Master Service Agreement (MSA)

This Master Service Agreement (MSA) is entered into between GMS Management Solutions S.L. (or "**MS**" or "**THE PROVIDER**") and the other party, the client (or "**THE CLIENT**"). By signing an Order Form, the Client accepts the terms of this MSA.

Definitions

The following terms will have the meanings set out below:

- **Agreement:** Refers to this **Master Service Agreement**, for **SIRO-GRC**, which includes the standard Service Level Agreement, Security and Personal Data Protection clauses, and any Annex, Addendum, or document that the Parties attach or incorporate.
- **Authorized Users:** Refers to the personnel designated by THE CLIENT that remotely may access to and use the **SIRO GRC Software as a Service**. THE CLIENT is responsible for their identification and authentication.
- **Client Content:** Refers to any data, including text files or information, uploaded to the **SIRO GRC Software as a Service** platform for processing or storage by THE CLIENT or any party authorized by THE CLIENT. It does not include usage or telemetry data generated by THE PROVIDER for infrastructure monitoring.
- **Contract**: Refers to this **Agreement** and **Statement of Work** together. The Contract is a document that is signed and accepted in its entirety by both parties.
- **Contracted Modules**: Refers to the subset of the **SIRO GRC Modules** that under the scope of the agreement.
- **Documentation:** Refers to the written user manuals, online help, and guides for the **Contracted Modules** of **SIRO GRC**.
- **Purchase Order:** Refers to the document representing the purchase of the **Subscription** to the **SIRO GRC Contracted Modules**.
- **Service Level Agreement**: Refers to quantifiable objectives / metrics for the **SIRO GRC Software, Professional and Support Services** that the PROVIDER commits to achieve while providing the Services.
- **SIRO GRC**: Refers to the commercial name of the software platform that is offered as a service and to which this **MSA** makes reference. SIRO GRC is a Governance, Risk and Compliance Solutions that covers also Internal Audit, Business Continuity and Insurance Portfolio management.
- **SIRO GRC Modules:** Refers to the following blocks of functionality of **SIRO GRC**:
  - Operational Risk
  - Compliance
  - Business Continuity
  - Internal Audit
  - Cybersecurity
  - Privacy
  - Third Party Management (Outsourcing)
  - Insurable Operational Risk
  - Climate Risk on Physical Assets
- **SIRO GRC Professional services**: Refers to any consulting services, implementation, integration, migration, training, or any other than the **SIRO GRC Sorftware as a Service** requested by THE CLIENT

- **SIRO GRC Software as aService or SaaS**: Refers to the limited, non-exclusive, non-sublicensable, non-transferable license to use the Contracted Modules of SIRO GRC service hosted and supported by THE PROVIDER.
- **SIRO GRC Support Services**: Refers to the support and corrective maintenance services of the **SIRO GRC Software as a Service** according to the SLAs established in the **Contract** and any evolutionary services or additional modules outside the scope of the **Contract** that might be required by THE CLIENT.
- **Statement of Work or SoW**: Refers to document that specifies the details for the provision of the **SIRO GRC Software as a Service**, and the required **SIRO GRC Professional Services** and **SIRO GRC Support Services**.
- **Subscription:** Refers the user of **Authorized Users** to acess and utilize the **SIRO GRC Software as a Service** during the term of the **Contract**.

1 Scope of Services

1.1 License Subscription

THE PROVIDER grants THE CLIENT a limited, non-exclusive, non-sublicensable, non-transferable license to use the contracted modules of the **SIRO GRC Software as a Service**, subject to the terms and conditions of the **Contract**, solely for THE CLIENT's internal purposes, and not for subsequent commercialization. The CLIENT may designated the **Authorized Users** that will be able to remotely access and use the Service.

1.2 Scope of the Service

The Service, unless othewise stated in the **Contract**, includes remote access to SIRO, corrective maintenance, user support, and cloud administration. The Service also includes all the **SIRO GRC Professional Services** explicitly present in the **Contract**, such as consultancy services, custom developments, integrations with external systems.

Evolutionary maintenance is optional and at an additional cost.

