Information Security Management System:
ISO/IEC 27001:2022

Sustainability Solutions SL

Initial Certification Stage 2 Audit Report
June 18, 2026

Table of Contents

Contact Information and Audit Criteria 3
Opening & Closing Meetings 5
Management System Audit Time 6
Audit Summary 7
Audit Conclusions 10
Documents Reviewed and Audit Trail 11
Conformance Testing Results 14
ISO/IEC 27001:2022 Mandatory Clauses 14
ISO/IEC 27001:2022 Annex A Controls 21
Findings 27
Details of Findings 28

© 2025 Insight Assurance LLC - All Rights Reserved
This document may contain proprietary information and may only be released to third parties with approval of management.

Contact Information and Audit Criteria

Client	
Company Name	Sustainability Solutions SL
Company Address	Buenos Aires 38, sobreatico 4ta, 08036 Barcelona, Spain
Company Description	Manglai is an AI-powered environmental management platform that helps companies measure, analyze, and reduce their carbon footprint, water usage, and waste. It centralizes ESG (Environmental, Social, and Governance) data to automate reporting, ensure regulatory compliance (such as CSRD), and streamline sustainability audits.
Company Contact Name	Andres Cester, CEO
Location(s) in Scope of the Certification	Buenos Aires 38, sobreatico 4ta, 08036 Barcelona, Spain
Certification Company	
Company Name	Insight Assurance, LLC.
Company Address	400 N Tampa St, Suite 129, Tampa, FL 33602
Company Contact Name	Mario Vlieg, Senior Director
Audit Team	
Lead Auditor Name	Alvaro Tejada
Audit Team Members	N/A
Others	N/A
Audit Criteria and Objectives	
Audit standard(s) to be certified	ISO/IEC 27001:2022
Additional audit criteria	ISO/IEC 17021-1:2015 ISO/IEC 27006-1:2024 Insight Assurance Certification Terms and Conditions
Type of audit	Initial Certification Stage 2
Audit objectives	**Stage 2 Objectives:** 1. To determine the effectiveness of the management system 2. To ensure the client has implemented applicable controls and established management system objectives based on the risk assessment. 3. To confirm that the management system conforms with all the applicable requirements of the audit standard(s) and criteria; 4. To confirm that the organization has effectively implemented its planned arrangements.

© 2025 Insight Assurance LLC - All Rights Reserved
This document may contain proprietary information and may only be released to third parties with approval of management.

	5. To confirm that the management system conforms to the organization's own policies, procedures and objectives. 6. Evaluation of the ability of the management system to ensure the organization meets applicable statutory, regulatory, and contractual requirements; 7. If applicable, to identify areas for potential improvement of the management system; 8. To determine the effectiveness of the management system to ensure the client can reasonably expect to achieve its specified objectives;
Areas of Focus	Include but are not limited to: **ISO/IEC 27001:2022 Areas of Focus:** 1. Top management leadership and commitment to information security policy and the information security objectives; 2. Documentation requirements listed in ISO/IEC 27001; 3. Assessment of information security related risks and that the assessments produce consistent, valid and comparable results if repeated; 4. Determination of control objectives and controls based on the information security risk assessment and risk treatment processes; 5. Information security performance and the effectiveness of the ISMS, evaluating against the information security objectives; 6. Correspondence between the determined controls, the Statement of Applicability and the results of the information security risk assessment and risk treatment process and the information security policy and objectives 7. Implementation of taking into account the external and internal context and related risks, the organization's monitoring, measurement and analysis of information security processes and controls, to determine whether controls are implemented and effective and meet their stated information security objectives; 8. Programs, processes, procedures, records, internal audits and reviews of the ISMS effectiveness to ensure that these are traceable to top management decisions and the information security policy and objectives.

© 2025 Insight Assurance LLC - All Rights Reserved
This document may contain proprietary information and may only be released to third parties with approval of management.

Opening & Closing Meetings

List of participants in opening meeting and closing meeting.

Opening Meeting

Date: May 11, 2026
Time: 8:00AM CEST

#	Attendee name	Role/Title	Organization
1	Alvaro Tejada	Lead Auditor	Insight Assurance, LLC.
2	Roger Gonzalez Hermosa	Software Engineer	Sustainability Solutions SL
3	Christopher Buffkin	GRC Consultant	Agency Cyber, Inc.

Closing Meeting

Date: May 15, 2026
Time: 5:00PM CEST

#	Attendee name	Role/Title	Organization
1	Alvaro Tejada	Lead Auditor	Insight Assurance, LLC.
2	Roger Gonzalez Hermosa	Software Engineer	Sustainability Solutions SL
3	Christopher Buffkin	GRC Consultant	Agency Cyber, Inc.

© 2025 Insight Assurance LLC - All Rights Reserved
This document may contain proprietary information and may only be released to third parties with approval of management.

Management System Audit Time

Audit Dates and Duration	
Total audit time	7 days
Stage 1 MS audit time	2 days
Stage 1 dates	27-Apr-26 to 28-Apr-26
Stage 2 MS audit time	5 days
Stage 2 dates	11-May-26 to 15-May-26
Deviations from audit time	There were no deviations in the audit time.

© 2025 Insight Assurance LLC - All Rights Reserved
This document may contain proprietary information and may only be released to third parties with approval of management.

Audit Summary

Certification Scope Overview		
Certification scope statement	*The scope of Manglai's Information Security Management System includes the assets, technologies and processes for the secure provision of Manglai's AI-powered environmental management platform.*	
Number of personnel (FTE and contractor)	30	
Processes & activities in-scope	Sales, Tech, Climate, and Corporate.	
Third parties	Vendor Name Google Cloud Platform GitHub Google Workspace Slack Linear MongoDB	
Audit participants	Roger Gonzalez Hermosa, Software Engineer, Sustainability Solutions SL Christopher Buffkin, GRC Consultant, Agency Cyber, Inc. Alvaro Tejada, Lead Auditor, Insight Assurance, LLC.	
Other information, if applicable	Not applicable	
Detail of Sites		
Address	**MS**	**Site-specific activities**
Buenos Aires 38, sobreatico 4ta, 08036 Barcelona, Spain	ISMS	Sales, Tech, Climate, and Corporate.
Audit Information		
Audit methodology	The audit methods used were inquiry & interviews of client personnel and subject matter experts, observations of systems and sites, sampling & review of documentation and records. The auditor conducted a process-based audit focusing on significant aspects/risks and objectives required by ISO/IEC 27001:2022, ISO 17021-1:2015, ISO/IEC 27006-1:2024.	
Deviations from the audit plan	None	
Significant issues impacting the audit program	All audit procedures were performed remotely as no substantial risks associated to a remote audit had been identified upon application.	

© 2025 Insight Assurance LLC - All Rights Reserved
This document may contain proprietary information and may only be released to third parties with approval of management.

