tables

Table 1 – Overview of Governance Models	3
Table 2 – Example Responsibility Allocation Matrix	8
Table 3 – Example taxonomy dimensions in SLA clauses	10
Table 4 – Service Provider and Services	21
Table 5 - Interdependencies	22
Table 6 - Interdependencies	27
Table 7 – Example SLO Categories and Metrics	31
Table 8 – Applicable Frameworks	36
Table 9 – Example	37



## 1.1 What are we talking about?

Digital services today are no longer confined to isolated cloud platforms. They span distributed infrastructures across cloud, edge, and connectivity layers – often operated by multiple independent providers. In such ecosystems, reliable coordination, predictable performance, and joint accountability become critical. For example, in a smart-city mobility scenario, vehicles, roadside units, and edge computing nodes must interact within milliseconds to manage traffic safely. Meeting a latency objective of below 100 ms requires seamless cooperation among telecom operators, cloud providers, and edge service platforms. Determining who is responsible when such targets are missed is complex – and this is precisely where joint, multi-provider SLAs are needed.

While traditional SLA models evolved within entangled supply chains managed by a single lead provider, modern digital ecosystems increasingly rely on federated cooperation among autonomous service providers. These federated constellations require explicit governance of interfaces, harmonized measurement methods, and coordinated accountability mechanisms.

These challenges illustrate the need for federated and transparent SLA governance frameworks that can link business outcomes with technical guarantees across multiple service domains – which is the central focus of this Playbook.

## 1.2 The Playbook

The purpose and scope of this Playbook is to provide a practical, modular framework for designing, negotiating, implementing, monitoring, and enforcing Service Level Agreements (SLAs) across complex, federated digital ecosystems that span cloud and edge environments.

It aims to enable consistent, transparent, and enforceable governance across multiple providers, layered platforms, and data services.

The Playbook supports both new procurements and the modernization of existing contracts by offering structure, model language, and measurement guidance applicable across sectors and projects.

Its target audience includes technical leads, legal advisors, service architects, project teams, and vendor managers who require a shared, plain-language reference for translating business outcomes into measurable service commitments.

Readers should use this document as a modular toolkit: start with the base structure, add service-specific and sector-specific annexes as required, and apply the monitoring and reporting practices to operationalize the agreed terms. Each section builds on the previous one so that a multidisciplinary team can move from intent to enforceable obligations without losing clarity or accountability.

This Playbook builds on the FACIS Taxonomy for SLAs, which defines the conceptual foundation and terminology used throughout. It provides practical guidance on how to implement the key building blocks defined in FACIS Taxonomy for SLAs – from Service Level Objectives (SLOs) and Service Level Indicators (SLIs) to monitoring and remedying processes – ensuring alignment between legal design and operational execution.

**Note on Terminology:** For clarity and consistency, key terms used throughout this Playbook are defined in Annex C (Glossary of Terms). Readers unfamiliar with specific technical or legal terminology may wish to consult it when first encountering unfamiliar expressions.

# SLA Governance in a Federated, Multi-Provider Environment



**Definition and Rationale** – In a decentralized service ecosystem, SLA governance means establishing the policies, contractual language, measurement methods, and enforcement mechanisms that keep service quality predictable when multiple independent parties contribute to a shared outcome. This Playbook applies to both entangled supply chains – where a lead provider manages multiple sub-providers – and federated ecosystems in which independent providers interoperate on demand under separate agreements. (See also the FACIS Taxonomy for SLAs, Section 2, for the underlying conceptual model.)

The rationale is straightforward. Without a common vocabulary and aligned measurement rules, fragmented responsibilities, divergent compliance regimes, and limited cross-provider visibility make it difficult to attribute faults, remedy harm, or improve performance consistently.

**Key Challenges and Objectives** – The key challenges addressed by this Playbook are:

- the allocation of responsibilities at the points where services or providers interact,
- the alignment of compliance and certification requirements across jurisdictions,
- the management of cross-provider risk and cascading failures, and
- the creation of end-to-end visibility into service guarantees across all contributing providers.

The objectives of SLA governance in federated and multi-provider environments are to:

- define clear ownership for each obligation and ensure that accountability can be demonstrated,
- cascade critical duties and measurement obligations to sub-providers where feasible,
- implement observability that allows consistent measurement and attribution across all layers, and
- tie remediation to business impact rather than narrowly defined technical thresholds.

Together, these objectives create the foundation for predictable, enforceable, and transparent performance management in decentralized digital ecosystems.

**Governance Principles** – Effective SLA governance is grounded in five guiding principles:

1. **Transparency** – requires plain definitions, published metrics, and auditable records across all providers and service layers.
2. **Modularity** – ensures a stable base contract with annexes for services, sectors, and jurisdictions, aligned with the structure of the FACIS Taxonomy for SLAs.
3. **Proportionality** – scales obligations and reporting depth to the level of risk, criticality, and control each provider holds.
4. **Enforceability** – mandates measurable Service Level Objectives (SLOs), practicable cure periods, and credible remedies that are proportionate to business impact.
5. **Data Minimization** – limits the collection and retention of data to what is necessary for service delivery, security, and compliance purposes.

These principles ensure that governance models remain both legally defensible and operationally executable, bridging the gap between contractual language and day-to-day service management.

# Multi-Provider Governance Models



## 3.1 Definition and Purpose

In complex service ecosystems, the governance model defines how multiple providers coordinate responsibilities, share information, and ensure that end-to-end obligations remain enforceable. While Section 2 describes the rationale for SLA governance, this section classifies the main coordination archetypes and compares their respective strengths, limitations, and implications for transition and continuity. Selecting and documenting the applicable governance model at the outset of a program avoids ambiguity during later SLA negotiations, particularly when accountability or fault attribution extend across organizational boundaries.

## 3.2 Overview of Governance Models

Multi-provider ecosystems can be organized under three principal governance models. Each determines how monitoring, reporting, and escalation are coordinated.

Within federated and multi-provider environments, the Dedicated SLA Broker and Decentralized/Peer-to-Peer models are of particular relevance. They reflect the principles of cooperation, transparency, and shared accountability that underpin federated cloud and edge ecosystems. Both models enable providers to align service measurement and governance without central dependency, supporting dynamic composition of services and joint compliance management. The Lead Provider model remains an established option for traditional or highly regulated environments, but emerging federated architectures increasingly rely on neutral brokerage or peer-based coordination to achieve interoperability and resilience across multiple autonomous providers.

The detailed operational implications of each model are described in Section 4.3 Cross-Provider Coordination.

## 3.3 Lead Service Provider Model (hub-and-spoke)

In the lead service provider model, the customer contracts with a single prime supplier – the Lead Provider – who integrates and manages several sub-providers. The Lead Provider acts as the central governance and accountability point: it consolidates performance data, orchestrates incident and change management, and ensures that all sub-providers meet the service levels and compliance obligations defined in the master SLA. Sub-providers are bound through back-to-back commitments that mirror the customer-facing terms, allowing end-to-end accountability through one contractual interface.

Operationally, the Lead Provider establishes a unified measurement and reporting framework covering all service layers. Common definitions, metrics, time windows, and exclusions apply across the chain. The Lead Provider provides consolidated dashboards and periodic SLO reports, coordinates incident response through a single escalation channel, and delivers root-cause analyses and service-improvement plans when thresholds are not met. This model gives the customer clarity and simplicity but also concentrates dependency and information control in one entity.

To mitigate opacity, the SLA should require the Lead Provider to maintain an auditable register of sub-providers, disclose material changes, and provide performance data and compliance evidence upon request. Audit and inspection rights – whether document based or tool based – help preserve transparency without undermining operational security. Remedies follow the principle of “one counterparty, one outcome”: the customer enforces credits or other remedies against the Lead Provider alone, while the Lead Provider manages recourse internally. Chronic failure should trigger enhanced remedies, such as mandatory service-improvement plans, termination for cause, or step-in rights allowing temporary operational control by the customer or a

Model	Description	Typical Use Case
<b>Lead Service Provider (hub-and-spoke)</b>	A single prime provider coordinates all sub-providers and acts as the customer’s main interface.	Complex ecosystems with a dominant contractor.
<b>Dedicated SLA Broker/ Central SLA Manager</b>	A neutral governance function consolidates metrics, harmonizes SLOs, and coordinates cross-provider activities.	Federated ecosystems with balanced responsibilities.
<b>Decentralized/Peer-to-Peer</b>	Providers coordinate directly via standardized interfaces and joint processes without a central authority.	Loosely coupled innovation ecosystems.

Table 1 – Overview of Governance Models

nominated third party.

Provider transitions are the most complex aspect of this model. Because multiple contractual chains converge under the Lead Provider, replacement requires careful planning. The SLA should therefore include detailed exit and transition clauses: obligations to cooperate during transition, data and documentation hand-over (runbooks, CMDB extracts, monitoring configurations), and transitional service agreements that maintain service continuity during hand-over. Anti-assignment or exclusivity clauses that block substitution should be prohibited, and “no degradation” obligations should protect service quality until completion of transition.

From a compliance standpoint, the Lead Provider consolidates privacy, security, and regulatory reporting. It manages sub-processor lists, coordinates incident notifications, and ensures consistent control frameworks across the supply chain. Commercially, pricing must reflect the added coordination role but remain transparent; pass-through of credits from sub-providers must be timely and proportional to protect the customer’s value.

In summary, the Lead Service Provider model provides unified accountability, consistent governance, and simplified communication – benefits that make it well-suited for large or regulated environments. Its drawbacks – dependency, limited visibility, and more complex transitions – can be mitigated through strong flow-down clauses, transparency rights, and detailed exit and continuity provisions. When properly governed, it delivers the clarity of a single accountable entity without sacrificing resilience or contractual fairness.

### 3.4 Dedicated SLA Broker/ Central SLA Manager Model

**The Dedicated SLA Broker** (also referred to as a Central SLA Manager) provides a neutral coordination layer between multiple providers and the customer.

Acting under a jointly agreed governance charter, the broker harmonizes SLOs and SLIs, reconciles measurement data, validates performance results, and facilitates coordinated reviews and dispute resolution.