1.3 Use of the Service

The CLIENT is responsible for: (i) any usage of the Service that occurs using the credentials of its **Authorized Users**; (ii) the **Client Content**; and (iii) the compliance of its **Authorized Users** with the **Agreement**. The CLIENT is also responsible for the security of its own network and systems.

The PROVIDER shall not be liable for any damage caused by persons or systems who were not authorized to use the **SIRO GRC Software as a Service**, but who were able to do so using usernames, passwords, or accounts provided to the CLIENT by reasons beyond the PROVIDER's control.

1.3.1 Client Complementary Controls

The CLIENT shall be responsible for implementing and maintaining the following additional controls:

- **Credential Management**: including the use of Multi-Factor Authentication (MFA) and any other technical measures aimed to protect the confidentiality of all assigned credentials and access keys.
- **Internal Access Control**: Define, assign, and monitor the access roles and permissions of its **Authorized Users** within the **SIRO GRC Software as a Service** application, adhering to the principle of least privilege.
- **Endpoint Security**: Ensure that all devices used by its **Authorized Users** to access the **SIRO GRC Sofware as a Service** are properly protected with antimalware software, up-to-date patches and all the reasonable security related techical measures.

1.4 Usage restrictions

The CLIENT may not, under any circumstances:

- Download, decompile, disassemble, or modify the **SIRO GRC Software as a Service**, in whole or in part.
- Use a non-production environment for production purposes.
- Use the **SIRO GRC Software as a Service** for purposes that violate intellectual property rights or applicable laws.
- Perform penetration testing, scanning, or benchmarking without the prior written consent of the PROVIDER.

2 Software Property Rights

2.1 Propiedad del Servicio

The PROVIDER retains all rights, titles, and interests in and to the **SIRO GRC Software as a Service** and all its component parts, modifications, versions, updates, and derivatives, including all associated intellectual property rights (patents, copyrights, trade secrets, trademarks, and other intellectual property rights associated with the Software).

Nothing in this Agreement shall be construed as transferring to the CLIENT any ownership rights in the Software.

2.2 Client Content Property

The CLIENT retains all rights, titles, and interests in and to the **Client Content**. The PROVIDER shall have a limited, non-exclusive license to use the **Client Content** solely for the purpose of providing the Service and fulfilling its obligations under the **Agreement**.

2.3 *Feedback*

The CLIENT may communicate to the PROVIDER suggestions, comments, improvement proposals, recommendations, or any other information relating to the **SIRO GRC Software as a Service** (hereinafter, the “Feedback”).

The CLIENT grants the PROVIDER an irrevocable, perpetual, worldwide, non-exclusive, sublicensable, and royalty-free right to use, reproduce, modify, adapt, incorporate, exploit, and commercialize such Feedback as part of the **SIRO GRC Software as a Service** platform. The PROVIDER may use the Feedback without restriction, provided that such use does not directly or indirectly identify the CLIENT or disclose any of the CLIENTS’s Confidential Information.

3 Fees and Payments

3.1 Fees

The CLIENT will pay the PROVIDER the **SIRO GRC Software as a Service** license fees and other financial terms set forth in the **Contract**. The fees include cloud hosting, maintenance, and support, including security updates and general improvements.

3.2 Taxes

The Service fees are exempt from any sales tax, VAT, usage tax, or similar charges. The CLIENT will pay or reimburse the PROVIDER for all applicable taxes, so that the PROVIDER receives the net amount stated in the **Contract**.

4 Temporal Suspension

4.1 General

The PROVIDER may suspend the CLIENT’s use of **SIRO GRC Software as a Service** if the CLIENT breaches the terms of the **Contract**, including payment of the fees, and fails to remedy the breach within a period of **30 days**. The suspension will only apply to the Service that is the subject of the breach.

5 Term and Termination

5.1 Term

The **Contract** shall enter into force on the date of its signature and shall remain in effect until the expiration of the **SIRO GRC Software as a Service** (and **SIRO GRC Support Service** if contracted), with an initial term of **one (1) year**, renewable for identical periods, unless one of the Parties notifies

the other of its intention not to renew the **SIRO GRC Software as a Service (and SIRO GRC Support Service)** at least sixty (60) days prior to any renewal or extension thereof.