	No other significant issues impacting the audit program were identified.
Significant changes, if any, that affect the management system of the client since the last audit took place	None
Sampling information	• Audit conclusions are based on a sampling process of available information. • The audit included sampling of ISMS locations and evidence as to the implementation and effectiveness of controls. • The auditor selected some samples out of existing records such as management reviews and audit reports. • Results based on sampling are not perfect. • The audit was based on remote interviews and documentation review.
Use of information communication tools	To perform the audit, remote teleconferencing and screensharing were used to conduct interviews of personnel, observe documents, records, and other artifacts. The additional risks introduced by the use of ICT to conduct the audit were evaluated during the application review process and discussed with the client during the planning process. All audit activities normally performed while onsite were effectively performed by the auditor using these remote conferencing and collaboration tools, and all audit objectives were successfully achieved.
Statement of applicability	Version: 2 Date: 8-May-26 Some necessary controls had been omitted from the statement of applicability. Appropriate justifications for inclusions and, where applicable, exclusions of controls were documented.
Management Review	Version: 14-Apr-26 Date: 14-Apr-26 The Information Security Team was comprised of the following members: • CIO • System & network administrators • Senior engineer and it is scheduled to meet at least annually. During management reviews the organization considers the results of the internal & external audits, associated findings and corrective actions, risk assessment & treatments, monitoring and measuring of MS performance.

© 2025 Insight Assurance LLC - All Rights Reserved
This document may contain proprietary information and may only be released to third parties with approval of management.

	The organization documents the approvals, feedback & outcome of these reviews.
Internal Audit Report	Version: 2.0 Date: 5-Feb-26 The internal audit followed the organization's internal audit program and it identified fifty-eight (58) findings. The results of the most recent internal audit, including findings, root cause analyses, and remediations had been reviewed and approved by the organization's Management.
Risk assessment and treatment overview	Version: 1.0 Date: 7-May-26 The organization's latest risk assessment identified a total of (ten) 10 risks. Which two (2) were classified as critical risks, three (3) were classified as high risks, four (4) were classified as medium risks, and one (1) was classified as low risk. All risks were treated as mitigated.

© 2025 Insight Assurance LLC - All Rights Reserved
This document may contain proprietary information and may only be released to third parties with approval of management.

Audit Conclusions

Summary of Findings of Nonconformity	
Major nonconformities	Zero (0)
Minor nonconformities	Three (3)
Conclusions and Recommendation	
Audit conclusion and auditor recommendation	The auditor concludes that the organization's management system is conforming with the audit criteria and requirements and recommends the organization for certification.
Confirmation that the audit objectives have been fulfilled	Due to the remote nature of the Organization and the Certification Body, all audit activities were conducted fully remotely. All audit objectives were fulfilled.
Auditor's conclusion on the appropriateness of the certification scope	The auditor determined that the audit and certification scope were appropriate based on the information obtained during the stage 2 audit about the management system audited.
Conformity and the effectiveness of the management system	• The auditor determined that the ISMS has been implemented effectively and that it is capable of meeting applicable requirements and expected outcomes. • Management demonstrated commitment to the ISMS and that it can be trusted to ensure the effective operation and continual improvement of the MS. • The internal audit(s) and nonconformity handling process were effective in the identification and treatment of findings.

© 2025 Insight Assurance LLC - All Rights Reserved
This document may contain proprietary information and may only be released to third parties with approval of management.

Documents Reviewed and Audit Trail

The information request list and audit evidence are stored in the client's Drata GRC Tool instance. The evidence reviewed during the audit includes, but is not limited to the following artifacts:

ISO/IEC 27001 items	Artifact Description	Version	Date
Interested Parties and their Requirements	01-ISMS - Scope of the ISMS 02-ISMS - Information Security Management System ISMS Policy	1.0 1.1	9-Mar-26 28-Jan-26
Scope of the ISMS	01-ISMS - Scope of the ISMS 02-ISMS - Information Security Management System ISMS Policy	1.0 1.1	9-Mar-26 28-Jan-26
Information security policy	02-ISMS - Information Security Management System ISMS Policy AcceptableUsePolicy-v1 AssetManagementPolicy-v1 BackupPolicy-v1 BusinessContinuityPlan-v1 CodeofConduct-v1 DataProtectionPolicy-v1 DataRetentionPolicy-v1 DisasterRecoveryPlan-v1	1.1 1 1 1 1 1 1 1 1 1	28-Jan-26 10-Jan-26 10-Jan-26 10-Jan-26 10-Jan-26 10-Jan-26 10-Jan-26 10-Jan-26 10-Jan-26 10-Jan-26
Definition of security roles and responsibilities	02-ISMS - Information Security Management System ISMS Policy ManglaiOrgChart InformationSecurityPolicy-v1	1.1 27-Apr-26 1	28-Jan-26 27-Apr-26 10-Jan-26
Information security risk assessment process	RiskAssessmentPolicy-v1.1 MangleaiRiskAssessment(1)	1.1 1.0	6-May-26 7-May-26
Information security risk treatment process	RiskAssessmentPolicy-v1.1 MangleaiRiskAssessment(1)	1.1 1.0	6-May-26 7-May-26
Statement of Applicability	Mangleai 11-ISMS Statement of Applicability (SoA) - incl. 27701 & 27001_2022	2	8-May-26
Information security objectives	02-ISMS - Information Security Management System ISMS Policy InformationSecurityPolicy-v1 PhysicalSecurityPolicy-v1	1.1 1 1	28-Jan-26 10-Jan-26 10-Jan-26
Planning of Changes	02-ISMS - Information Security Management System ISMS Policy isms-management-review	1.1 14-Apr-26	28-Jan-26 14-Apr-26
Evidence of Competence	MangleaiSoftwareEngineerJobDescription Outboundrecruitingcandidates InformationSecurityPolicy-v1	11-Jan-26 15-Jan-26 1	11-Jan-26 15-Jan-26 10-Jan-26
Security awareness	IncidentResponsePlan-v1 AcceptableUsePolicy-v1 AssetManagementPolicy-v1 BackupPolicy-v1 BusinessContinuityPlan-v1 CodeofConduct-v1 DataProtectionPolicy-v1	1 1 1 1 1 1 1	10-Jan-26 10-Jan-26 10-Jan-26 10-Jan-26 10-Jan-26 10-Jan-26 10-Jan-26

© 2025 Insight Assurance LLC - All Rights Reserved
This document may contain proprietary information and may only be released to third parties with approval of management.