This model enhances **transparency and comparability** across providers, as uniform metrics and definitions are applied consistently. It reduces conflicts of interest since no single service provider controls the measurement or escalation process. Each provider remains contractually accountable for its own SLOs,

while the broker ensures aligned monitoring and consolidated reporting.

Challenges include additional coordination costs and the need for clear mandates: the broker may recommend corrective actions and mediate issues but does not replace the contractual accountability of individual providers. The governance framework should therefore define data-sharing rights, escalation authority, dispute-resolution mechanisms, and the independence of the broker role.

In transition scenarios, this model offers strong continuity because each provider maintains a direct contract with the customer. Replacing one vendor does not affect the others, and the broker ensures consistent oversight. This makes it particularly suitable for federated ecosystems, public-sector collaborations, and industries requiring demonstrable neutrality.

### 3.5 Decentralized/Peer-to-Peer Model

In the decentralized model, coordination is distributed across peers instead of being centralized. Each provider interacts directly with others through standardized interfaces, shared telemetry, and linked incident-management processes. Responsibility is networked: accountability for individual components remains with each provider, while overall service quality depends on transparent cooperation and aligned measurement methods.

This approach offers maximum flexibility and scalability. Providers can be added or replaced quickly, supporting innovation and rapid adaptation in dynamic ecosystems such as IoT or edge-computing collaborations. It avoids a single point of failure or dependency but requires mature operational discipline: clear interface contracts, synchronized change windows, and robust information exchange protocols.

SLA language under this model should mandate **federated monitoring standards, mutual notification duties, and joint escalation procedures**. Linked ticketing systems and distributed tracing are essential for end-to-end visibility. Because accountability is shared, remedies may need proportional allocation based on each provider’s verified contribution to an incident.

While this model minimizes structural dependency, it increases coordination effort and may complicate root-cause analysis or fault attribution. It is best suited for environments where modularity, autonomy, and speed of change outweigh the need for central control.



### 3.6 Implications for Transition and Continuity

Each governance model influences how transitions and continuity are managed:

- **Lead Service Provider:** requires detailed step-in, substitution, and transition-support clauses to maintain service if the lead provider fails or is replaced.
- **Dedicated SLA Broker:** enables smooth substitution of individual providers while preserving measurement continuity through the neutral coordination layer.
- **Decentralized Model:** depends on open standards, shared data formats, and maintained interface registries to avoid lock-in and ensure interoperability.

Exit plans must explicitly address ownership of monitoring data, retention of performance history, cooperation obligations during dual operations, and the re-qualification of successor providers.

Including these provisions early in contract design helps prevent continuity risks during provider transitions or ecosystem restructuring.

In multiparty SLA constellations, transitions not only involve the substitution of one provider but also the coordinated update of inter-provider dependencies.

A structured change-management procedure must be defined for provider onboarding and offboarding, ensuring continuity of monitoring, reporting, and data retention.

The procedure should specify:

- notification timelines for planned changes;
- validation and acceptance of new providers before integration;
- re-baselining of metrics and SLOs;
- migration of monitoring data and dashboards;
- and coordinated contract amendments under the governance charter.

This ensures that the overall SLA framework remains intact even as individual providers change.

# Roles and Responsibilities



## 4.1 Context: Multi-Provider Provisioning Scenarios

Following the FACIS Taxonomy for SLAs (Section 3.2.3), this Playbook distinguishes two primary models of multi-provider service delivery, as they fundamentally determine how roles, responsibilities, and accountability must be allocated within SLAs.

**Entangled Supply Chains** – Historically the prevalent model: digital services are layered (e.g., SaaS on PaaS on IaaS) and depend on sequences of sub-providers. Customers typically contract with a lead provider, who manages several subcontractors. While this centralizes the contractual interface, it limits transparency and can create “blame chains.” Among the implications for SLAs are that obligations must cascade to sub-providers, back-to-back commitments are required, and accountability is consolidated under the lead provider.

**Federated Cloud Ecosystems** – The emerging and primary focus of this Playbook: independent providers collaborate as peers via interoperable interfaces and shared governance to deliver integrated services. This enables flexibility, innovation, and data sovereignty, yet requires explicit interface governance, harmonized metrics and definitions, coordinated incident response, and end-to-end monitoring across providers. For SLAs, this means that roles must be defined across organizations, measurement must be comparable, and remedies must propagate coherently in multi-party constellations.

This Playbook builds on experience with entangled supply chains while prioritizing federated ecosystems as the key innovation area for SLA governance. The roles and responsibilities described in the remainder of Section 5 should be interpreted in light of the selected model.

## 4.2 Actors and Stakeholders

The ecosystem typically includes a combination of the following actors:

- Service Providers – deliver IaaS, PaaS, SaaS, Edge, IoT, or AI/ML-based services.
- Connectivity and Carrier Providers – ensure network availability, latency, and throughput between cloud and edge components.
- Platform Operators and Integrators – orchestrate multiple services into an end-to-end capability.
- Data Brokers and Marketplaces – intermediate real-time data feeds or datasets used across providers.
- Auditors and Assessors – verify compliance, certifications, and evidence artefacts.
- Consultants and Advisors – provide design and governance guidance for providers or customers.
- Customers/Consumers – business units, applications, or organizations that rely on these federated services.
- Contract Owner/SLA Custodian – responsible for maintaining the consistency, version control, and continuous improvement of all SLA artefacts within the organization.
- Regulatory Compliance Officer – ensures that SLA terms and processes reflect applicable legal and supervisory obligations (e.g., DORA, GDPR, NIS2) and are demonstrably implemented in practice.

Security, privacy, and compliance functions ensure that controls and certifications are maintained, while vendor management and legal teams negotiate terms, manage renewals, and enforce remedies. (See also FACIS Taxonomy for SLAs, Section 3.2.3 for role definitions.)

### 4.3 Cross Provider Coordination

The selected governance model must be explicitly reflected in the SLA to avoid gaps in accountability. Rather than repeating the definitions of the three models (Lead Provider, SLA Broker, Peer-to-Peer), this section focuses on how coordination is implemented contractually and operationally:

- Lead Provider model: designate the prime contractor as responsible for consolidating performance data, reporting, and incident management.
- SLA Broker model: define the broker's mandate, data-access rights, and coordination procedures in a dedicated governance annex.
- Peer-to-Peer model: include reciprocal obligations for data sharing, incident escalation, and change management among all providers.

Each SLA should clearly reference which model applies and how coordination interfaces are maintained when providers join or leave the ecosystem.

### 4.4 Responsibility Allocation

Dependencies among providers must be disclosed with enough specificity to assess aggregate risk, including critical sub-processors and networks that materially affect service quality. SLAs must define which SLOs are local to a component and which are measured end-to-end across the chain, who is responsible for traffic steering, capacity management, and failover, and how telemetry is correlated across providers to support incident triage, root-cause analysis, and remedy calculation.

Responsibility allocation should be documented in a **Responsibility Assignment Matrix (RACI)** and mirrored in SLA language to ensure unambiguous ownership, accountability, consultation, and information duties. Escalation paths should be time-bound and role-based rather than person-dependent, with continuous coverage for critical incidents and clear routes to senior engineering and management oversight.



## Example: Responsibility Allocation Matrix

Activity/Obligation	Lead Provider	Sub-Provider(s)	Customer	SLA Manager/ Governance Function
Define SLA metrics and targets	A	C	C	R
Monitor and consolidate SLOs	R	C	I	A
Incident detection and triage	R	R	I	C
Root cause analysis	A	R	I	C
Change coordination	A	C	I	R
Reporting and QBR preparation	A	C	I	R
Compliance evidence & audits	A	R	I	R
Credit/remedy calculation	A	C	I	R
Executive escalation	R	I	C	A

Table 2 – Example Responsibility Allocation Matrix

**Legend:** R = Responsible A = Accountable C = Consulted I = Informed

This matrix should be maintained as a living artefact, updated whenever provider composition or service scope changes. Critical processes such as incident response, disaster recovery, and compliance reporting should directly reference this matrix in operational runbooks and governance protocols.

### 4.5 Liability and Risk Allocation

According to the FACIS Taxonomy for SLAs (Section 3.2.4), the SLA may cover liability and remedy restrictions at a general level that govern the entire agreement.

Typical elements include:

- Responsibility should follow fault and control principles, with proportional allocation when fault cannot be definitively determined.
- Fallback and Continuity Provisions – step-in rights, substitution rights, or resourcing at the provider's cost safeguard continuity where a material breach occurs.
- Limits and Carve-Outs – liability caps (e.g. 12 months' service fees) balanced with higher or uncapped exposure for willful misconduct, IP infringement, or confirmed data-protection breaches.
- Insurance Requirements – technology professional liability insurance (technology E&O), cyber liability, and business interruption coverage should be evidenced upon request.
- Scope of Liability – covers SLA breaches, service downtime, data loss, security incidents, and continuity failures, while excluding force majeure, customer-caused issues, and third-party network failures beyond contracted scope.
- Multi-Provider Allocation – critical obligations should flow down to sub-providers where feasible, ensuring back-to-back commitments.

# SLA Structure and Core Components



## 5.1 Core Structure

The FACIS Taxonomy for SLAs defines four foundational building blocks that together form a complete and operationally enforceable Service Level Agreement. Each building block establishes a distinct layer of control, from definition to enforcement:

1. **Foundation** – sets the stage and scope of the SLA by defining terminology, actors, and applicability.
2. **Service Level Objectives (SLOs)** – describe the measurable commitments the provider makes about a service, such as availability or performance.
3. **Monitoring** – specifies how compliance with those commitments is measured through Service Level Indicators (SLIs) and defined metrics.
4. **Enforcement** – determines remedies, escalation paths, and rights in case of non-adherence.

When designing or revising SLAs, each building block should be addressed explicitly to ensure that technical, legal, and operational stakeholders share a common understanding. Every SLA – regardless of service type – should clearly state:

- what is in **scope** and **out of scope**,
- the metrics and calculation rules used to measure performance,
- applicable **exclusions** and maintenance windows,
- **incident classification** and response/resolution times,
- **change-management procedures**,
- **support hours**, **update** cadence, and
- escalation and reporting obligations.

