INSIGHT ASSURANCE

Integrated Management System:

ISO/IEC 27001:2022
ISO/IEC 42001:2023
CSA STAR Level 2

Fulcrum Global Technologies, Inc.;
Fulcrum Global Technologies UK Ltd.;
Fulcrum Global Technologies Private, Ltd.;
Focus Core Inc.

Surveillance Audit Report
October 9, 2026

Table of Contents

Contact Information and Audit Criteria 3
Opening & Closing Meetings 6
Management System Audit Time 8
Audit Summary 9
Audit Conclusions 14
Documents Reviewed and Audit Trail 15
Conformance Testing Results 24
Surveillance Requirements 24
ISO/IEC 27001:2022 Mandatory Clauses 25
ISO/IEC 27001:2022 Annex A Controls 31
ISO/IEC 42001:2023 Clauses 37
ISO/IEC 42001:2023 Annex A Controls 44
CSA STAR CCM v4.1 48
Findings 69
Details of Findings 70

© 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	Fulcrum Global Technologies, Inc.; Fulcrum Global Technologies UK Ltd.; Fulcrum Global Technologies Private, Ltd.; Focus Core Inc.
Company Address	1901 N Roselle Road, Schaumburg, Chicago, IL 60195
Company Description	Fulcrum Global Technologies, Inc. provides cloud solutions to the global legal and professional services markets. The Fulcrum Snap™ system comprises a set of modules designed to support the business operations of legal and professional services firms.
Company Contact Name	Ahmed Shaaban, Managing Director
Location(s) in Scope of the Certification	• 1901 N Roselle Road, Schaumburg, Chicago, IL 60195 • 1 St. Katharine's Way, London E1W 1UN, United Kingdom • My Home Twitza, 14th Floor APIIC Hyderabad Knowledge City Raidurg, Hyderabad 50081, Telagana, India • D. No. 4-57-6, Plot No. 103, Lawsons Bay Colony, North East Layout, Visakhapatnam, 530017, Andhra Pradesh, India
Certification Company	
Company Name	Insight Assurance, LLC
Company Address	400 N Tampa St, Suite 129, Tampa, FL 33602
Company Contact Name	Mario Vlieg, Manager
Audit Team	
Lead Auditor Name	Gerardo Valderrama
Audit Team Members	N/A
Others	N/A
Audit Criteria and Objectives	
Audit standard(s) to be certified	ISO/IEC 27001:2022 ISO/IEC 42001:2023
Additional audit criteria	ISO/IEC 17021-1:2015 ISO/IEC 27006-1:2024 ISO/IEC 42006:2025 CSA STAR Level 2 Insight Assurance Certification Terms and Conditions
Type of audit	ISO/IEC 27001:2022 2nd Surveillance

© 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 42001:2023 1st Surveillance
Audit objectives	**Surveillance Objectives:** 1. To verify that representative areas and functions covered by the scope of the management system continue to operate effectively; 2. To review internal audits and management review; 3. To review actions taken on nonconformities identified during the previous audit; 4. To review complaints handling; 5. To review the effectiveness of the management system with regard to achieving the certified client's objectives and the intended results of the respective management system(s); 6. To review the progress of planned activities aimed at continual improvement; 7. To review continuing operational control; 8. Review of any changes; 9. To review the use of marks and/or any other reference to certification
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

© 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 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. **ISO/IEC 42001:2023 Areas of Focus:** 1. Top management leadership and commitment to the AI policy and objectives for the AI system; 2. Functional testing for the documentation requirements, controls, committees, risk assessment processes, reporting processes and handling of complaints listed in ISO/IEC 42001; 3. Assessment of the risks associated with the AI system and the degree to which repeated assessments, produce consistent, valid, and comparable results. 4. Determination of the objectives of action and measures based on the AI risk assessment and risk treatment process; 5. Effectiveness of the AIMS against the set AI objectives and scopes; 6. Programs, processes, procedures, records, internal audits, and evaluation of AIMS effectiveness to ensure they are consistent with senior management decisions and AI policies and objectives; 7. The AIMS requirements for functional testing through representative sampling for controls that affect the quality of the product, service, or process related to the quantity of AI products placed on the market or related to the amount of users of an AI system.