	DataRetentionPolicy-v1 DisasterRecoveryPlan-v1	1 1	10-Jan-26 10-Jan-26
Communications plan	06-ISMSInformationSecurityCommunicationPlan-v1.1 IncidentResponsePlan-v1 InformationSecurityPolicy-v1 Capturadepantalla2026-01-16alas16.37.37 (intrusion report from user)	1.1 1 1 16-Jan-26	28-Jan-26 10-Jan-26 10-Jan-26 16-Jan-26
Documented Information Determined by the Organization as being Necessary for the Effectiveness of the ISMS	05-ISMSProcedurefortheControlofDocumentedInformation-v1.1	1.1	28-Jan-26
Operations Planning and Control	02-ISMS - Information Security Management System ISMS Policy InformationSecurityPolicy-v1 PhysicalSecurityPolicy-v1 RiskAssessmentPolicy-v1.1 MangleaiRiskAssessment(1)	1.1 1 1 1.1 1.0	28-Jan-26 10-Jan-26 10-Jan-26 6-May-26 7-May26
Results of the Information Security Risk Assessments	RiskAssessmentPolicy-v1.1 MangleaiRiskAssessment(1)	1.1 1.0	6-May-26 7-May-26
Results of the Information Security Risk Treatment	RiskAssessmentPolicy-v1.1 MangleaiRiskAssessment(1)	1.1 1.0	6-May-26 7-May-26
Evidence of the Monitoring and Measurement Results	02-ISMS - Information Security Management System ISMS Policy AssetManagementPolicy-v1 InformationSecurityPolicy-v1 LoggingandMonitoringPolicy-v1 2_5_26ManglaiISO27001InternalAudit(2)	1.1 1 1 1 2.0	28-Jan-26 10-Jan-26 10-Jan-26 10-Jan-26 5-Feb-26
Internal audit	2_5_26ManglaiISO27001InternalAudit(2)	2.0	5-Feb-26
Internal audit program	2_5_26ManglaiISO27001InternalAudit(2)	2.0	5-Feb-26
Management review inputs	isms-management-review	14-Apr-26	14-Apr-26
Evidence of the Results of the Management Reviews	isms-management-review	14-Apr-26	14-Apr-26
Nonconformity and corrective action	02-ISMS - Information Security Management System ISMS Policy ManglaiISONCTracker(2)	1.1 10-May-26	28-Jan-26 10-May-26
Inventory of Information and Other Associated Asset	AssetManagementPolicy-v1	1	10-Jan-26
Acceptable Use of Information And Other Associated Assets	AcceptableUsePolicy-v1	1	10-Jan-26
Access control	githubaccessrequest SystemAccessControlPolicy-v1	21-Jan-26 1	21-Jan-26 10-Jan-26
Information security in supplier relationships	VendorManagementPolicy-v1.2	1.2	7-May-26
Information Security for use of Cloud Services (New control)	VendorManagementPolicy-v1.2	1.2	7-May-26
Response to information security events	ManglaiIncidentResponseProgramLog IncidentResponsePlan-v1	1.0 1	13-Jan-26 10-Jan-26

© 2025 Insight Assurance LLC - All Rights Reserved
This document may contain proprietary information and may only be released to third parties with approval of management.

Information and Communication Technology (ICT) Readiness for Business Continuity (New control)	BusinessContinuityPlan-v1 IncidentResponseTabletopExercise BusinessImpactAnalysis(BIA) DisasterRecoveryPlan-v1	1 8-May-26 2-Feb-26 1	10-Jan-26 8-May-26 2-Feb-26 10-Jan-26
Legal, Statutory, Regulatory, and Contractual Requirements	12-ISMSRelevantLaws,Regulations,andContractualRequirements-v1.2	1.2	7-May-26
Confidentiality / non-disclosure agreements	CodeofConduct-v1 Manglai-AnexodeconfidencialidadyprotecciÃ³ndelainformaciÃ³n VendorManagementPolicy-v1.2	1 11-Jan-26 1.2	10-Jan-26 11-Jan-26 7-May-26
Configuration Management (New control)	AssetManagementPolicy-v1 VulnerabilityManagementPolicy-v1 BaselineConfigurationDocumentationâ EngineeringSystems	1 1 2-Feb-26	10-Jan-26 10-Jan-26 2-Feb-26
Data Masking (New control)	Excluded per SoA	N/A	N/A
Monitoring Activities / Network Monitoring (New control)	AssetManagementPolicy-v1 MangleaiAuditLogs2026-01-20at4.24.45â¯PM MangleaiNetworkSecurityConfigurations2026-01-27at1.47.02â¯PM LoggingandMonitoringPolicy-v1 NetworkSecurityPolicy-v1	1 20-Jan-26 27-Jan-26 1 1	10-Jan-26 20-Jan-26 27-Jan-26 10-Jan-26 10-Jan-26
Secure systems architecture and engineering principles	ChangeManagementPolicy-v1 ChangeManagementPolicy(EngineeringSOP)(1) SoftwareDevelopmentLifeCyclePolicy-v1 stagingmockdata	1 7-Apr-26 1 21-Jan-26	10-Jan-26 7-Apr-26 10-Jan-26 21-Jan-26
Secure Coding (New control)	ChangeManagementPolicy-v1 ChangeManagementPolicy(EngineeringSOP)(1) SoftwareDevelopmentLifeCyclePolicy-v1 SecureSecretStorage2026-01-12at4.50.40aÌÂ¯PM(1)	1 7-Apr-26 1 12-Jan-26	10-Jan-26 7-Apr-26 10-Jan-26 12-Jan-26

© 2025 Insight Assurance LLC - All Rights Reserved
This document may contain proprietary information and may only be released to third parties with approval of management.

Conformance Testing Results

ISO/IEC 27001:2022 Mandatory Clauses

Number	Requirement	Conformance Testing Result
Clause 4	**Context of the organization**	
4.1	The organization shall determine external and internal issues that are relevant to its purpose and that affect its ability to achieve the intended outcome(s) of its information security management system	Conforming
4.2	Understanding the needs and expectations of interested parties	
4.2.a	The organization shall determine: a) interested parties that are relevant to the information security management system; and	Conforming
4.2.b	the relevant requirements of these interested parties;	Conforming
4.2.c	which of these requirements will be addressed through the information security management system.	Conforming
4.3	Determining the scope of the information security management system	
The organization shall determine the boundaries and applicability of the information security management system to establish its scope. When determining this scope, the organization shall consider:		
4.3.a	the external and internal issues referred to in 4.1	Conforming
4.3.b	the requirements referred to in 4.2; and	Conforming
4.3.c	interfaces and dependencies between activities performed by the organization, and those that are performed by other organizations.	Conforming
4.4	The organization shall establish, implement, maintain and continually improve an information security management system, including the processes needed and their interactions, in accordance with the requirements of this document.	Conforming
Clause 5	**Leadership**	
5.1	Leadership and commitment	
Top management shall demonstrate leadership and commitment with respect to the information security management system by:		
5.1.a	ensuring the information security policy and the information security objectives are established and are compatible with the strategic direction of the organization;	Conforming
5.1.b	ensuring the integration of the information security management system requirements into the organization's processes;	Conforming
5.1.c	ensuring that the resources needed for the information security management system are available;	Conforming
5.1.d	communicating the importance of effective information security management and of conforming to the information security management system requirements;	Conforming
5.1.e	ensuring that the information security management system achieves its intended outcome(s);	Conforming
5.1.f	directing and supporting persons to contribute to the effectiveness of the information security management system;	Conforming
5.1.g	promoting continual improvement; and	Conforming

© 2025 Insight Assurance LLC - All Rights Reserved
This document may contain proprietary information and may only be released to third parties with approval of management.