The SLA must also specify the tangible **consequences of non-performance** and provide a controlled amendment mechanism for evolving services without diluting agreed protections.

## 5.2 Hierarchy of SLA Commitments

SLA commitments follow a structured hierarchy derived from the FACIS Taxonomy for SLAs:

- **SLA** → contains one or more **Service Level Objectives (SLOs)**.
- Each **SLO** is operationalized through one or more **Service Level Indicators (SLIs)**.
- Each **SLI** is measured by defined **metrics**.

For example:

Objective: ensure high service availability.

Indicator: uptime percentage of the service.

Metric: monthly average uptime ≥ 99.9 %, excluding approved maintenance windows.

To express this hierarchy clearly, the SLA should describe for each SLO:

1. **Definition/Purpose** – what characteristic is guaranteed and why it matters.
2. **Indicator (SLI)** – how the characteristic is measured.
3. **Metric and Calculation Method** – parameters, formulas, measurement intervals.
4. **Target Value** – quantitative threshold (e.g., ≥ 99.5 %).
5. **Exclusions** – events or conditions that do not count as breaches.
6. **Remedy Mechanism** – credits, service adjustments, or termination rights if unmet.

### 5.3 Design and Documentation Guidance

Each SLA should document not only the values and formulas but also who owns and verifies each obligation:

- Scope – the service boundaries within which the SLO applies.
- Responsibility – the accountable party for measurement and reporting.
- Boundaries – dependencies on external or sub-providers.
- Timing – frequency of measurement and reporting.
- Authenticity – data-integrity controls ensuring trustworthy results.

All SLIs and metrics should be machine-readable and, where feasible, the data should be elucidated through APIs or dashboards. This supports automation of SLA management, consistent with the FACIS objective of fostering machine-interpretable governance artefacts.

### 5.4 Practical Examples

Dimension	Illustrative Clause
Availability	"The Provider shall maintain a minimum monthly uptime of 99.9%, measured by Provider telemetry validated by agreed customer probes."
Performance	"The 95th percentile response time for API calls shall not exceed 200 ms at the Provider's gateway."
Support Responsiveness	"Priority 1 incidents shall be acknowledged within 15 minutes and resolved within four hours."
Change Management	"Breaking API changes require at least 90 days' prior notice and dual-version support for six months."

Table 3 – Example taxonomy dimensions in SLA clauses

These examples illustrate how abstract taxonomy dimensions – SLO, SLI, metric – translate into enforceable SLA clauses.

### 5.5 Integration with Sector-Specific Annexes

The base SLA should remain sector-agnostic and stable. Sector-specific or jurisdiction-specific requirements are captured in **dedicated annexes**, which overlay the base SLA without rewriting it. Each annex should identify mandatory external obligations (laws, standards, supervisory guidance) and map them to measurable SLOs and evidence obligations. This modular approach allows precise tailoring where regulation or risk differs, while preserving a consistent core structure.

## 6.1 Purpose and Relation to the FACIS Taxonomy for SLAs

This section operationalizes the abstract concepts of the *FACIS Taxonomy for SLAs* into concrete, enforceable SLA clauses. While the FACIS Taxonomy for SLAs defines what an SLA should contain – its dimensions, structure, and metrics – this section describes how these dimensions are written as binding contractual terms. The Playbook follows a modular approach: each SLA consists of a base layer defining minimum requirements and a set of optional modules for sectoral or functional extensions. This modularity allows organizations to combine standardized core clauses with specialized add-ons without fragmenting the overall governance model.

Put simply:

Taxonomy = Framework of SLA dimensions

This Playbook = Language templates and examples

Each clause template below follows the FACIS hierarchy: Service Level Objective (SLO) → Service Level Indicator (SLI) → Metric and Target Value → Exclusions and Remedy.

## 6.2 Design Approach

Each SLO should follow a consistent structure. Each technical objective defined in service architecture or operational policies must be translated into enforceable contractual language. Every metric or threshold appearing in design documentation must have a corresponding SLO entry in the SLA template to ensure legal enforceability and auditability.

1. **SLO – Objective:** What service aspect is guaranteed (e.g., availability, latency).
2. **SLI – Indicator:** How the aspect is measured (e.g., uptime %).
3. **Metric:** Parameters, expressions, and measurement rules.
4. **Target Value:** Guaranteed threshold (e.g., ≥ 99.9 %).
5. **Exclusions:** Circumstances that suspend obligations.
6. **Remedy:** Credits, adjustments, or termination rights.

All SLOs must be measurable, auditable, and traceable to business outcomes.

Avoid ambiguous verbs such as “strive to ensure” – use enforceable verbs: “shall maintain,” “shall notify,” “shall resolve.” Where multiple providers are involved, clarify how metrics correlate, how fault is attributed, and how remedies propagate along the chain. Each SLO category described in the following examples follows this six-part structure.

For brevity, the examples below focus on the most illustrative contractual language, while the full SLO definition – including metric formulas, exclusions, and remedies – should be documented in the SLA template (see Annex A).

## 6.3 Example Service Level Objectives

The following examples illustrate how each SLO can be expressed in enforceable contractual language. Each example corresponds to the six structural elements defined in Section 6.2 – objective, indicator, metric, target, exclusions, and remedy – although some details (e.g., calculation formulas or credit scales) are provided in Annex A for clarity.

### 6.3.1 Availability

**SLO (Objective):** The service shall remain accessible and usable for customers at or above **99.9 % per calendar month**, excluding approved maintenance windows and defined excluded events. For critical edge workloads, local processing components shall maintain availability at **≥ 99.5 %**, measured at site level, with fallback to regional nodes if connectivity to the core cloud is lost.

**SLI (Measurement):** Availability is measured based on provider telemetry validated by agreed customer probes. Downtime includes all periods when the service is not accessible through the primary interface or fails to meet minimum responsiveness thresholds. Maintenance events and approved exceptions are logged and excluded from downtime calculations.

**Example Clause:**

“The Provider shall make the service available at or above 99.9 % per calendar month, excluding approved maintenance windows and defined excluded events. Credits apply on a tiered basis for shortfalls; chronic failures grant termination rights.”

### 6.3.2 Performance

**SLO (Objective):** The service shall maintain defined performance levels for key transactions, including latency and throughput. The **95th percentile response time for read operations shall not exceed 200 ms** at the Provider's API gateway, and sustained throughput shall remain  $\geq 500$  requests per second under standard load conditions. Breaches persisting for two consecutive months trigger a mandatory remediation plan.

**SLI (Measurement):** Performance is measured using a combination of synthetic and real-user monitoring at agreed vantage points (e.g., API gateway, client edge, or network ingress). Latency is calculated as the elapsed time between client request and server response. Throughput is measured as the number of successful requests per second under typical operating load.

**Example Clause:**

"The 95th percentile response time for read operations shall not exceed 200 ms at the Provider's API gateway. Breaches persisting for two consecutive months trigger a mandatory remediation plan."

### 6.3.3 Customer Support

**SLO (Objective):** Incidents shall be acknowledged and resolved within defined timeframes based on severity level. Priority 1 incidents must be acknowledged within 15 minutes and resolved within four hours.

**SLI (Measurement):** Response and resolution times are measured from ticket creation timestamps in the incident management system. Escalation metrics track compliance with severity-based timelines.

**Example Clause:**

"Priority 1 incidents shall be acknowledged within 15 minutes and resolved within four hours. Escalation to executive management is mandatory if resolution exceeds this timeframe."

SLAs should also define communication channels, supported languages, operating hours, and reporting cadence.





### 6.3.4 Maintainability

**SLO (Objective):** Maintenance activities shall be scheduled and communicated to minimize disruption. Planned maintenance shall occur only within approved windows and be announced at least 14 days in advance.

**SLI (Measurement):** Change and maintenance records are tracked via the change-management system. Metrics include the percentage of planned vs. unplanned maintenance and the number of out-of-window activities.

**Example Clause:**

“Planned maintenance shall occur only within approved windows announced  $\geq$  14 days in advance. Emergency maintenance requires immediate notice and post-event validation.”

### 6.3.5 Change Management

**SLO (Objective):** API and schema changes must ensure backward compatibility and allow sufficient transition periods. Breaking changes require at least 90 days’ prior notice and dual support for a minimum of six months.

**SLI (Measurement):** Measured by change-log analysis and release-management documentation.

Metrics include notice periods, percentage of dual-supported versions, and number of breaking changes per quarter.

**Example Clause:**

“Breaking API changes require at least 90 days’ prior notice and dual support for a minimum of six months.”

### 6.3.6 Data Protection and Privacy

**SLO (Objective):** The provider shall process customer data solely for service delivery as defined in the Data Processing Agreement (DPA). Confirmed data breaches must be reported to the customer within 24 hours of detection.

**SLI (Measurement):** Measured through incident reports, audit logs, and compliance with DPA notification timelines. Metrics include number of data breaches, time-to-notify, and sub-processor disclosures.

**Example Clause:**

“The Provider shall process customer data solely for service delivery as defined in the DPA and shall notify the Customer within 24 hours of confirmed detection of a data breach.”

### 6.3.7 Information Security

**SLO (Objective):** Security controls shall prevent, detect, and respond to threats affecting customer systems. Confirmed security incidents must be reported to the customer within one hour of detection, with a root-cause analysis provided within five business days.

**SLI (Measurement):** Measured by Security Information and Event Management (SIEM) logs and incident-report timestamps. Metrics include time to detect, time to notify, and time to remediate.

**Example Clause:**

“Security incidents with confirmed impact on customer systems shall be reported by the Provider to the Customer within one hour of detection, followed by a root-cause analysis that shall be reported by the Provider to the Customer within five business days of detection.”

### 6.3.8 Reliability and Operational Resilience

**SLO (Objective):** The provider shall maintain business continuity and disaster-recovery capabilities to restore critical services within agreed thresholds. Recovery Time Objective (RTO) shall not exceed 4 hours, and Recovery Point Objective (RPO) shall not exceed 15 minutes. Disaster-recovery plans must be tested annually and include critical third-party dependencies.