5.2 Termination

Either Party may terminate the **Contract** by written notice if:

- The breaching Party fails to remedy the manifest breach of any of its obligations within 60 days of notification of breach.
- The Party is included on the **OFAC Sanctions List** maintained by the US DoT.

5.3 Effect of Termination

- **Return of Information**: Upon termination, the **Client Content** will be returned and deleted from the PROVIDER's systems using a secure deletion method, along with the necessary documentation.
- **•Maintenance of the Cloud Environment**: If the PROVIDER terminates the contract before the end of the initial term or any of its extensions, a transition plan will be established with the CLIENT so that all stored information is returned in a mutually agreed-upon format. The PROVIDER is obligated to maintain the cloud environment available for the duration of the transition, which shall not exceed two months.
- **Destruction of Infrastructure and Client Content**: Upon termination of the contractual relationship between the CLIENT and the PROVIDER, the latter will destroy all the **Client Content** in its possession and securely erase or delete the cloud infrastructure, including the data it contains.
- **Failure to comply with the Notice Period**: If THE CLIENT fails to comply with the notice period to early terminate the **Contract**, the CLIENT will be obliged to pay the proportional price equivalent to 2 months of maintenance of the annual price.

6 Guarantees

6.1 Service Guarantee

The PROVIDER shall be diligent in correcting any verifiable and reproducible significant defect that may be identified by any party at no additional cost to the CLIENT.

6.2 Guarantee of Tested Service Continuity

The PROVIDER guarantees:

1. **Documented Policies**: The PROVIDER maintains Business Continuity / Disaster Recovery Plans (BCP / DRP) for the **SIRO GRC Software as a Service** which are reviewed annually.
2. **Periodic Testing**: The PROVIDER conducts comprehensive testing of the DRP and BCP at least once a year. The results of these tests are documented, evaluated, and any deficiencies are remedied promptly.
3. **Sharing Results**: The PROVIDER will provide the CLIENT, upon request, a summary of the DRP/BCP test results for the CLIENT's audit purposes.

6.3 Processing Integrity Guarantee

The PROVIDER guarantees that the **SIRO GRC Software as a Service** has been designed to process the CLIENT's data comprehensively, timely and accurately, as described in the **Documentation**. The PROVIDER will maintain controls to monitor critical application processes and correct any deviations in processing integrity in accordance with the **SLA**.

The PROVIDER will maintain documented procedures to verify the accuracy and integrity of the results, reports, and critical calculations generated by the **SIRO GRC Software as as Service** before they are

made available to the CLIENT, confirming that they comply with the agreed-upon specifications and business logic.

7 Limitation of Liability

The total liability of THE PROVIDER shall not exceed the fees charged for the affected **SIRO GRC Software as Service**, except in cases of fault, negligence, or willful misconduct confirmed by a court judgment. In any event, THE PROVIDER shall not be liable under any circumstances for lost profits, consequential damages, or opportunity costs. Notwithstanding the foregoing, the limitation of liability established herein shall not apply to damages arising from a breach of the security, confidentiality, and personal data protection obligations set forth in the Personal Data Protection Clause of the **Contract**.

THE PROVIDER's liability to THE CLIENT in relation to the Services is conditional upon the CLIENT submitting a written claim, specifying in sufficient detail the nature of the claim and the amount claimed.

The PROVIDER does not guarantee and will not be liable for third-party products or services (unless contracted by the PROVIDER for the provision of the service). Any claim of the CLIENT in this regard shall be against the third-party providers, with the PROVIDER being held fully harmless.

The PROVIDER assumes no responsibility for the reliability, availability, or security of the Internet or systems of the CLIENT or third parties, or of hardware, that are not within the scope of the **Contract**.