© 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: August 31, 2026
Time: 8:00 AM CDT

#	Attendee name	Role/Title	Organization
1	Gerardo Valderrama	Lead Auditor	Insight Assurance, LLC.
2	John Kinnane	Exec VP of Security - Network, Information, and Compliance	Fulcrum Global Technologies, Inc.; Fulcrum Global Technologies UK Ltd.; Fulcrum Global Technologies Private, Ltd.; Focus Core Inc.
3	Martin Telfer	CIO / CISO	Fulcrum Global Technologies, Inc.; Fulcrum Global Technologies UK Ltd.; Fulcrum Global Technologies Private, Ltd.; Focus Core Inc.
4	Vincent Puzar	Assistant Director, Security Operations	Fulcrum Global Technologies, Inc.; Fulcrum Global Technologies UK Ltd.; Fulcrum Global Technologies Private, Ltd.; Focus Core Inc.
5	Kanika Capoor	GRC Analyst	Fulcrum Global Technologies, Inc.; Fulcrum Global Technologies UK Ltd.; Fulcrum Global Technologies Private, Ltd.; Focus Core Inc.
6	Suzan Mustafi	Vanta Administrator	Fulcrum Global Technologies, Inc.; Fulcrum Global Technologies UK Ltd.; Fulcrum Global Technologies Private, Ltd.; Focus Core Inc.
7	Ryan George	Senior Security Engineer	Fulcrum Global Technologies, Inc.; Fulcrum Global Technologies UK Ltd.; Fulcrum Global Technologies Private, Ltd.; Focus Core 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.

Closing Meeting

Date: September 25, 2026
Time: 5:00 PM CDT

#	Attendee name	Role/Title	Organization
1	Gerardo Valderrama	Lead Auditor	Insight Assurance, LLC.
2	John Kinnane	Exec VP of Security - Network, Information, and Compliance	Fulcrum Global Technologies, Inc.; Fulcrum Global Technologies UK Ltd.; Fulcrum Global Technologies Private, Ltd.; Focus Core Inc.
3	Martin Telfer	CIO / CISO	Fulcrum Global Technologies, Inc.; Fulcrum Global Technologies UK Ltd.; Fulcrum Global Technologies Private, Ltd.; Focus Core Inc.
4	Vincent Puzar	Associate Director, Security Operations	Fulcrum Global Technologies, Inc.; Fulcrum Global Technologies UK Ltd.; Fulcrum Global Technologies Private, Ltd.; Focus Core Inc.
5	Kanika Capoor	GRC Analyst	Fulcrum Global Technologies, Inc.; Fulcrum Global Technologies UK Ltd.; Fulcrum Global Technologies Private, Ltd.; Focus Core Inc.
6	Suzan Mustafi	Vanta Administrator	Fulcrum Global Technologies, Inc.; Fulcrum Global Technologies UK Ltd.; Fulcrum Global Technologies Private, Ltd.; Focus Core Inc.
7	Ryan George	Senior Security Engineer	Fulcrum Global Technologies, Inc.; Fulcrum Global Technologies UK Ltd.; Fulcrum Global Technologies Private, Ltd.; Focus Core Inc.
8	Vincent Maggio	Senior Information Technology Manager	Fulcrum Global Technologies, Inc.; Fulcrum Global Technologies UK Ltd.; Fulcrum Global Technologies Private, Ltd.; Focus Core 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	20 days
Surveillance ISMS audit time	12.5 days
Surveillance dates	31-Aug-26 to 25-Sep-26
Surveillance AIMS audit time	7.5 days
Surveillance dates	31-Aug-26 to 25-Sep-26
Deviations from audit time	No audit time deviations.