**SLI (Measurement):** Measured by recovery test results, failover simulations, and audit documentation. Metrics include achieved RTO/RPO, test success rates, and frequency of plan updates.

**Example Clause:**

“The Provider shall maintain disaster-recovery plans that are tested at least annually and that must achieve an RTO ≤ 4 hours and RPO ≤ 15 minutes for critical services.”

## 6.4 Escalation Paths

Escalation must be time-bound and role-based. Critical incidents should have 24/7 coverage with defined response tiers up to executive level. In multi-provider environments, escalation rules must align with the coordination model (Lead Service Provider, Dedicated SLA Broker, or Decentralized Peer-to-Peer).

## 6.5 Remedies and Penalties

Per the FACIS Taxonomy for SLAs (Section 3.5), remedies compensate the customer when SLOs are not met. They may take the form of service credits, refunds, or termination rights. For multi-provider chains, remedies should propagate across providers so that the customer receives a coherent outcome even when fault attribution is complex.

### 6.6 Relationship to the General Terms and Complementary Agreements

This Playbook and its SLA templates are designed to complement, not replace, general contractual terms such as the Master Services Agreement (MSA), General Terms and Conditions (GTC/AGB), or dedicated security and data processing agreements.

For transparency, the SLA should explicitly reference these accompanying documents and clarify the hierarchy of obligations.

In particular,

- the SLA governs measurable service commitments and remedies;
- the Security Annex or DPA governs confidentiality, integrity, and protection of information; and
- the GTC governs commercial and procedural aspects.

This separation ensures legal clarity, avoids conflicting clauses, and enhances contract transparency – especially when integrating hyperscaler or third-party terms.

# Monitoring and Reporting



## 7.1 Purpose

Effective SLA governance depends on transparent, verifiable, and consistent measurement of all Service Level Objectives (SLOs). Monitoring transforms contractual commitments into operational accountability by providing objective data on performance, availability, and compliance across all providers involved in the service delivery.

## 7.2 Real-Time and Periodic Monitoring

Monitoring should combine real-time data collection with periodic reporting to ensure continuous visibility and traceable performance history.

- Real-Time Monitoring – Core metrics (availability, latency, throughput) must be captured continuously and visualized in dashboards accessible to authorized customer and governance users. Machine-readable telemetry enables automated validation of SLO compliance and supports predictive analytics for early risk detection.
- Periodic Monitoring – Complementary monthly or quarterly reports summarize quantitative results, incident statistics, and remediation activities. These reports should include explanations for deviations, improvement actions, and trend analyses over defined periods.

To maintain consistency, metrics and data collection methods must align with the FACIS Taxonomy for SLAs measurement principles (Section 3.4.2) and be documented in each SLA or annex.

## 7.3 Data Sources and Verification

All Service Level Indicators (SLIs) must reference verified data sources.

Providers and customers should agree on:

- the measurement point (e.g., provider API gateway, customer probe, edge node),
- the data origin and timestamp precision, and
- the validation method (e.g., mirrored probes, synthetic transactions, or independent telemetry).

Cross-provider environments require shared or federated observability, allowing metrics from multiple providers to be correlated for end-to-end visibility and defensible fault attribution.

### Example Clause:

“Provider and Customer shall maintain synchronized telemetry interfaces allowing real-time access to agreed SLA metrics. Where multiple providers contribute to a composite service, aggregated metrics shall be reconciled by the Dedicated SLA Broker or equivalent governance function.”

## 7.4 Reporting Requirements

Each provider must supply regular SLA performance reports that include:

- quantitative results for each SLO and SLI,
- list of incidents and root-cause summaries,
- credits or remedies issued,
- upcoming maintenance or change activities,
- improvement and prevention measures.

Reports should be made available both as human-readable summaries and as machine-readable exports (e.g., CSV, JSON, API) for automated integration into customer monitoring systems.

### Example Clause:

“Provider shall deliver monthly SLA performance reports within ten business days after each reporting period, in both PDF and machine-readable formats. The report shall include a narrative summary, metric tables, and improvement actions.”

## 7.5 Dashboards and KPIs

Providers should operate secure dashboards offering:

- current SLO attainment (e.g., uptime %, response-time percentiles),
- historical trends,
- open and resolved incidents, and
- planned maintenance windows.

Dashboards must differentiate between live data and validated monthly results to prevent misinterpretation. Where a Dedicated SLA Broker or centralized governance function exists, dashboards across providers should be federated to allow consolidated KPIs and trend analysis.

## 7.6 Audit and Verification Rights

Customers and authorized auditors shall have reasonable rights to verify measurement processes, without undue disruption to the provider's operations. Verification may include:

- review of monitoring configurations and calculation scripts,
- inspection of raw metric samples, or
- validation through parallel measurement probes.

The SLA should specify notification periods, confidentiality protections, and cooperative procedures for such audits.

### Example Clause:

"Upon reasonable notice, the Customer or its auditor may verify the Provider's measurement and reporting processes once per year. Provider shall cooperate and make relevant evidence available in secure viewing mode."

## 7.7 Governance Reviews

Regular governance reviews ensure continuous alignment between contractual and operational realities. Typical cadence: quarterly business reviews (QBRs) and annual strategic reviews.

Each review should cover:

- SLA performance and remedy status,
- upcoming service or architecture changes,
- regulatory or compliance updates, and
- proposed improvements to SLOs, metrics, or thresholds.

Minutes, actions, and agreed changes must be documented and stored as part of the governance record.

## 7.8 Integration with Other Frameworks

Monitoring and reporting processes should integrate with:

- incident-management systems (for escalation data),
- change-management tools (for planned downtime correlation), and
- compliance frameworks (e.g., ISO 27001, ITIL, or sector-specific supervisory requirements).

This integration ensures that SLA governance is embedded within broader operational and regulatory controls rather than maintained in isolation.



# Using This Playbook in Practice



## 8.1 Purpose

This Playbook is designed as a living governance toolkit. It can be used to design, negotiate, implement, and continuously improve SLAs across multi-provider and federated ecosystems. It provides reusable patterns, definitions, and templates that help organizations translate strategic goals and compliance obligations into measurable service commitments. While the FACIS Taxonomy for SLAs defines the abstract framework, this Playbook offers the operational language and process view that makes those concepts executable in real projects.

## 8.2 Typical Use Cases

The Playbook can be applied in multiple organizational contexts:

- **Procurement and Contracting** – to structure RFPs, evaluation criteria, and model SLA language for supplier selection.
- **Vendor Management** – to align reporting and remediation processes across diverse service providers.
- **Legal and Compliance** – to translate regulatory requirements (e.g., DORA, NIS2, GDPR) into measurable SLOs.
- **Service Architecture and Operations** – to design service blueprints and monitoring structures consistent with contractual obligations.
- **Audit and Assurance** – to verify SLA compliance through standardized, machine-readable metrics and dashboards.

## 8.3 Implementation Steps

When introducing this Playbook, organizations should follow a structured approach to ensure alignment across legal, technical, and operational teams.

1. **Scoping and Model Selection:** Identify which services and providers fall under SLA governance. Select the applicable governance model (Lead Service Provider, Dedicated SLA Broker, or Decentralized Peer-to-Peer). Define integration points between providers, data sources, and monitoring tools.
2. **Baseline and Template Configuration:** Start with the core SLA structure (see Section 6) and adapt the templates to your organizational terminology and measurement standards. Use existing annexes (sector-specific, regulatory, or technical) to avoid duplication.

3. **Cross-Functional Validation:** Conduct joint reviews between Legal, Compliance, IT Operations, and Vendor Management. Validate that each SLO is measurable, enforceable, and consistent with the Data Processing Agreement (DPA) and Business Continuity plans.
4. **Operationalization and Onboarding:** Establish shared dashboards, reporting intervals, and escalation protocols. Train responsible teams on metric interpretation, credit calculation, and governance workflows.
5. **Continuous Review and Improvement:** Integrate SLA metrics into quarterly business reviews (QBRs). Adjust SLOs to reflect evolving business priorities, risk exposure, or regulatory updates. Document all updates as controlled revisions in the SLA register.

## 8.4 Governance Integration

SLA governance should be embedded into the organization's overall control system rather than treated as a standalone document. Integration touchpoints include:

- **Risk Management Frameworks** – mapping SLOs to risk indicators and control objectives.
- **Change and Release Management** – ensuring SLO updates are synchronized with product and infrastructure changes.
- **Incident and Problem Management** – linking SLA breaches to root-cause analysis and preventive actions.
- **Compliance and Audit** – connecting SLA evidence to audit trails and regulatory reporting.

The Playbook can serve as a reference baseline for internal governance policies, supplier management procedures, and regulatory submissions.

## 8.5 Maintenance and Version Control

Because service ecosystems evolve, the Playbook must be maintained as a controlled document.

Each update should include:

- a change log summarizing revisions,
- version numbering aligned with the FACIS release cycle, and
- ownership and review metadata.

Organizations should appoint a Playbook Custodian or Governance Office responsible for:

- validating new SLO templates,
- aligning terminology with current regulatory frameworks,
- coordinating updates across stakeholders, and
- communicating major changes to affected providers.

## 8.6 Continuous Improvement

Consistent with the FACIS principles of transparency and modularity, SLA governance is an iterative process. Data collected through monitoring (Section 7) and operational feedback should be analyzed to identify trends, bottlenecks, and systemic weaknesses. Improvements can include:

- revising SLO definitions,
- refining measurement methods,
- adjusting credit schemes, or
- introducing automation for compliance verification.

Continuous improvement ensures that SLAs remain relevant, enforceable, and aligned with both customer expectations and regulatory oversight.

### Summary of Key Recommendations:

- Apply the modular FACIS structure (Foundation – SLO – Monitoring – Enforcement).
- Define clear roles, especially SLA Custodian and Compliance Officer.
- Translate all technical objectives into enforceable SLO clauses.
- Maintain continuous alignment with legal frameworks (DORA, NIS2, GDPR).
- Establish structured provider-change and SLA-update procedures.
- Use Annex A–E for templates, metrics, glossary, and sector-specific guidance.