5.1.h	supporting other relevant management roles to demonstrate their leadership as it applies to their areas of responsibility.	Conforming
5.2	Policy	
5.2.a	is appropriate to the purpose of the organization;	Conforming
5.2.b	includes information security objectives (see 6.2) or provides the framework for setting information security objectives;	Conforming
5.2.c	includes a commitment to satisfy applicable requirements related to information security;	Conforming
5.2.d	includes a commitment to continual improvement of the information security management system.	Conforming
The information security policy shall:		
5.2.e	be available as documented information;	Conforming
5.2.f	be communicated within the organization; and	Conforming
5.2.g	be available to interested parties, as appropriate.	Conforming
5.3	Organizational roles, responsibilities, and authorities	
Top management shall ensure that the responsibilities and authorities for roles relevant to information security are assigned and communicated within the organization. Top management shall assign the responsibility and authority for:		
5.3.a	ensuring that the information security management system conforms to the requirements of this document;	Conforming
5.3.b	reporting on the performance of the information security management system to top management.	Conforming
Clause 6	**Planning**	
6.1	Actions to address risks and opportunities	
When planning for the information security management system, the organization shall consider the issues referred to in 4.1 and the requirements referred to in 4.2 and determine the risks and opportunities that need to be addressed to:		
6.1.1.a	ensure the information security management system can achieve its intended outcome(s);	Conforming
6.1.1.b	prevent, or reduce, undesired effects; and	Conforming
6.1.1.c	achieve continual improvement.	Conforming
The organization shall plan:		
6.1.1.d	actions to address these risks and opportunities; and	Conforming
6.1.1.e.1	how to: integrate and implement the actions into its information security management system processes; and	Conforming
6.1.1.e.2	evaluate the effectiveness of these actions.	Conforming
6.1.2	Information security risk assessment	
The organization shall define and apply an information security risk assessment process that:		
6.1.2.a	a) establishes and maintains information security risk criteria that include:	Conforming
6.1.2.a.1	1) the risk acceptance criteria; and	Conforming
6.1.2.a.2	criteria for performing information security risk assessments;	Conforming
6.1.2.b	ensures that repeated information security risk assessments produce consistent, valid and comparable results;	Conforming
6.1.2.c	identifies the information security risks:	Conforming
6.1.2.c.1	apply the information security risk assessment process to identify risks associated with the loss of confidentiality, integrity and availability for information within the scope of the information security management system; and	Conforming
6.1.2.c.2	identify the risk owners;	Conforming
6.1.2.d	analyses the information security risks:	Conforming

© 2025 Insight Assurance LLC - All Rights Reserved
This document may contain proprietary information and may only be released to third parties with approval of management.

6.1.2.d.1	assess the potential consequences that would result if the risks identified in 6.1.2 c) 1) were to materialize;	Conforming
6.1.2.d.2	assess the realistic likelihood of the occurrence of the risks identified in 6.1.2 c) 1); and	Conforming
6.1.2.d.3	determine the levels of risk;	Conforming
6.1.2.e	evaluates the information security risks:	Conforming
6.1.2.e.1	compare the results of risk analysis with the risk criteria established in 6.1.2 a); and	Conforming
6.1.2.e.2	prioritize the analysed risks for risk treatment.	Conforming
6.1.3	Information security risk treatment	
6.1.3.a	select appropriate information security risk treatment options, taking account of the risk assessment results;	Conforming
6.1.3.b	determine all controls that are necessary to implement the information security risk treatment option(s) chosen;	Conforming
6.1.3.c	compare the controls determined in 6.1.3 b) above with those in Annex A and verify that no necessary controls have been omitted;	Conforming
6.1.3.d	produce a Statement of Applicability that contains the necessary controls (see 6.1.3 b) and c)) and justification for their inclusion, whether the necessary controls are implemented or not, the justification for excluding any of the Annex A controls	Conforming
6.1.3.e	formulate an information security risk treatment plan; and	Conforming
6.1.3.f	obtain risk owners' approval of the information security risk treatment plan and acceptance of the residual information security risks.	Conforming
6.2	Information security objectives and planning to achieve them	
The organization shall establish information security objectives at relevant functions and levels. The information security objectives shall:		
6.2.a	be consistent with the information security policy;	Conforming
6.2.b	be measurable (if practicable);	Conforming
6.2.c	take into account applicable information security requirements, and results from risk assessment and risk treatment;	Conforming
6.2.d	be monitored;	Conforming
6.2.e	be communicated;	Conforming
6.2.f	be updated as appropriate	Conforming
6.2.g	be available as documented information	Conforming
When planning how to achieve its information security objectives, the organization shall determine:		
6.2.h	what will be done;	Conforming
6.2.i	what resources will be required;	Conforming
6.2.j	who will be responsible;	Conforming
6.2.k	when it will be completed; and	Conforming
6.2.l	how the results will be evaluated.	Conforming
6.3	Planning of changes	
6.3	When the organization determines the need for changes to the information security management system, the changes shall be carried out in a planned manner.	Conforming
Clause 7	**Support**	
7.1	The organization shall determine and provide the resources needed for the establishment, implementation, maintenance and continual improvement of the information security management system.	Conforming

© 2025 Insight Assurance LLC - All Rights Reserved
This document may contain proprietary information and may only be released to third parties with approval of management.

7.2	Competence	
The organization shall:		
7.2.a	determine the necessary competence of person(s) doing work under its control that affects its information security performance;	Conforming
7.2.b	ensure that these persons are competent on the basis of appropriate education, training, or experience;	Conforming
7.2.c	where applicable, take actions to acquire the necessary competence, and evaluate the effectiveness of the actions taken; and	Conforming
7.2.d	retain appropriate documented information as evidence of competence.	Conforming
7.3	Awareness	
Persons doing work under the organization's control shall be aware of:		
7.3.a	the information security policy;	Conforming
7.3.b	their contribution to the effectiveness of the information security management system, including the benefits of improved information security performance; and	Conforming
7.3.c	the implications of not conforming with the information security management system requirements.	Conforming
7.4	Communication	
The organization shall determine the need for internal and external communications relevant to the information security management system including:		
7.4.a	on what to communicate;	Conforming
7.4.b	when to communicate;	Conforming
7.4.c	with whom to communicate;	Conforming
7.4.d	how to communicate; and	Conforming
7.5	**Documented information**	
7.5.1	General	
The organization's information security management system shall include:		
7.5.1.a	documented information required by this document; and	Conforming
7.5.1.b	documented information determined by the organization as being necessary for the effectiveness of the information security management system.	Conforming
7.5.2	Creating and updating	
When creating and updating documented information the organization shall ensure appropriate:		
7.5.2.a	identification and description (e.g. a title, date, author, or reference number);	Conforming
7.5.2.b	format (e.g. language, software version, graphics) and media (e.g. paper, electronic); and	Minor Nonconformity
7.5.2.c	review and approval for suitability and adequacy.	Conforming
7.5.3	Control of documented information	
Documented information required by the information security management system and by this International Standard shall be controlled to ensure:		
7.5.3.a	it is available and suitable for use, where and when it is needed; and	Conforming
7.5.3.b	it is adequately protected (e.g. from loss of confidentiality, improper use, or loss of integrity).	Conforming
For the control of documented information, the organization shall address the following activities, as applicable:		
7.5.3.c	distribution, access, retrieval and use;	Conforming
7.5.3.d	storage and preservation, including the preservation of legibility;	Conforming
7.5.3.e	control of changes (e.g. version control); and	Minor Nonconformity
7.5.3.f	retention and disposition.	Conforming

© 2025 Insight Assurance LLC - All Rights Reserved
This document may contain proprietary information and may only be released to third parties with approval of management.