© 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	ISMS: *"Fulcrum Global Technologies, Inc. along with the organizational units Fulcrum Global Technologies UK Ltd., Fulcrum Global Technologies Private, Ltd., and Focus Core Inc. has implemented an Information Security Management System to support the design, development, testing, deployment, operation, maintenance and support of its Fulcrum Snap™ solutions for the legal and professional services markets."* AIMS: *"Fulcrum Global Technologies, Inc. along with the organizational units Fulcrum Global Technologies UK Ltd., Fulcrum Global Technologies Private, Ltd., and Focus Core Inc. have implemented an Artificial Intelligence Management System that governs the use of generative AI systems within its business for content creation and the integration of AI technologies in the design, development, deployment and operation of its Fulcrum Snap™ system to provide intelligent process automation solutions for the legal and professional services markets."*
AIMS role(s)	AI Developer
Number of personnel (FTE and contractor)	441
Processes & activities in-scope	Development, delivery, and management of Fulcrum Snap system.
Third parties	Google, Inc. Digital Realty Trust Microsoft Gitlab PenTest Tools Atlassian Zendesk ServiceNow LinkSquares AlertFind AlertMedia 1Password Mimecast Vanta

© 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.

	SAP
Audit participants	Gerardo Valderrama, Lead Auditor, Insight Assurance, LLC.; John Kinnane, Exec VP of Security - Network, Information, and Compliance, Fulcrum Global Technologies, Inc.; Fulcrum Global Technologies UK Ltd.; Fulcrum Global Technologies Private, Ltd.; Focus Core Inc.; Martin Telfer, CIO / CISO, Fulcrum Global Technologies, Inc.; Fulcrum Global Technologies UK Ltd.; Fulcrum Global Technologies Private, Ltd.; Focus Core Inc.; Vincent Puzar, Associate Director, Security Operations, Fulcrum Global Technologies, Inc.; Fulcrum Global Technologies UK Ltd.; Fulcrum Global Technologies Private, Ltd.; Focus Core Inc.; Kanika Capoor, GRC Analyst, Fulcrum Global Technologies, Inc.; Fulcrum Global Technologies UK Ltd.; Fulcrum Global Technologies Private, Ltd.; Focus Core Inc.; Suzan Mustafi, Vanta Administrator, Fulcrum Global Technologies, Inc.; Fulcrum Global Technologies UK Ltd.; Fulcrum Global Technologies Private, Ltd.; Focus Core Inc.; Ryan George, Senior Security Engineer, Fulcrum Global Technologies, Inc.; Fulcrum Global Technologies UK Ltd.; Fulcrum Global Technologies Private, Ltd.; Focus Core Inc.; Vincent Maggio, Senior Information Technology Manager, Fulcrum Global Technologies, Inc.; Fulcrum Global Technologies UK Ltd.; Fulcrum Global Technologies Private, Ltd.; Focus Core Inc.
Other information, if applicable	Not applicable

Detail of Sites

Address	MS	Site-specific activities
Central site: 1901 N Roselle Road, Schaumburg, Chicago, IL 60195	ISMS & AIMS	Development, delivery, and management of Fulcrum Snap system.
Site 1: 1 St. Katharine's Way, London E1W 1UN, United Kingdom	ISMS & AIMS	Development, delivery, and management of Fulcrum Snap system.
Site 2: My Home Twitza, 14th Floor APIIC Hyderabad Knowledge City Raidurg, Hyderabad 50081, Telagana, India	ISMS & AIMS	Development, delivery, and management of Fulcrum Snap system.
Site 3: D. No. 4-57-6, Plot No. 103, Lawsons Bay Colony, North East Layout, Visakhapatnam, 530017, Andhra Pradesh, India	ISMS & AIMS	Development, delivery, and management of Fulcrum Snap system.