Furthermore, THE CLIENT assumes full responsibility, holding THE PROVIDER harmless, for:

- Determining the existence of, and complying with, import / export controls; requirements for obtaining and maintaining licenses and other permits, as they are applicable to transactions, commerce, electronic processes, or activities conducted via the Internet or any electronic network (“Transactions”).
- Requirements for assessing, paying, or withholding taxes, customs duties, or other charges or levies; and any other laws or regulations in any competent jurisdiction;
- The security of its network and any related systems, including the security, privacy, and confidentiality of any data, intellectual property, or other information belonging to THE CLIENT or third parties;
- To establish and determine the validity and enforceability of the processes of signing and executing contracts, as well as any other documentation necessary for or used within the framework of the Transactions;

8 Confidentiality and Security

8.1 Confidentiality

The Parties shall maintain as **Confidential** all proprietary information, trade secrets, or information identified as such, including **Customer Content**, using it only for the execution of this Agreement. The PROVIDER agrees to indemnify and hold harmless the CLIENT from any disclosure of Confidential Information of the CLIENT or its clients.

If one Party is legally obligated to disclose any Confidential Information provided by the other Party, it shall promptly notify the other Party in writing, to the extent legally permitted, so that the other Party may take appropriate administrative, judicial, or extrajudicial actions to attempt to prevent the disclosure. If it is not legally possible to prevent disclosure, the Party obligated to disclose the Confidential Information agrees that only the portion of the Confidential Information that must be legally disclosed will be disclosed, and all reasonable steps will be taken to ensure that it is treated confidentially.

This confidentiality obligation shall apply even after the termination of the **Contract**.

The PROVIDER agrees that once it has used the **Client Content** to perform the Services, it will proceed as described in the clause 5.3. “Effect of Termination”

The PROVIDER hereby acknowledges and understands that the content of this **Contract** does not suggest, imply, or grant any right to the PROVIDER to use the CLIENT’s name, trademarks, logos, trade names, patents, or intellectual property in general. Likewise, the CLIENT hereby acknowledges and understands that the content of this **Contract** does not suggest, imply, or grant any right to use the PROVIDER's name, trademarks, logos, trade names, patents, or intellectual property in general.

The PROVIDER agrees to hold the CLIENT harmless from any disclosure of **Client Content**, whether due to cyberattacks, operational failures, internal fraud or any other cause.

8.2 Required Security Measures

The PROVIDER commits to implement the following security measures:

- **Encryption at rest**.Secure encryption of the information used to deliver the **SIRO GRC Software as a Service**.
- **Identity management**; Access with personally identifiable user accounts and credentials subject to a renewal policy.
- **Malware control** Antivirus, anti-spam, software installation restrictions, browsing control.
- **Patch policy**. Zero-day policy for applying security patches.
- **Secure communications**: Use of VPN and secure protocols with encryption.
- **Penetration tests and vulnerability scanning**:• Annual scanning of external and internal vulnerabilities with defined closure deadlines (Urgent: 4 days; Critical-High: 30 days; Medium: 90 days).
- **Audit logs**: Changes records containing at least: user identifier, date and time, action description, and IP address identifier.
- **Cryptographic Management**: THE PROVIDER maintains a formal policy and procedures for managing the cryptographic key lifecycle, including generation, secure storage, periodic rotation, and revocation for all keys used to encrypt CLIENT information and Service communications. It will be ensured that master encryption keys are kept separate from the development and operations functions of the **SIRO GRC Software as a Service**.

8.3 Segregation of Duties

The PROVIDER shall maintain a documented Segregation of Duties structure to mitigate the risk of material error or fraud in critical processes. This includes, but is not limited to, the separation of responsibilities between:

1. The Software Development/Testing function and the Operations / Administration (DevOps) function.
2. Individuals with privileges to administer the system and individuals who manage customer data (Confidentiality).
3. The Change Management (Authorization) function and the Change Implementation function.

8.4 Change and Configuration Management

The PROVIDER agrees to maintain and operate a formal **Change Management Procedure** for all infrastructure, application, and security configuration of the **SIRO GRC Softare as Service**. This process includes, but is not limited to:

1. **Request and Approval**: All changes are documented, their potential impact assessed, and approved by an authorized role before implementation.

2. **Testing and Rollback**: Appropriate testing performed in non-production environments before production implementation. A documented rollback plan must be part of every change request.
3. **Security Review**: Changes related to security, infrastructure that may impact the security of the **Client Content** are reviewed by the Security team before implementation.