Clause 8	Operation	
8.1	Operational planning and control	
8.1.a	The organization shall plan, implement and control the processes needed to meet requirements, and to implement the actions determined in Clause 6, by: establishing criteria for the processes; implementing control of the processes in accordance with the criteria.	Conforming
8.1.b	Documented information shall be available to the extent necessary to have confidence that the processes have been carried out as planned.	Conforming
8.1.c	The organization shall control planned changes and review the consequences of unintended changes, taking action to mitigate any adverse effects, as necessary.	Conforming
8.1.d	The organization shall ensure that externally provided processes, products or services that are relevant to the information security management system are controlled.	Conforming
8.2	Information security risk assessment	
8.2.a	The organization shall perform information security risk assessments at planned intervals or when significant changes are proposed or occur, taking account of the criteria established in 6.1.2 a).	Conforming
8.2.b	The organization shall retain documented information of the results of the information security risk assessments.	Conforming
8.3	Information security risk treatment	
8.3.a	The organization shall implement the information security risk treatment plan.	Conforming
8.3.b	The organization shall retain documented information of the results of the information security risk treatment.	Conforming
Clause 9	**Performance evaluation**	
9.1	Monitoring, measurement, analysis and evaluation	
The organization shall determine:		
9.1.a	what needs to be monitored and measured, including information security processes and controls	Conforming
9.1.b	the methods for monitoring, measurement, analysis and evaluation, as applicable, to ensure valid results; The methods selected should produce comparable and reproducible results to be considered valid;	Conforming
9.1.c	when the monitoring and measuring shall be performed;	Conforming
9.1.d	who shall monitor and measure;	Conforming
9.1.e	when the results from monitoring and measurement shall be analysed and evaluated; and	Conforming
9.1.f	who shall analyse and evaluate these results.	Conforming
9.2	Internal audit	
The organization shall conduct internal audits at planned intervals to provide information on whether the information security management system:		
9.2.a.1	conforms to the organization's own requirements for its information security management system; and	Conforming
9.2.a.2	the requirements of this document	Conforming
9.2.b	is effectively implemented and maintained.	Conforming
9.2.2	The organization shall plan, establish, implement and maintain an audit program(s), including the frequency, methods, responsibilities, planning requirements and reporting. When establishing the internal audit program(s), the organization shall consider the importance of the processes concerned and the results of previous audits. The organization shall:	
9.2.2.a	define the audit criteria and scope for each audit;	Conforming

© 2025 Insight Assurance LLC - All Rights Reserved
This document may contain proprietary information and may only be released to third parties with approval of management.

9.2.2.b	select auditors and conduct audits that ensure objectivity and the impartiality of the audit process;	Conforming
9.2.2.c	ensure that the results of the audits are reported to relevant management; and	Conforming
9.3	Management review	
9.3.1.a	Top management shall review the organization's information security management system at planned intervals to ensure its continuing suitability, adequacy and effectiveness.	Conforming
9.3.2	Management review inputs	
9.3.2.a	the status of actions from previous management reviews;	Conforming
9.3.2.b	changes in external and internal issues that are relevant to the information security management system;	Conforming
9.3.2.c	changes in needs and expectations of interested parties that are relevant to the information security management system;	Conforming
9.3.2.d	feedback on the information security performance, including trends in:	Conforming
9.3.2.d.1	nonconformities and corrective actions;	Conforming
9.3.2.d.2	monitoring and measurement results;	Conforming
9.3.2.d.3	audit results;	Conforming
9.3.2.d.4	fulfilment of information security objectives;	Conforming
9.3.2.e	feedback from interested parties;	Conforming
9.3.2.f	results of risk assessment and status of risk treatment plan;	Conforming
9.3.2.g	opportunities for continual improvement	Conforming
9.3.3	The results of the management review shall include decisions related to continual improvement opportunities and any needs for changes to the information security management system.	Conforming
Clause 10	**Improvement**	
10.1	Continual Improvement	
10.1.1	The organization shall continually improve the suitability, adequacy and effectiveness of the information security management system.	Conforming
10.2	Nonconformity and corrective action	
When a nonconformity occurs, the organization shall:		
10.2.a	react to the nonconformity, and as applicable:	Minor Nonconformity
10.2.a.1	take action to control and correct it; and	Minor Nonconformity
10.2.a.2	deal with the consequences;	Minor Nonconformity
10.2.b	evaluate the need for action to eliminate the causes of nonconformity, in order that it does not recur or occur elsewhere, by:	Minor Nonconformity
10.2.b.1	reviewing the nonconformity;	Minor Nonconformity
10.2.b.2	determining the causes of the nonconformity; and	Minor Nonconformity
10.2.b.3	determining if similar nonconformities exist, or could potentially occur;	Minor Nonconformity
10.2.c	implement any action needed;	Minor Nonconformity
10.2.d	review the effectiveness of any corrective action taken; and	Minor Nonconformity
10.2.e	make changes to the information security management system, if necessary.	Minor Nonconformity
Documented information shall be available as evidence of:		
10.2.f	the nature of the nonconformities and any subsequent actions taken, and	Minor Nonconformity

© 2025 Insight Assurance LLC - All Rights Reserved
This document may contain proprietary information and may only be released to third parties with approval of management.

10.2.g	the results of any corrective action.	Minor Nonconformity

© 2025 Insight Assurance LLC - All Rights Reserved
This document may contain proprietary information and may only be released to third parties with approval of management.

ISO/IEC 27001:2022 Annex A Controls

5	Organizational Controls		
5.1	Policies for information security	Information security policy and topic-specific policies shall be defined, approved by management, published, communicated to and acknowledged by relevant personnel and relevant interested parties, and reviewed at planned intervals and if significant changes occur.	Conforming
5.2	Information security roles and responsibilities	Information security roles and responsibilities shall be defined and allocated according to the organization needs.	Conforming
5.3	Segregation of duties	Conflicting duties and conflicting areas of responsibility shall be segregated.	Conforming
5.4	Management responsibilities	Management shall require all personnel to apply information security in accordance with the established information security policy, topic-specific policies and procedures of the organization.	Conforming
5.5	Contact with authorities	The organization shall establish and maintain contact with relevant authorities.	Conforming
5.6	Contact with special interest groups	The organization shall establish and maintain contact with special interest groups or other specialist security forums and professional associations.	Conforming
5.7	Threat intelligence	Information relating to information security threats shall be collected and analysed to produce threat intelligence.	Conforming
5.8	Information security in project management	Information security shall be integrated into project management.	Conforming
5.9	Inventory of information and other associated assets	An inventory of information and other associated assets, including owners, shall be developed and maintained.	Conforming
5.10	Acceptable use of information and other associated assets	Rules for the acceptable use and procedures for handling information and other associated assets shall be identified, documented and implemented.	Conforming
5.11	Return of assets	Personnel and other interested parties as appropriate shall return all the organization's assets in their possession upon change or termination of their employment, contract or agreement.	Conforming
5.12	Classification of information	Information shall be classified according to the information security needs of the organization based on confidentiality, integrity, availability and relevant interested party requirements.	Conforming
5.13	Labelling of information	An appropriate set of procedures for information labelling shall be developed and implemented in accordance with the information classification scheme adopted by the organization.	Conforming
5.14	Information transfer	Information transfer rules, procedures, or agreements shall be in place for all types of transfer facilities within the organization and between the organization and other parties.	Conforming
5.15	Access Control	Rules to control physical and logical access to information and other associated assets shall be established and	Conforming