## 8.7 Future Extension – SLA Repository

To support consistent application and continuous improvement, organizations may establish an SLA Repository as a structured collection of reusable service definitions, metrics, and clause templates derived from this Playbook. Such a repository would serve as a living knowledge base for federated SLA design and governance, ensuring that lessons learned, validated SLO definitions, and agreed measurement approaches remain available and version-controlled.

The repository can enable:

- **Reuse and consistency** – standardized clauses and metrics across projects and providers;
- **Transparency and auditability** – traceable evolution of service definitions and thresholds;
- **Collaboration** – shared development of federated SLA components within provider ecosystems.

While this Playbook provides the conceptual and structural foundation, the repository would complement it as a practical implementation layer that evolves with operational experience and regulatory change. Importantly, the repository is intended as a supporting resource, not a constraint.

Users may adopt, adapt, or extend the sample definitions according to their own service context, risk profile, and regulatory environment. This flexibility ensures that federated SLA governance remains both consistent and adaptable across diverse domains.



- **Annex A:** Generic SLA Templates
- **Annex B:** Example Metrics and Dashboards
- **Annex C:** Glossary of Terms
- **Annex D:** Legal and Regulatory Frameworks (e.g., GDPR, NIS2, AI Act...)
- **Annex E:** Sector-Specific SLA Parameters (Optional Guidance)

## Annex A: Generic SLA Templates

**Disclaimer:** Please note that the following templates are provided for information purposes only and are neither intended as nor should be construed as legal advice. Each user is responsible for asking their own lawyers for advice before using these templates.

### A. Service Level Agreement Template for dedicated SLA Broker and Decentralized-Models – Version 1.0

#### Service Level Agreement

between

X  
 \_\_\_\_\_  
 („Service Recipient“)

and

X  
 \_\_\_\_\_  
 („Service Provider 1“)

and

X  
 \_\_\_\_\_  
 („Service Provider 2“)

and

X  
 \_\_\_\_\_  
 („Service Provider 3“)

**!**  
**NOTE TO USER:** Add each parties' legal name and full address at [ X ]. Add more service providers if necessary.

(each also „Party“ and together „Parties“)

## Preamble

- (A) The Service Recipient agreed separate service agreements with each Service Provider („**Main Agreement**“). The Parties agree that the total of all Services provided by the Service Providers constitutes a service product („**Service Product**“) which performance depends on the performance of each individual Service.
- (B) The Parties therefore indent to agree a common service level for the Service Product with this Service Level Agreement („**SLA**“) that defines the allocation of responsibilities, escalation paths, and coordination mechanisms. Each Service Provider shall cooperate to ensure seamless service delivery and incident resolution.

Against this background, the Parties agree as follows:

## 1. Definitions

- 1.1 **Force Majeure Event** shall have the meaning given to it in Section 10.
- 1.2 **Incident** shall mean a single event that results in a Malfunction.
- 1.3 **Malfunction** shall mean any breach of an agreed Service Level Objective.
- 1.4 **Planned Downtime** shall mean any non-availability or limited functionality of a Service due to maintenance, repair or upgrade work that is announced by the responsible Service Provider at least X \_\_\_\_\_ days prior to the start of the work.
- 1.5 **Services** means the services agreed within each Main Agreement.
- 1.6 **Service Credit Incident** shall mean any incident where the agreed target value of a Service Level Objective was not reached.

**!**  
**NOTE TO USER:** Add number of days.

**!**  
**NOTE TO USER:** Add all additional definition used when filling out this template, e.g. Monthly Uptime Percentage, Downtime.

## 2. Service Description

2.1 **Precedence.** The Parties agree, and each Party represents and warrants, that this SLA shall supersede any deviating or supplementary clauses within each Main Agreements to the same subject matter.

2.2 **Responsibilities.** The Services governed by this SLA are defined within the Master Agreements. The Service Providers' responsibility for specific Services is defined below:

 **NOTE TO USER:** Add the included Services.

Name of Service	Responsible Service Provider
Example: Cloud Storage Service	Example: Service Provider 1

Table 4 – Service Provider and Services

The Parties acknowledge each Service Provider shall only be responsible for its Service and not for the performance of Services provided by the other Service Providers. Nonetheless, the Service Providers agree to work together cooperatively to provide the best possible Service Product for the Service Recipient.

2.3 **Interdependencies.** The Parties agree that the orderly performance of a Service may depend on the performance of one or more other Service(s) and that a Malfunction of a Service („**Causing Service**“) may be the root cause for another Service („**Impaired Service**“) having a Malfunction („**Interdependency Malfunction**“).

2.4 The Parties agree to the following hierarchy of the Services whereby the higher ranked Service is dependent on the performance of the lower ranked Service:



**NOTE TO USER:** Rank the included Services.

Rank	Name of the Service
1	Example: Cloud Application Service
2	Example: Cloud Storage Service
3	
4	
5	
6	

Table 5 – Interdependencies

### 3. SLA Exclusions

- 3.1 This SLA does not apply to Malfunctions caused by
- Force Majeure Event (as defined below at Section 10);
  - the Service Recipient's own hardware or software or other technology used in relation to the Services;
  - actions or omissions by or on behalf of the Service Recipient which constitute a breach of the Main Agreement or this SLA; or
  - Planned Downtime.
- 3.2 In case of Interdependency Malfunctions, this SLA shall not apply to the Impaired Service but solely to the Causing Service.
- 3.3 In case the Main Agreement with one or more Service Provider is terminated, the remaining Service Providers are released from their obligations under this SLA, unless the remaining Service Providers expressly confirm this SLA.

### 4. SLA Manager / Service Contact

- 4.1 The Parties nominate X \_\_\_\_\_ as the SLA manager („SLA Manager“).



**NOTE TO USER:** This can be a representative of one of the service providers or a dedicated external manager.

- 4.2 The SLA Manager is responsible for the communication and coordination between the Parties but is not responsible in its role as the SLA Manager towards the Service Recipient for the performance of the Service Product.
- 4.2 Each Service Provider shall apply reasonable means to make available to SLA Manager the relevant information about the performance of its Service (e.g. dashboard access).
- 4.2 Each Party shall nominate one of its personnel as the Party's Service contact who will be responsible for the communication with the SLA Manager.

## 5. Service Levels



**NOTE TO USER:** Add a service level for each Service. The service level should be defined by service level objective, service level indicator, the target value and the measurement metric.

**Example for Availability:** The Service availability offered by the Service Provider is an Uptime of  $\geq 99,5\%$  per month („Monthly Uptime Percentage“).

The Monthly Uptime Percentage means the difference between the total number of minutes in a month (as the minuend) and the number of minutes of all Downtime Periods in that month (as the subtrahend), divided by the total number of minutes in that month:

$(\text{Total number of minutes in a month} - \text{number of minutes of Downtime Periods}) / \text{Total number of minutes in a month} \times 100 = \text{Monthly Uptime Percentage}$

## 6. Service Monitoring

6.1 The Parties agree that each Service shall be monitored as follows:



**NOTE TO USER:** Add the monitoring means used for each Service.

(„Service Monitoring“)

6.2 The Parties agree that the SLA Manager shall have access to the Service Monitoring and shall be entitled to inform all Service Providers in case of a Malfunction of one or more Services.

## 7. Support

7.1 The Parties agree that the SLA Manager’s operating hours shall be X.

7.2 The Parties further agree that the operating hours of the support for the Services shall be the following:  
X



**NOTE TO USER:** Add the support operating hours for each Service and how it can be contacted, e.g. phone, email, ticket system, here.

7.3 The Parties agree the following response/resolving times for each Service:  
X



**NOTE TO USER:** Add the specific response/resolving times here.

## 8. Remedies

8.1 **Service Credits.** In case of a Service Credit Incident the Service Recipient shall be entitled to receive Service Credits as the Service Recipient’s exclusive remedy and the Service Provider’s entire liability. The details of the Service Credits are defined in Annex 1.



**NOTE TO USER:** Add a Service Credits definition as Annex 1.

8.2 **Claiming.** To receive Service Credits the Service Recipient must notify the Service Provider within X days from the time Service Recipient becomes eligible to receive Service Credits whereby such notice must include information allowing the Service Provider to identify the Service Credit Incident and the date and time of the Service Credit Incident.



**NOTE TO USER:** Add the number of days.

8.3 **Service Credits Dispute.** In case of a dispute regarding a Service Credit notification the affected Parties shall first escalate the dispute to the SLA Manager.

## 9. Term and Exit Management

- 9.1 **Term.** The term of this SLA is the same as the term of the Main Agreement („**Term**“). The Term ends automatically at the end of the term of the Main Agreement.
- 9.2 **Termination.** During the Term, the ordinary right of early termination is excluded. Each Party’s statutory right to terminate this SLA for cause without notice remains unaffected.
- 9.3 **Notification.** In the event of termination or expiry of this SLA or any Main Agreement, the Party receiving the termination notice shall be entitled to and obligated to notify the SLA Manager about the termination. The SLA Manager shall inform the other Parties about the termination and discuss with the other Parties the implications of the termination.
- 9.4 **Exit Management.** Upon termination or expiry of this SLA for any reason, each Service Provider shall provide reasonable assistance to ensure an orderly transition of the Services to the Service Recipient or to a replacement service provider, as directed by the Service Recipient. This includes, but is not limited to:
- Providing all relevant documentation, records, and information necessary for the transition;
  - Cooperating with the Service Recipient and/or any replacement provider to facilitate the transfer of services and knowledge;
  - Ensuring the migration of all Service Recipient data, including backups, to the Service Recipient or to a third party nominated by the Service Recipient, in a commonly used and machine-readable format, within a reasonable timeframe and at a reasonable cost;
  - Deleting or returning all Service Recipient data in accordance with the Service Recipient’s instructions and applicable data protection laws, subject to any legal retention requirements;
  - Providing reasonable support for a period of up to [30/60/90] days following termination or expiry, as agreed between the Parties, to address any issues arising from the transition.