8.5 Right of Audit and Verification

Right of Verification: THE CLIENT or its designated auditor shall have the right, upon reasonable request (at least 30 days in advance), and with a frequency not exceeding once a year, to conduct a limited review of THE PROVIDER's relevant security documents and policies, provided that such review is carried out during working hours, does not interfere with operations, and the costs are borne by THE CLIENT.

9 Personal Data Protection / Privacy

9.1 Role and Purpose

The PROVIDER acts as the **Data Processor** with respect to the personal data of the CLIENT, which assumes the role of **Data Controller** for this **Agreement**.

The data subjects to which the personal data belongs are the **Authorized Users** of the system, employees of third party personnel contracted by the CLIENT. The purpose of the processing is to Store and to Query the data with the objective of fullfilling the delivery of **SIRO GRC Software as a Service**. The types of personal data is Personally Identifiable Data: user id, email, first and last name.

The PROVIDER does not inspect any other information that the CLIENT utilizes in the system and does not make any assumption about whether **Personally Idenfitiable Data** is present in the System..

The PROVIDER will process the personal data exclusively on behalf of the CLIENT and in accordance with its instructions.

The PROVIDER, in its role of Personal Data Processor, declares and guarantees to the CLIENT the following:

a) That it has sufficient technical capacity to fulfill the obligations arising from the **Contract** in full compliance with regulations on the protection of personal data, and may commit, to the extent required for the provision of the **Services**, to comply with the requirements of current personal data processing regulations.
b) That it will maintain the **secrecy and confidentiality** of the personal data under the CLIENT's responsibility to which it will have access.
c) That it will process the personal data to which it will have access exclusively on behalf of the CLIENT and, in any case, in accordance with the instructions transmitted to it by the CLIENT. Likewise, it undertakes to use said data solely for the provision of the Services and, consequently, not to use or apply it in any way that exceeds said purpose.
d) That it will not **disclose to third parties**, even for storage purposes, the data to which it has access by virtue of providing the Services, nor any processing, evaluation, or similar procedures carried out with said data, nor will it duplicate or reproduce all or part of the information, results, or relationships concerning said data, except in those cases where legally required.
e) That it will ensure that the persons authorized to process personal data expressly and in **writing commit** to respecting confidentiality. To this end, THE PROVIDER will keep available to THE CLIENT the documentation proving compliance with the obligation established in this paragraph.
f) That it will ensure the necessary **training** in personal data protection for the persons authorized to process personal data under its supervision.
g) That it will support the CLIENT in carrying out **Data Privacy Impact Analysis** relating to the personal data to which it has access, where applicable.

h) That it will support the CLIENT in carrying out **prior consultations** with the Control Authority, where applicable.

i) That, should the PROVIDER consider that compliance with a particular instruction received from the CLIENT could entail a breach of the current Personal Data Processing Regulations or any other applicable regulations that modify or supplement them, the PROVIDER shall immediately inform the CLIENT and request that the CLIENT withdraw, amend, or confirm the relevant instruction. The PROVIDER may suspend the application of the relevant instruction pending the CLIENT's decision regarding the withdrawal, amendment, or confirmation of the corresponding instruction.

j) Upon termination of the Services, and at the CLIENT's request, the PROVIDER shall immediately delete, as instructed by the CLIENT, all personal data to which it has had access, as well as any documents or media containing such data. Specifically, the PROVIDER undertakes to delete: (i) data included in files under the CLIENT's responsibility, which the CLIENT has made available to the PROVIDER as a result of the provision of the Services; (ii) any data generated as a result of the PROVIDER's processing of data under the CLIENT's responsibility; and (iii) all media or documents containing any of such data. Data shall not be destroyed when there is a legal obligation to retain it, in which case the PROVIDER shall return the data to the CLIENT, as instructed by the CLIENT, who shall be responsible for ensuring its retention.

k) That it will assist the CLIENT when requested, providing any information and/or documentation necessary for the appropriate response to the exercise of the rights of access, rectification, erasure, objection, restriction of processing, and/or data portability that it may receive from interested parties, all within reasonable timeframes and, in any case, with sufficient advance notice to allow the CLIENT to comply with the legally applicable deadlines for addressing said rights.