© 2025 Insight Assurance LLC - All Rights Reserved
This document may contain proprietary information and may only be released to third parties with approval of management.

		implemented based on business and information security requirements.	
5.16	Identity management	The full life cycle of identities shall be managed.	Conforming
5.17	Authentication information	Allocation and management of authentication information shall be controlled by a management process, including advising personnel on appropriate handling of authentication information.	Conforming
5.18	Access rights	Access rights to information and other associated assets shall be provisioned, reviewed, modified and removed in accordance with the organization's topic-specific policy on and rules for access control.	Conforming
5.19	Information security in supplier relationships	Processes and procedures shall be defined and implemented to manage the information security risks associated with the use of supplier's products or services.	Conforming
5.20	Addressing information security within supplier agreements	Relevant information security requirements shall be established and agreed with each supplier based on the type of supplier relationship.	Conforming
5.21	Managing information security in the information and communication technology (ICT) supply chain	Processes and procedures shall be defined and implemented to manage the information security risks associated with the ICT products and services supply chain.	Conforming
5.22	Monitoring, review and change management of supplier services	The organization shall regularly monitor, review, evaluate and manage change in supplier information security practices and service delivery.	Conforming
5.23	Information security for use of cloud services	Processes for acquisition, use, management and exit from cloud services shall be established in accordance with the organization's information security requirements.	Conforming
5.24	Information security incident management planning and preparation	The organization shall plan and prepare for managing information security incidents by defining, establishing and communicating information security incident management processes, roles and responsibilities.	Conforming
5.25	Assessment and decision on information security events	The organization shall assess information security events and decide if they are to be categorized as information security incidents.	Conforming
5.26	Response to information security incidents	Information security incidents shall be responded to in accordance with the documented procedures.	Conforming
5.27	Learning from information security incidents	Knowledge gained from information security incidents shall be used to strengthen and improve the information security controls.	Conforming
5.28	Collection of evidence	The organization shall establish and implement procedures for the identification, collection, acquisition and preservation of evidence related to information security events.	Conforming

© 2025 Insight Assurance LLC - All Rights Reserved
This document may contain proprietary information and may only be released to third parties with approval of management.

5.29	Information security during disruption	The organization shall plan how to maintain information security at an appropriate level during disruption.	Conforming
5.30	ICT readiness for business continuity	ICT readiness shall be planned, implemented, maintained and tested based on business continuity objectives and ICT continuity requirements.	Conforming
5.31	Legal, statutory, regulatory and contractual requirements	Legal, statutory, regulatory and contractual requirements relevant to information security and the organization's approach to meet these requirements shall be identified, documented and kept up to date.	Conforming
5.32	Intellectual property rights	The organization shall implement appropriate procedures to protect intellectual property rights.	Conforming
5.33	Protection of records	Records shall be protected from loss, destruction, falsification, unauthorized access and unauthorized release.	Conforming
5.34	Privacy and protection of personal identifiable information (PII)	The organization shall identify and meet the requirements regarding the preservation of privacy and protection of PII according to applicable laws and regulations and contractual requirements.	Conforming
5.35	Independent review of information security	The organization's approach to managing information security and its implementation including people, processes and technologies shall be reviewed independently at planned intervals, or when significant changes occur.	Conforming
5.36	Compliance with policies, rules and standards for information security	Compliance with the organization's information security policy, topic-specific policies, rules and standards shall be regularly reviewed.	Conforming
5.37	Documented operating procedures	Operating procedures for information processing facilities shall be documented and made available to personnel who need them.	Conforming
6	**People controls**		
6.1	Screening	Background verification checks on all candidates to become personnel shall be carried out prior to joining the organization and on an ongoing basis taking into consideration applicable laws, regulations and ethics and be proportional to the business requirements, the classification of the information to be accessed and the perceived risks.	Conforming
6.2	Terms and conditions of employment	The employment contractual agreements shall state the personnel's and the organization's responsibilities for information security.	Conforming
6.3	Information security awareness, education and training	Personnel of the organization and relevant interested parties shall receive appropriate information security awareness, education and training and regular updates of the organization's information security policy, topic-specific policies and procedures, as relevant for their job function.	Conforming
6.4	Disciplinary process	A disciplinary process shall be formalized and communicated to take actions against personnel and other relevant interested parties who have committed an information security policy violation.	Conforming
6.5	Responsibilities after termination	Information security responsibilities and duties that remain valid after termination or change of employment shall be	Conforming

© 2025 Insight Assurance LLC - All Rights Reserved
This document may contain proprietary information and may only be released to third parties with approval of management.

	or change of employment	defined, enforced and communicated to relevant personnel and other interested parties.	
6.6	Confidentiality or non-disclosure agreements	Confidentiality or non-disclosure agreements reflecting the organization's needs for the protection of information shall be identified, documented, regularly reviewed and signed by personnel and other relevant interested parties.	Conforming
6.7	Remote working	Security measures shall be implemented when personnel are working remotely to protect information accessed, processed or stored outside the organization's premises.	Conforming
6.8	Information security event reporting	The organization shall provide a mechanism for personnel to report observed or suspected information security events through appropriate channels in a timely manner.	Conforming
7	**Physical controls**		
7.1	Physical security perimeters	Security perimeters shall be defined and used to protect areas that contain information and other associated assets.	Excluded per SoA
7.2	Physical entry	Secure areas shall be protected by appropriate entry controls and access points.	Excluded per SoA
7.3	Securing offices, rooms, and facilities	Physical security for offices, rooms and facilities shall be designed and implemented.	Excluded per SoA
7.4	Physical security monitoring	Premises shall be continuously monitored for unauthorized physical access.	Excluded per SoA
7.5	Protecting against physical and environmental threats	Protection against physical and environmental threats, such as natural disasters and other intentional or unintentional physical threats to infrastructure shall be designed and implemented.	Excluded per SoA
7.6	Working in secure areas	Security measures for working in secure areas shall be designed and implemented.	Excluded per SoA
7.7	Clear desk and clear screen	Clear desk rules for papers and removable storage media and clear screen rules for information processing facilities shall be defined and appropriately enforced.	Conforming
7.8	Equipment siting and protection	Equipment shall be sited securely and protected.	Excluded per SoA
7.9	Security of assets off-premises	Off-site assets shall be protected.	Conforming
7.10	Storage media	Storage media shall be managed through their life cycle of acquisition, use, transportation and disposal in accordance with the organization's classification scheme and handling requirements.	Minor Nonconformity
7.11	Supporting utilities	Information processing facilities shall be protected from power failures and other disruptions caused by failures in supporting utilities.	Excluded per SoA
7.12	Cabling security	Cables carrying power, data or supporting information services shall be protected from interception, interference or damage.	Excluded per SoA
7.13	Equipment maintenance	Equipment shall be maintained correctly to ensure availability, integrity and confidentiality of information.	Conforming
7.14	Secure disposal or re-use of equipment	Items of equipment containing storage media shall be verified to ensure that any sensitive data and licensed software has been removed or securely overwritten prior to disposal or re-use.	Conforming
8	**Technological controls**		