The Service Provider shall not impose any unreasonable restrictions, delays, or additional charges for exit management or data migration services, except as expressly agreed in advance.

The obligations in this clause shall survive termination or expiry of the SLA to the extent necessary to complete the exit management process.



**NOTE TO USER:** The exit management clause in 9.4 is only optional.

## 10. Force Majeure

- 10.1 Neither Party shall be liable for any failure or delay in performing its obligations under this SLA if and to the extent such failure or delay results from circumstances beyond its reasonable control (“**Force Majeure Event**“). Force Majeure Events include, but are not limited to:
- Acts of God (such as earthquakes, floods, storms, or other natural disasters),
  - War, hostilities (whether declared or not), invasion, act of foreign enemies,
  - Terrorist acts, civil commotion, riots, or insurrection,
  - Government actions, embargoes, or blockades in effect on or after the date of this SLA,
  - Strikes, lockouts, or other industrial disputes (excluding those involving the affected Party’s own personnel),
  - Epidemics or pandemics,
  - Fire or explosion, and
  - Power outtakes or Internet connection failures/outtakes not under the control of the affected Party.
- 10.2 The affected Party shall notify the other Parties in writing as soon as reasonably practicable, and in any event within X hours of becoming aware of the Force Majeure Event, specifying the nature and expected duration of the event and the steps being taken to mitigate its effects.



**NOTE TO USER:** Add number of hours.

- 10.3. In case a Force Majeure causes an Interdependency Malfunction the Impaired Service shall be released from its liability for any failure or delay in performing its obligation under this SLA for the period the Force Majeure Event impacts the Causing Party.

## 11. Additional Terms



**NOTE TO USER:** Only to be used if additional terms are necessary, e.g. regulatory specific terms. Otherwise, clause 11 can be deleted.

## 12. Miscellaneous

- 12.1 **No Agency.** Nothing in this SLA shall be construed as creating a partnership, joint venture, or agency relationship between the Parties. Neither Party shall have the authority to act for, bind, or otherwise create or assume any obligation on behalf of the other Party for any purpose whatsoever. Each Party acts as an independent contractor and is solely responsible for its own actions, employees, and sub-providers.
- 12.2 **Written Form.** Any amendment, modification, or supplement to this SLA, as well as any waiver of rights or obligations under this SLA, shall only be valid if made in writing and signed by authorized representatives of all Parties. This requirement for written form may only be waived by a written agreement expressly referring to this clause. For the purposes of this clause, "in writing" includes documents signed by hand or by electronic signature but excludes informal email correspondence.
- 12.3 **Severability.** If any provision of this SLA is held to be invalid, illegal, or unenforceable by a court of competent jurisdiction, such provision shall be deemed severed from this SLA and shall not affect the validity or enforceability of the remaining provisions. The Parties shall use reasonable endeavors to replace any invalid or unenforceable provision with a valid and enforceable provision that achieves, as far as possible, the original intent and economic effect of the invalid or unenforceable provision.

12.4 **Dispute Resolution.** In the event of any dispute, controversy, or claim arising out of or in connection with this SLA, the Parties shall refer the matter to the SLA Manager, who shall use reasonable endeavors to facilitate a resolution between the Parties. The SLA Manager shall have thirty (30) days from the date the dispute is formally notified in writing by either Party to resolve the dispute. If the SLA Manager is unable to resolve the dispute within this period, either Party may refer the matter to the competent courts as specified in this SLA.

12.5 **Governing Law/Jurisdiction.** This SLA shall be governed by the laws of the Federal Republic of Germany. To the extent permitted by law, the courts of X shall have exclusive jurisdiction for all disputes out of or in relation to this SLA



**NOTE TO USER:** Please chose a German city which courts should have jurisdiction.



**NOTE TO USER:** Add signature line.

## B. Service Level Agreement Template for Lead Service Provider-Model – Version 1.0

### Service Level Agreement

between

X

(„Service Provider“)

and

X

(„Service Recipient“)



**NOTE TO USER:** Add each parties' legal name and full address at [ X ].

(each also „Party“ and together „Parties“)

### Preamble

- (A) The Parties agreed a service agreement, under which the Service Provider provides certain services („**Main Agreement**“).

This Service Level Agreement („**SLA**“) outlines the service level commitments for the services agreed in the Main Agreement.

- (B) The Parties acknowledge that service delivery may involve multiple providers as sub-providers of the Service Provider. This SLA especially defines the interdependencies between the services and the role of the Service Provider.

Against this background, the Parties agree as follows:

## 1. Definitions

- 1.1 **Force Majeure Event** shall have the meaning given to it in Section 10.
- 1.2 **Incident** shall mean a single event that results in a Malfunction.
- 1.3 **Malfunction** shall mean any breach of an agreed Service Level Objective.
- 1.4 **Planned Downtime** shall mean any non-availability or limited functionality of a Service due to maintenance, repair or upgrade work that is announced by the Service Provider at least 5 days prior to the start of the work.
- 1.5 **Services** means the services agreed within the Main Agreement.
- 1.6 **Service Credit Incident** shall mean any incident where the agreed target value of a Service Level Objective was not reached.



**NOTE TO USER:** Add all additional definition used when filling out this template, e.g. Monthly Uptime Percentage, Downtime.

## 2. Service Description

- 2.1 **Scope.** The Services governed by this SLA are defined within the Master Agreement.
- 2.2 **Responsibilities.** The Parties acknowledge that the provision of the Services may involve multiple providers as sub-providers of the Service Provider. In relation to the Service Recipient, the Service Provider shall act as the lead provider and shall remain fully responsible for the performance of all obligations under this SLA, including those performed by any sub-provider. Unless expressly agreed otherwise, the Service Provider shall ensure that all sub-providers comply with the terms and service levels set out in this SLA and the Main Agreement. Any act or omission of a sub-provider that results in a breach of this SLA shall be deemed an act or omission of the Service Provider.
- 2.3 **Interdependencies.** The Parties agree that the orderly performance of a Service may depend on the performance of one or more other Service(s) and that a Malfunction of a Service („Causing Service“) may be the root cause for another Service („Impaired Service“) having a Malfunction („Interdependency Malfunction“).

2.4 The Parties agree to the following hierarchy of the Services whereby the higher ranked Service is dependent on the performance of the lower ranked Service:

**NOTE TO USER:** Rank the included Services.

Rank	Name of the Service
1	Example: Cloud Application Service
2	Example: Cloud Storage Service
3	
4	
5	
6	

Table 6 – Interdependencies

### 3. SLA Exclusions

- 3.1 This SLA does not apply to Malfunctions caused by
  - (a) Force Majeure Event (as defined below at Section 10);
  - (b) the Service Recipient’s own hardware or software or other technology used in relation to the Services;
  - (c) actions or omissions by or on behalf of the Service Recipient which constitute a breach of the Main Agreement or this SLA; or
  - (d) Planned Downtime.
- 3.2 In case of Interdependency Malfunctions, this SLA shall not apply to the Impaired Service but solely to the Causing Service.

### 4. Service Levels

**NOTE TO USER:** Add a service level for each Service. The service level should be defined by service level objective, service level indicator, the target value and the measurement metric.

**Example for Availability:** The Service availability offered by the Service Provider is an Uptime of  $\geq 99,5\%$  per month („Monthly Uptime Percentage“).

The Monthly Uptime Percentage means the difference between the total number of minutes in a month (as the minuend) and the number of minutes of all Downtime Periods in that month (as the subtrahend), divided by the total number of minutes in that month:

$$\text{(Total number of minutes in a month - number of minutes of Downtime Periods) / Total number of minutes in a month} \times 100 = \text{Monthly Uptime Percentage}$$

## 5. Service Monitoring

- 5.1 The Parties agree that each Service shall be monitored as follows:



**NOTE TO USER:** Add the monitoring means used for each Service.

(„Service Monitoring“)

- 5.2 The Service Provider shall ensure that the Service Recipient has reasonable access to the service monitoring means provided by the sub-providers to Service Provider.
- 5.3 Each Party shall nominate one person of its personnel as a lead SLA contact who shall be responsible for the communication between the Parties in relation to any questions and disputes arising out of this SLA („SLA Lead Contact“).

## 6. Support

- 6.1 The Parties agree that the operating hours of the support for the Services shall be the following:  
X \_\_\_\_\_



**NOTE TO USER:** Add the support operating hours for each Service and how it can be contacted, e.g. phone, email, ticket system, here.

- 6.2 The Parties agree the following response/resolving times for each Service:  
X \_\_\_\_\_



**NOTE TO USER:** Add the specific response/resolving times here.

## 7. Remedies

- 7.1 **Service Credits.** In case of a Service Credit Incident the Service Recipient shall be entitled to receive Service Credits as the Service Recipient's exclusive remedy and the Service Provider's entire liability. The details of the Service Credits are defined in Annex 1.



**NOTE TO USER:** Add a Service Credits definition as Annex 1.

- 7.2 **Claiming.** To receive Service Credits the Service Recipient must notify Service Provider within X \_\_\_\_\_ days from the time the Service Recipient becomes eligible to receive Service Credits whereby such notice must include information allowing the Service Provider to identify the Service Credit Incident and the date and time of the Service Credit Incident.



**NOTE TO USER:** Add the number of days.

- 7.3 **Service Credits Dispute.** In case of a dispute regarding a Service Credit notification the affected Parties shall first escalate the dispute to the SLA Lead Contacts.

## 8. Term and Exit Management

- 8.1 **Term.** The term of this SLA is the same as the term of the Main Agreement („Term“). The Term ends automatically at the end of the term of the Main Agreement.
- 8.2 **Termination.** During the Term, the ordinary right of early termination is excluded. Each Party's statutory right to terminate this SLA for cause without notice remains unaffected.
- 8.3 **Exit Management.** Upon termination or expiry of this SLA for any reason, each Service Provider shall provide reasonable assistance to ensure an orderly transition of the Services to the Service Recipient or to a replacement service provider, as directed by the Service Recipient. This includes, but is not limited to:
- Providing all relevant documentation, records, and information necessary for the transition;
  - Cooperating with the Service Recipient and/or any replacement provider to facilitate the transfer of services and knowledge;

- (c) Ensuring the migration of all Service Recipient data, including backups, to the Service Recipient or to a third party nominated by the Service Recipient, in a commonly used and machine-readable format, within a reasonable timeframe and at a reasonable cost;
- (d) Deleting or returning all Service Recipient data in accordance with the Service Recipient's instructions and applicable data protection laws, subject to any legal retention requirements;
- (e) Providing reasonable support for a period of up to [30/60/90] days following termination or expiry, as agreed between the Parties, to address any issues arising from the transition.