l) That, in those cases where the PROVIDER receives a request directly from the data subject for access, rectification, erasure, objection, restriction of processing, and/or portability, it undertakes to forward said request to the CLIENT so that the latter may address it within the legally established timeframes.

m) The PROVIDER undertakes to maintain strict confidentiality regarding the personal data of the CLIENT or third parties that are delivered or transferred to it in connection with the performance of this Contract.

n) That it will maintain a **Record of the Categories of Processing Activities** carried out under the **Contract**, containing:
   - The name and contact details of the PROVIDER and the CLIENT and, where applicable, of the CLIENT's and the PROVIDER's Data Protection Officer;
   - The categories of processing carried out under the Contract;
   - The identification of any International Data Transfers that may be carried out for the provision of the Service.

o) That it will not carry out **International Transfers** of personal data to which it has access under the responsibility of the CLIENT, unless they are duly regulated or authorized by the CLIENT.

p) That the PROVIDER will have a general description of the technical and organizational security measures.

Furthermore, the PROVIDER undertakes to implement all applicable technical and organizational security measures, based on the data processed and in accordance with current Personal Data Processing Regulations and any other applicable regulations that modify, supplement, or replace them. In the specific context of this relationship, following the relevant risk analysis, the PROVIDER shall implement the security measures deemed appropriate, as described in the **Contract**.

These security measures, and any others that may be implemented, may be modified at the CLIENT's request solely to adapt them to regulatory changes or variations in the type of personal data to which the PROVIDER will have access.

If, after the execution of the corresponding Contract, the CLIENT requires the PROVIDER to adopt or maintain security measures different from those agreed upon, or if such measures are mandated by any future regulations, and this significantly affects the costs of providing the services contracted under the Contract, the PROVIDER and the CLIENT will agree on the appropriate measures to resolve the situation and the effect that such modifications may have on the prices of the services covered by the **Contract**.

In accordance with data protection legislation, the PROVIDER will be considered responsible for the processing of personal data if it uses the data for other purposes, discloses it, or uses it in breach of the stipulations of this **Contract**, and will be liable for any infringements it has personally committed.

The Parties will process the personal data of signatories to this **Agreement** based on their legitimate interest, solely for the purpose of maintaining this relationship and for its duration. They may subsequently retain this data in a blocked state for the periods applicable to any legal actions related to such processing. Data subjects may exercise their rights of access, rectification, erasure, restriction of processing, and objection at any time by contacting the processing party at the address indicated in the preamble to this **Agreement**. They may also contact the competent authority to assert their rights. For your information, the signatories' data will not be transferred to any third party.

9.2 Personal Data Breaches

The PROVIDER shall notify the CLIENT of any personal data breaches or security incidents without undue delay and no later than twenty-four (24) hours after its detection. The notification must include the nature, categories, and approximate number of data subjects and records affected, the consequences, and the measures taken or proposed.

In this regard, if available, the following information shall be provided as a minimum:

- Description of the nature of the data breach, including, where possible, the categories and approximate number of data subjects affected, and the categories and approximate number of personal data records affected;
- Name and contact details of the Data Protection Officer or other contact person where further information can be obtained;
- Description of the likely consequences of the data breach; and
- Description of the measures taken or proposed to remedy the data breach, including, where applicable, measures taken to mitigate its possible adverse effects.

Furthermore, it will assist the CLIENT, in the event of a personal data security breach, in order to ensure compliance with the obligations to notify a personal data security breach in accordance with the current Personal Data Processing Regulations and any other applicable regulations that modify, supplement or that may be enacted in the future.

9.3 Subcontracting

Neither Party may assign its rights and obligations under this Agreement to third parties without the prior written consent of the other Party.

The PROVIDER shall not subcontract the Services to third parties, except with the prior written authorization of the CLIENT, or if the Services are essential ancillary services, or if they are subcontracted to any entity belonging to the PROVIDER’s Group of Companies. The PROVIDER assumes full responsibility to the CLIENT for any breach of contract by the sub-processor.