© 2025 Insight Assurance LLC - All Rights Reserved
This document may contain proprietary information and may only be released to third parties with approval of management.

8.1	User endpoint devices	Information stored on, processed by or accessible via user end point devices shall be protected.	Minor Nonconformity
8.2	Privileged access rights	The allocation and use of privileged access rights shall be restricted and managed.	Conforming
8.3	Information access restriction	Access to information and other associated assets shall be restricted in accordance with the established topic-specific policy on access control.	Conforming
8.4	Access to source code	Read and write access to source code, development tools and software libraries shall be appropriately managed.	Conforming
8.5	Secure authentication	Secure authentication technologies and procedures shall be implemented based on information access restrictions and the topic-specific policy on access control.	Conforming
8.6	Capacity management	The use of resources shall be monitored and adjusted in line with current and expected capacity requirements.	Conforming
8.7	Protection against malware	Protection against malware shall be implemented and supported by appropriate user awareness.	Conforming
8.8	Management of technical vulnerabilities	Information about technical vulnerabilities of information systems in use shall be obtained, the organization's exposure to such vulnerabilities shall be evaluated and appropriate measures shall be taken.	Conforming
8.9	Configuration management	Configurations, including security configurations, of hardware, software, services and networks shall be established, documented, implemented, monitored and reviewed.	Conforming
8.10	Information deletion	Information stored in information systems, devices or in any other storage media shall be deleted when no longer required.	Conforming
8.11	Data masking	Data masking shall be used in accordance with the organization's topic-specific policy on access control and other related topic-specific policies, and business requirements, taking applicable legislation into consideration.	Conforming
8.12	Data leakage prevention	Data leakage prevention measures shall be applied to systems, networks and any other devices that process, store or transmit sensitive information.	Conforming
8.13	Information backup	Backup copies of information, software and systems shall be maintained and regularly tested in accordance with the agreed topic-specific policy on backup.	Conforming
8.14	Redundancy of information processing facilities	Information processing facilities shall be implemented with redundancy sufficient to meet availability requirements.	Conforming
8.15	Logging	Logs that record activities, exceptions, faults and other relevant events shall be produced, stored, protected and analysed.	Conforming
8.16	Monitoring	Networks, systems and applications shall be monitored for anomalous behaviour and appropriate actions taken to evaluate potential information security incidents.	Conforming
8.17	Clock synchronization	The clocks of information processing systems used by the organization shall be synchronized to approved time sources.	Conforming
8.18	Use of privilege utility programs	The use of utility programs that can be capable of overriding system and application controls shall be restricted and tightly controlled.	Conforming
8.19	Installation of software on	Procedures and measures shall be implemented to securely manage software installation on operational systems.	Conforming

© 2025 Insight Assurance LLC - All Rights Reserved
This document may contain proprietary information and may only be released to third parties with approval of management.

	operational systems		
8.20	Networks security	Networks and network devices shall be secured, managed and controlled to protect information in systems and applications.	Conforming
8.21	Security of network services	Security mechanisms, service levels and service requirements of network services shall be identified, implemented and monitored.	Conforming
8.22	Segregation of networks	Groups of information services, users and information systems shall be segregated in the organization's networks.	Conforming
8.23	Web filtering	Access to external websites shall be managed to reduce exposure to malicious content.	Conforming
8.24	Use of cryptography	Rules for the effective use of cryptography, including cryptographic key management, shall be defined and implemented.	Conforming
8.25	Secure development lifecycle	Rules for the secure development of software and systems shall be established and applied.	Conforming
8.26	Application security requirements	Information security requirements shall be identified, specified and approved when developing or acquiring applications.	Conforming
8.27	Secure system architecture and engineering principles	Principles for engineering secure systems shall be established, documented, maintained and applied to any information system development activities.	Conforming
8.28	Secure coding	Secure coding principles shall be applied to software development.	Conforming
8.29	Security testing in development and acceptance	Security testing processes shall be defined and implemented in the development life cycle.	Conforming
8.30	Outsourced development	The organization shall direct, monitor and review the activities related to outsourced system development.	Conforming
8.31	Separation of development, test and production environments	Development, testing and production environments shall be separated and secured.	Conforming
8.32	Change management	Changes to information processing facilities and information systems shall be subject to change management procedures.	Conforming
8.33	Test information	Test information shall be appropriately selected, protected and managed.	Conforming
8.34	Audit testing	Audit tests and other assurance activities involving assessment of operational systems shall be planned and agreed between the tester and appropriate management.	Conforming

© 2025 Insight Assurance LLC - All Rights Reserved
This document may contain proprietary information and may only be released to third parties with approval of management.

Findings

Definition of findings:

Conforming: A standard clause or annex control, a client's policy and/or procedure or certification body's requirement is fulfilled.

Non-conformity*:* A standard clause or annex control, a client's policy and/or procedure or certification body's requirement is not fulfilled.

Major non-conformity: a non-conformity that affects the capability of the management system to achieve the intended results. Nonconformities could be classified as major in the following circumstances:

- If there is significant doubt that effective process control is in place or that products or services will meet specified requirements.
- A number of minor nonconformities associated with the same requirement or issue could demonstrate a systemic failure and thus constitute a major non-conformity.

Minor non-conformity: a non-conformity that does not affect the capability of the management system to achieve the intended results.

Remediating nonconformities:

1. **For major nonconformities –** An in-depth root cause analysis, documented plans for correction & corrective action, and evidence of full implementation for each are due to your auditor within 90 calendar days of the audit closing meeting, on a per site basis.
2. **For minor nonconformities –** An in-depth root cause analysis, documented plans for correction & corrective action, and evidence of full implementation for correction are due within 30 calendar days of the audit closing meeting, on a per site basis. Only the evidence of full implementation for corrective action may be deferred until the next review.
3. **Definitions:**
    a. **Root Cause Analysis**: Identification of the core cause, or group of causes resulting in nonconformities or potential nonconformities.
    b. **Correction:** Means the actions implemented to eliminate the nonconformity identified.
    c. **Evidence of Correction:** Evidence that correction has been fully and correctly implemented.
    d. **Corrective Action:** Means the actions implemented to address or eliminate the root cause, to ensure the nonconformities identified (or other nonconformities that could potentially result from the same root cause) do not occur again. Also known as corrective action plan or CAP.
    e. **Evidence of Corrective Action:** Evidence that corrective action has been fully and correctly implemented.
4. **Failure to provide complete and acceptable remediations –** Failure to provide acceptable remediations as described above within the specified timeframe may result in the need for an audit reperformance and/or suspension/withdrawal of certification as determined by the ISO Certification and Accreditation Board.