The Service Provider shall not impose any unreasonable restrictions, delays, or additional charges for exit management or data migration services, except as expressly agreed in advance. The obligations in this clause shall survive termination or expiry of the SLA to the extent necessary to complete the exit management process.



**NOTE TO USER:** The exit management clause in 8.3 is only optional.

## 9. Force Majeure

- 9.1 Neither Party shall be liable for any failure or delay in performing its obligations under this SLA if and to the extent such failure or delay results from circumstances beyond its reasonable control ("**Force Majeure Event**"). Force Majeure Events include, but are not limited to:
- Acts of God (such as earthquakes, floods, storms, or other natural disasters),
  - War, hostilities (whether declared or not), invasion, act of foreign enemies,
  - Terrorist acts, civil commotion, riots, or insurrection,
  - Government actions, embargoes, or blockades in effect on or after the date of this SLA,
  - Strikes, lockouts, or other industrial disputes (excluding those involving the affected Party's own personnel),
  - Epidemics or pandemics,
  - Fire or explosion, and
  - Power outtakes or Internet connection failures/outtakes not under the control of the affected Party.

9.2 The affected Party shall notify the other Parties in writing as soon as reasonably practicable, and in any event within X hours of becoming aware of the Force Majeure Event, specifying the nature and expected duration of the event and the steps being taken to mitigate its effects.



**NOTE TO USER:** Add number of hours.

## 10. Additional Terms



**NOTE TO USER:** Only to be used if additional terms are necessary, e.g. regulatory specific terms. Otherwise, clause 10 can be deleted.

## 11. Miscellaneous

11.1 **No Agency.** Nothing in this SLA shall be construed as creating a partnership, joint venture, or agency relationship between the Parties. Neither Party shall have the authority to act for, bind, or otherwise create or assume any obligation on behalf of the other Party for any purpose whatsoever. Each Party acts as an independent contractor and is solely responsible for its own actions, employees, and sub-providers.

11.2 **Written Form.** Any amendment, modification, or supplement to this SLA, as well as any waiver of rights or obligations under this SLA, shall only be valid if made in writing and signed by authorized representatives of all Parties. This requirement for written form may only be waived by a written agreement expressly referring to this clause. For the purposes of this clause, "in writing" includes documents signed by hand or by electronic signature but excludes informal email correspondence.

11.3 **Severability.** If any provision of this SLA is held to be invalid, illegal, or unenforceable by a court of competent jurisdiction, such provision shall be deemed severed from this SLA and shall not affect the validity or enforceability of the remaining provisions. The Parties shall use reasonable endeavors to replace any invalid or unenforceable provision with a valid and enforceable provision that achieves, as far as possible, the original intent and economic effect of the invalid or unenforceable provision.

11.4 **Dispute Resolution.** In the event of any dispute, controversy, or claim arising out of or in connection with this SLA, the Parties shall refer the matter to the SLA Lead Contacts, who shall use reasonable endeavors to facilitate a resolution between the Parties. The SLA Lead Contacts shall have thirty (30) days from the date the dispute is formally notified in writing by either Party to resolve the dispute. If the SLA Lead Contacts are unable to resolve the dispute within this period, either Party may refer the matter to the competent courts as specified in this SLA.

11.5 **Governing Law/Jurisdiction.** This SLA shall be governed by the laws of the Federal Republic of Germany. To the extent permitted by law, the courts of X shall have exclusive jurisdiction for all disputes out of or in relation to this SLA.



**NOTE TO USER:** Please chose a German city which courts should have jurisdiction.



**NOTE TO USER:** Add signature line.

## Annex B: Example Metrics and Dashboards

### Purpose

This Annex provides examples of commonly used Service Level Indicators (SLIs) and corresponding metrics for measuring compliance with Service Level Objectives (SLOs). The examples illustrate how monitoring data can be structured and visualized to enable transparent performance tracking, trend analysis, and

early-warning alerts across providers in both entangled and federated environments.

### Example SLO Categories and Metrics

SLO Category	SLI/Metric	Measurement Method	Typical Target Value	Dashboard Visualization
<b>Availability</b>	Uptime %	Provider telemetry validated by customer probes	≥ 99.9 % per month	Line or area chart showing uptime %, with red thresholds for outages
<b>Performance</b>	95th percentile latency/throughput	Synthetic and real-user measurements from agreed vantage points	≤ 200 ms latency; ≥ 500 req/s throughput	Percentile-latency chart; heatmap per region
<b>Support Responsiveness</b>	Mean Time to Acknowledge (MTTA)/Mean Time to Resolve (MTTR)	Incident-management system timestamps	P1 ≤ 15 min acknowledge; ≤ 4 h resolve	Bar chart or SLA-gauge per priority
<b>Change Management</b>	Timely notification of planned changes	Change-log audit; % of changes announced ≥ 14 days in advance	≥ 95 %	Compliance-trend chart over time
<b>Maintainability</b>	Successful change rate/post-change incident rate	Correlation of change tickets and incidents	< 5 % failed changes	Dual axis chart: changes vs. incidents
<b>Security and Privacy</b>	Time to detect/notify security incidents	SIEM logs and incident records	≤ 1 h to notify customer after confirmation	Timeline of incidents and notification times
<b>Reliability/Resilience</b>	RTO/RPO achieved in testing	Annual DR test reports and audit evidence	RTO ≤ 4 h; RPO ≤ 15 min	Summary table and pass/fail status
<b>Compliance/Auditability</b>	% of metrics with validated data source	Cross-check of logs and evidence repositories	≥ 98 %	KPI dial or compliance scorecard

Table 7 – Example SLO Categories and Metrics

### Dashboard Design Guidelines

- **Transparency:** Display both current status and historical trend ( $\geq 12$  months).
- **Comparability:** Use common units and time frames across providers.
- **Drill-down Capability:** Allow navigation from aggregated KPIs to incident details.
- **Alerting:** Visualize threshold breaches and chronic violations with color coding.
- **Federated Reporting:** Enable data aggregation from multiple providers into a single governance dashboard or “single pane of glass.”

### Example Dashboard Structure

1. **Executive View** – aggregated KPI overview (Availability, Performance, Incidents).
2. **Operational View** – real-time SLI data per provider and service domain.
3. **Compliance View** – audit trail of SLA breaches and remediation status.
4. **Trend View** – 12-month trend analysis with forecasting for capacity planning.
5. **Federated View** – cross-provider comparison using harmonized metrics (see Section 3.4 of the FACIS Taxonomy for SLAs).

### Guidance Note

Actual metrics and dashboards should be implemented according to the organization’s monitoring tooling (e.g., Prometheus, Grafana, ELK, Splunk). This Annex provides a conceptual model for structuring SLI data and visualizations rather than prescribing specific technologies. All metrics must remain traceable to the SLOs defined in Section 7.3 and verifiable through audit evidence.



## Annex C: Glossary of Terms

### Purpose

This Glossary provides definitions of key terms and abbreviations used throughout the SLA Governance Framework Playbook. Its purpose is to establish a common vocabulary for technical, operational, and legal stakeholders involved in the design,

implementation, and governance of Service Level Agreements (SLAs) across multi-provider and federated environments. Definitions are aligned with the FACIS Taxonomy for SLAs and standard industry terminology.

<b>AI Act (Artificial Intelligence Act)</b>	EU regulation establishing a harmonized framework for the development, placement on the market, and use of artificial intelligence systems, introducing risk-based requirements for transparency, safety, accountability, and human oversight.
<b>Back-to-Back Commitment</b>	A contractual mechanism ensuring that obligations and remedies flow consistently from the lead provider to all sub-providers.
<b>Change Management</b>	The controlled process for planning, approving, communicating, and validating service changes to minimize risk and disruption.
<b>Data Processing Agreement (DPA)</b>	A contractual addendum required under GDPR defining obligations for processing personal data between controller and processor.
<b>DORA (Digital Operational Resilience Act)</b>	EU regulation establishing requirements for ICT risk management, incident reporting, testing, and third-party oversight in the financial sector.
<b>Entangled Supply Chain</b>	A traditional service model where a lead provider manages sub-providers in a hierarchical chain, often limiting transparency and accountability.
<b>Exclusion</b>	A framework defining the architectural, operational, and contractual foundations for federated digital ecosystems. It provides a unified taxonomy for SLA governance, focusing on interoperability, accountability, and resilience across independent service providers.
<b>Federated Ecosystem</b>	A cooperative service environment where independent providers interoperate through shared interfaces, aligned metrics, and joint governance structures.
<b>Incident</b>	Any unplanned event that interrupts or degrades normal service operation.
<b>Lead Provider</b>	The primary provider responsible for coordinating sub-providers and consolidating monitoring and reporting within an entangled supply-chain model.
<b>Metric</b>	The quantitative expression used to measure performance of an SLO (e.g., uptime %, latency ms).
<b>Monitoring</b>	The continuous observation of service performance to validate compliance with agreed SLOs using defined SLIs and metrics.
<b>NIS2 Directive</b>	EU directive setting cybersecurity and incident-reporting obligations for essential and important entities across sectors.
<b>Operational Resilience</b>	The ability of a service to continue or recover from disruptions within defined Recovery Time (RTO) and Recovery Point (RPO) objectives.