If the PROVIDER needs to subcontract any processing, it shall be obligated to inform the CLIENT of the services and processing it intends to subcontract, the identity of the subcontractor, and its contact information. The PROVIDER must provide this notification at least two weeks prior to signing the subcontract, during which time the CLIENT may object to the subcontracting. The Sub-processor shall also be subject to the obligations imposed on the PROVIDER in this Agreement and to any instructions given by the CLIENT. In this regard, the PROVIDER is obligated to formalize the sub-processor relationship and the sub-processor's obligations in a contract signed by the PROVIDER and the sub-processor, which complies with the formal requirements contained in this Agreement. In the event of a breach by the sub-processor of its data protection obligations, the PROVIDER shall assume full responsibility to the CLIENT for such breaches, as if the breach had been committed by the PROVIDER.

9.3.1 Security Commitments of the Sub-Processor

The PROVIDER undertakes that any Sub-processor (or Subcontractor) contracted for the provision of the Services will maintain a level of security and compliance equivalent to or greater than the commitments established in this **Contract**, including, without limitation, obtaining and maintaining a recognized security certification (e.g., SOC 2, ISO 27001).

9.3.2 Availability of SOC2 Reports

The PROVIDER will provide the CLIENT, upon request and under a confidentiality agreement, with the security audit reports (e.g., SOC2 Report or similar) of the Sub-processors that provide the infrastructure or primary storage of the **Client Content**, to the extent that the PROVIDER has the right to disclose such reports.

10 Miscellaneous

10.1 Applicable Legislation

The Contract is governed by and construed in accordance with **Spanish law**.

10.2 Jurisdiction

All disputes will be submitted to the **Courts and Tribunals of Spain**, waiving any other jurisdiction.

10.3 Force Majeure

Neither Party shall be liable for failure to perform its contractual obligations (except payment) if such failure is caused by force majeure as defined in Article 1105 of the Spanish Civil Code.

10.4 Security Governance Oversight

The PROVIDER guarantees that **SIRO GRC Software as a Service Management** actively oversees security risk management and regulatory compliance. This includes the annual review and approval of the Security Policy and the Risk Management Program for the SIRO service.

10.5 Order of precedence

In the event of a conflict, the provisions of the Contract/Order Form shall prevail over the provisions of this MSA.

11 Service Levels

11.1 SLA for Service Availability

- **SLA**: Maximum unjustified downtime: **0.5%** during business hours and **5%** outside of business hours.
- **Justified Exclusions**: Force majeure, transmission errors beyond the PROVIDER's control, internet or CLIENT network failures, and maintenance outages with prior notice (2 business days in advance, except in emergencies, and outside of the CLIENT's business hours).

- **RPO** (Recovery Point Objective): **24 hours**.
- **RTO** (Recovery Time Objective): The service will be recovered within **6 hours**.
- **Credit**: 3% of monthly fees in the form of upgrade credits if availability falls below 99.5% (business hours) or 95% (non-business hours).

11.2 SLA for Incident Resolution

Incident type	Severity definition	Maximum Response Time (Business Hours)	Maximum Temporary Workaround Time (Business Hours)	Maximum Time to Solution (Business Hours)
Critical	The production system is down, or a key functionality is inoperable or materially affected, and more than one user is impacted.	2h	4h	12h
High	The production system or a key functionality is materially affected, but the system is still usable, and more than one user is affected.	2h	6h	24h
Medium	The system is available, but a single user or non-critical processes are negatively impacted.	4h	12h	40h
Low	Does not materially affect access or use, or a reasonable solution exists.	8h	16h	80h

- **Compliance Target** (Response and Resolution): 95% of reported incidents.
- **Credit**: 3% of monthly fees in the form of upgrade credits if the SLA target for response or resolution is not met.

11.3 Commitment to Competence and Training

The PROVIDER agrees to:

1. **Recruitment and Screening**: Implement a selection process that includes background checks for its personnel, in accordance with applicable laws and the sensitivity of their roles.
2. **Ongoing Training**: Ensure that all personnel who access, develop, operate, or manage the **SIRO GRC Software as a Service** environment receive initial and recurring training in: (i) information security awareness, (ii) ethics, and (iii) procedures for handling the CLIENT's confidential data.
3. **Documented Responsibility**: Clearly define and communicate security and compliance responsibilities to all employees, auditing their compliance through performance evaluations.