© 2025 Insight Assurance LLC - All Rights Reserved
This document may contain proprietary information and may only be released to third parties with approval of management.

Details of Findings

2026	Initial Certification	Finding #1
Insight	**Finding**	Minor Nonconformity
	Location	Buenos Aires 38, sobreatico 4ta, 08036 Barcelona, Spain
	Audit Stage	Stage 2
	Requirement	Clauses 7.5.2.b & 7.5.3.e
	Domain	Support
	Audit Criteria	ISO/IEC 27001:2022
	Statement of Nonconformity	While reviewing the organization's procedure for control of documents policy 05 ISMSProcedurefortheControlofDocumentedInformation-v1.1.pdf (v1.1, dated 28-Jan-26) and reading the "Updates and Version Control" section, it is stated that the version of documents shall be updated and documented in their 00-ISMS Master List of Documents. However, when reviewing their 00-ISMSMasterListofDocuments-v1.2.pdf (v1.2, dated 7-Apr-26) it was noted that many of their policy documents do not reflect their current version number.
	Objective Evidence	00-ISMSMasterListofDocuments-v1.2.pdf (v1.2, dated 7-Apr-26)
	Finding Status	Open - CAP Accepted
	Auditor	Alvaro Tejada
	Date	15-May-26
Sustainability Solutions SL	**Root Cause Analysis**	ISMS policies 11 and 12 had incorrect version numbers listed in))-ISMS Master List of Documents policy.
	Correction (Describe how the nonconformity was fixed)	The master list of documents was updated to accurately reflect version numbers of all policies listed.
	Evidence of Correction Implementation	Manglaai 00-ISMS Master List of Documents (corrected).pdf
	Corrective Action Plan (CAP) (Describe plan to prevent reocurrence)	Upon a policy change the Master List of Documents will be updated to reflect the updated version number.
	Evidence of CAP Implementation	
	Approved by	Andres Cester
	Date of full implementation	19-May-26
Insight (Next Year)	**Effectiveness Verification** (Next Year)	
	Auditor	
	Date	
	Finding Status	
2026	**Initial Certification**	**Finding #2**
Insight	**Finding**	Minor Nonconformity
	Location	Buenos Aires 38, sobreatico 4ta, 08036 Barcelona, Spain
	Audit Stage	Stage 2

© 2025 Insight Assurance LLC - All Rights Reserved
This document may contain proprietary information and may only be released to third parties with approval of management.

	Requirement	Clause 10.2
	Domain	Improvement
	Audit Criteria	ISO/IEC 27001:2022
	Statement of Nonconformity	While reviewing the organization's non-conformities tracker document ManglaiISONCTracker(2).xlsx (v10-May26, dated 10-May-26) there was inconsistency noticed with the findings tracked in this document versus the ones identified during their internal audit program as documented in 2_5_26ManglaiISO27001InternalAudit(2).xlsx (v2.0, dated 5-Feb-26). The audit program identified 58 non-conformities while in the non-conformities tracker document only 54 were tracked and remediated.
	Objective Evidence	ManglaiISONCTracker(2).xlsx (v10-May26, dated 10-May-26) 2_5_26ManglaiISO27001InternalAudit(2).xlsx (v2.0, dated 5-Feb-26)
	Finding Status	Open - CAP Accepted
	Auditor	Alvaro Tejada
	Date	15-May-26
Sustainability Solutions SL	**Root Cause Analysis**	There were 4 controls that appeared in the internal audit but not in the non-conformity tracker. The controls were A.7.5, A.7.10, C.9.2.1, and C.9.2.2.
	Correction (Describe how the nonconformity was fixed)	A.7.5 was marked as not applicable. This control was tested which it should not have been. This control was not added to the tracker as a result. A.7.10, C.9.2.1, and C.9.2.2 and associated non-conformities was added to the non-conformity tracker.
	Evidence of Correction Implementation	Manglai ISO NC Tracker (revised).xlsx
	Corrective Action Plan (CAP) (Describe plan to prevent reocurrence)	For future internal audits, Non-conforming controls will be matched with those listed in non-conformity tracker to validate. Any inconsistencies will be evaluated.
	Evidence of CAP Implementation	
	Approved by	Andres Cester
	Date of full implementation	19-May-26
Insight (Next Year)	**Effectiveness Verification** (Next Year)	
	Auditor	
	Date	
	Finding Status	
2026	**Initial Certification**	**Finding #3**
Insight	**Finding**	Minor Nonconformity
	Location	Buenos Aires 38, sobreatico 4ta, 08036 Barcelona, Spain
	Audit Stage	Stage 2
	Requirement	Annex A.7.10 & A.8.1
	Domain	Physical and Technological Controls

© 2025 Insight Assurance LLC - All Rights Reserved
This document may contain proprietary information and may only be released to third parties with approval of management.

	Audit Criteria	ISO/IEC 27001:2022
	Statement of Nonconformity	No evidence was provided pertaining to the protection of use of removable storage devices. As per the organization's DataProtectionPolicy-v1.pdf (v1, dated 10-Jan-26) document it states under the "Movement of Media" section that removable media devices will be encrypted to protect the confidentiality of the information during movement. No evidence could be provided of a security control in place that would encrypt a connected removable storage device to a computer to protect any content stored to it.
	Objective Evidence	DataProtectionPolicy-v1.pdf (v1, dated 10-Jan-26)
	Finding Status	Open - CAP Accepted
	Auditor	Alvaro Tejada
	Date	15-May-26
Sustainability Solutions SL	**Root Cause Analysis**	No controls were implemented to enforce removable media encryption.
	Correction (Describe how the nonconformity was fixed)	Manglai has opted to create a policy within Falcon Go that blocks removable media usage. Any use of removable media must go through an approval process and an exception must be made to bypass the policy enforced in Falcon Go.
	Evidence of Correction Implementation	Captura de pantalla 2026-05-19 a las 13.36.47.png and Captura de pantalla 2026-05-19 a las 13.36.04.png
	Corrective Action Plan (CAP) (Describe plan to prevent reocurrence)	Falcon Go policy will prevent reoccurrence.
	Evidence of CAP Implementation	
	Approved by	Andres Cester
	Date of full implementation	19-May-26
Insight (Next Year)	**Effectiveness Verification** (Next Year)	
	Auditor	
	Date	
	Finding Status	

© 2025 Insight Assurance LLC - All Rights Reserved
This document may contain proprietary information and may only be released to third parties with approval of management.