<b>Remedy</b>	The contractual consequence of breaching an SLO (e.g., service credit, remediation plan, termination right).
<b>SLA (Service Level Agreement)</b>	A formal agreement defining measurable service commitments between a provider and a customer, including objectives, measurement, reporting, and remedies.
<b>SLA Broker/Central SLA Manager</b>	A neutral coordinating entity that harmonizes metrics, validates performance, and manages cross-provider reporting and escalation in federated ecosystems.
<b>SLI (Service Level Indicator)</b>	The metric or method used to measure compliance with a given SLO.
<b>SLO (Service Level Objective)</b>	A specific, measurable target within an SLA, describing the desired level of service (e.g., availability $\geq 99.9\%$ ).





## Annex D: Legal and Regulatory Frameworks

### Purpose

This Annex provides an overview of the key legal and regulatory frameworks that influence SLA design and governance in multi-provider environments. Its purpose is to ensure that SLA clauses are traceable to applicable obligations and that providers can demonstrate compliance, accountability, and operational resilience in line with supervisory expectations. SLAs are not stand-alone legal instruments; they complement the

overarching contractual framework – particularly the Master Services Agreement (MSA), Data Processing Agreement (DPA), and Security Annex – by translating regulatory requirements into measurable, auditable service-level commitments.

### Applicable Frameworks

Framework	Core Obligations	Relevance for SLAs
GDPR (General Data Protection Regulation)	Lawful processing, data-minimization, data-subject rights, breach notification within 72 h, and transfer restrictions.	Reference to DPA, define SLOs for breach notification timelines, data-handling, and sub-processor transparency.
NIS2 (EU Directive on Security of Network and Information Systems)	Security of networked systems, incident management, and reporting of significant incidents within 24 h/72 h.	SLO: Information Security/Incident Reporting, joint escalation and notification procedures.
DORA (Digital Operational Resilience Act)	ICT risk management, testing, and oversight of third-party service providers.	SLO: Reliability/Operational Resilience, obligations for testing, audit rights, and continuity.
AI Act	Transparency, data governance, and accountability for high-risk AI systems.	Optional SLOs for explainability, data-quality, and auditability when AI components are part of the service.
ISO 27001/ISO 22301	Information-security and business-continuity management standards.	Aligns measurement and audit requirements, referenced as baseline for certification and control validation.

Table 8 – Applicable Frameworks

### Guidance Note

The alignment between regulatory requirements and SLA clauses is illustrated throughout this Playbook – particularly in Section 7.3 and in Annex A (Generic SLA Template). This Annex provides a high-level orientation and does not replace detailed

legal mapping or analysis. Organizations should verify applicable frameworks per jurisdiction and ensure consistency across all related documents – including DPA, Security Annex, and sector-specific addenda.

## Annex E: Sector-Specific SLA Adaptation – Methodology and Example

### Purpose and Approach

This annex provides a practical method for tailoring the base SLA to meet sector-specific or regulatory obligations. Rather than listing all applicable laws or standards – which would be impossible to maintain across jurisdictions, this annex illustrates how legal and operational requirements can be translated into measurable SLA parameters. Teams should apply this approach whenever a service operates in a regulated domain such as healthcare, financial services, mobility, or the public sector.

#### Key Principles

**Traceability:** Every SLA clause addressing a regulatory requirement should clearly reference its source (e.g., directive, standard, or supervisory guidance).

**Proportionality:** The SLA should scale obligations to the criticality and regulatory exposure of the service.

**Verifiability:** Each added requirement must be measurable and evidenced.

**Isolation:** Sector-specific clauses should be grouped in a dedicated annex rather than embedded in the base SLA to preserve modularity.

### Step-by-Step Methodology for Sector-Specific Customization

- **Identify the Applicable Frameworks:** Determine which laws, regulations, or standards apply to the service (e.g., GDPR, NIS2, DORA).
- **Extract Operationally Relevant Requirements:** Focus on obligations that can be measured or evidenced operationally – such as recovery time, auditability, reporting, or data segregation.
- **Map to SLA Dimensions:** Align each requirement to the appropriate SLA category (availability, incident response, data protection, audit, continuity, etc.).
- **Define Verifiable Parameters:** Translate the legal or policy statement into measurable targets with defined metrics, time windows, and evidence requirements.
- **Validate with Stakeholders:** Review the draft with compliance, legal, and operations teams to ensure the obligations are satisfactory, realistic, enforceable, and consistent with existing controls.
- **Document as Sector Annex:** Insert the customized clauses into a dedicated annex referencing this methodology, preserving the same base structure.

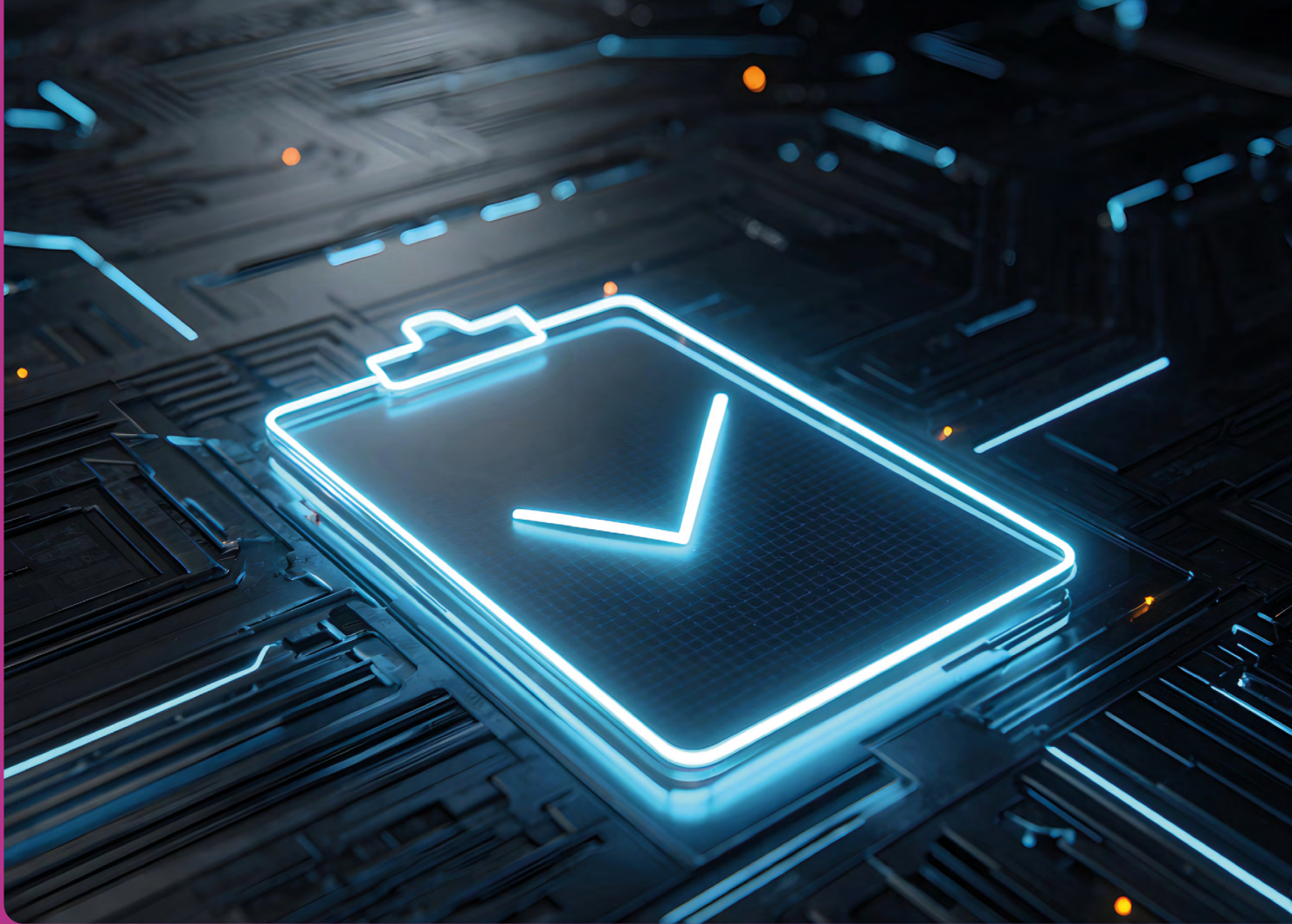
### Illustrative Example: Healthcare Services

Source obligation (simplified):  
Clinical systems must ensure data integrity, traceability of access, and guaranteed incident notification to medical staff within defined timeframes.

### Mapping Process

Regulatory Driver	SLA Dimension	Derived Obligation	Measurement/Evidence
Health data traceability	Security/Audit	"Provider shall maintain detailed access logs for all clinical data operations and retain them for at least 12 months."	Periodic audit report, log export
Critical incident notification	Incident Response	"Critical incidents affecting patient care must be communicated to designated clinical staff within 1 hour."	Incident records, notification logs
Data integrity	Data Protection	"Provider shall validate transactional integrity of medical records daily and provide verification reports."	Daily validation job, attestation report

Table 9 – Example



Resulting SLA language (example):

“For healthcare-related workloads, the Provider shall ensure that all access to patient data is fully logged and auditable for a minimum of twelve (12) months. Any incident classified as affecting patient safety or clinical workflows shall be notified to designated medical contacts within one (1) hour of detection. The Provider shall perform automated integrity checks of clinical data stores at least once per day and provide monthly summaries as evidence.”

Commentary:

This example shows how sector-specific obligations can be embedded within the same SLA structure – Availability, Incident, Security, Reporting – without rewriting the entire agreement. Other sectors (financial services, automotive, public sector) can apply the same pattern, replacing the regulatory driver and operational parameters.

#### **Template for a Sector Annex**

Each project or program may create its own Sector Annex following the same format:

- Section 1: Reference frameworks (laws, standards, or supervisory guidance)
- Section 2: Risk and criticality mapping
- Section 3: Derived SLA parameters and evidence obligations
- Section 4: Validation and review process

This structure allows consistent customization while keeping the Playbook itself evergreen.

#### **Maintenance and Review**

Sector Annexes should be reviewed annually or whenever major regulatory changes occur. Ownership should rest with the organization’s SLA Governance or Compliance Lead. Updates are approved through the same governance channels as SLA template revisions to ensure alignment and version control.