© 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 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/IEC 17021-1:2015, ISO/IEC 27006-1:2024, ISO/IEC 42001:2023, ISO/IEC 42006:2025, CSA STAR Level 2 & Insight Assurance Certification Terms and Conditions.
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. 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 & AIMS 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: 2.0.1 Date: 3-Mar-26 No necessary controls had been omitted from the statement of applicability. Appropriate justifications for

© 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.

	inclusions and, where applicable, exclusions of controls were documented.
Management Review	Version: 28-Aug-26 Date:28-Aug-26 The ISMS & AIMS committee was comprised by the following members: • Chief Information Officer / Chief Information Security Officer • EVP of Security - Network, Information, and Compliance • VP- Innovation and Solutions • Associate Director - Security, Information, and Compliance • Assistant Director - Security Operations • Sr. IT Manager • Compliance Officer, Office of General Counsel • Infrastructure Manager • Junior Security Engineer • Associate - Office of General Counsel and it is scheduled to meet monthly. 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. The organization documented the approvals, feedback & outcome of these reviews.
Internal Audit Report	Version: 28-Aug-26 Date: 28-Aug-26 ISMS & AIMS The internal audit followed the organization's internal audit program and it identified Eight (8) 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: 18-Aug-26 Date: 18-Aug-26 ISMS The organization's most recent risk assessment identified a total of 101 risks, categorized as 17 High, 43 Medium, 38 Low, and 3 Very Low. Of these, 45 risks were designated for mitigation, while the remaining 56 were accepted in accordance with the organization's established risk acceptance criteria. AIMS The organization's most recent risk assessment

© 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.

	identified a total of 113 risks, categorized as 18 High, 51 Medium, and 44 Low. Of these, 73 risks were designated for mitigation, while the remaining 40 were accepted in accordance with the organization's established risk acceptance criteria.
AI impact assessment overview	Version:17-Aug-26 Date:1.1 The AI System Impact Assessment for Llaila, conducted in alignment with ISO/IEC 42001:2023, evaluated key areas including fairness and accountability, transparency and explainability, security and privacy, safety and accessibility, and financial and legal considerations. The assessment reviewed relevant risks, potential biases, and existing controls, and concluded that appropriate governance and mitigation measures are in place to support the responsible use of the AI system. Based on the assessment results, the Y Information Security Team assigned Llaila a Low AI System Impact Score of 1.0 for 2026, and no Risk Treatment Plans were required at the time of the assessment.

© 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	Zero (0)
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 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 surveillance audit about the management system audited.
Conformity and the effectiveness of the management system	• The auditor determined that the ISMS & AIMS have been implemented effectively and that it is capable of meeting applicable requirements and expected outcomes. • Management demonstrated commitment to the ISMS & AIMS 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. • The organization demonstrates strong leadership commitment to security and compliance, supported by appropriate resource allocation for security initiatives. Operational integrity is upheld through well-defined segregation of duties and robust access controls applied to critical systems. The environment is further strengthened by the effective implementation of technological controls and a mature incident response capability, including regularly tested procedures. Additionally, comprehensive security awareness initiatives ensure a high level of security consciousness across personnel, contributing to a resilient and well-managed security posture

© 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 Vanta 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	Fulcrum GT Scope of the Information Security Management System (ISMS)	2.1.1	4-Mar-26
	Fulcrum GT Information Security Policy	2.0.1	4-Mar-26
	Fulcrum GT Policy Governance & Compliance Policy	2.0.1	4-Mar-26
	Fulcrum GT Operations Security Policy	2.0.1	21-Feb-26
Scope of the ISMS	Fulcrum GT Scope of the Information Security Management System (ISMS)	2.1.1	4-Mar-26
Information security policy	Fulcrum GT Information Security Policy	2.0.1	4-Mar-26
Definition of security roles and responsibilities	Information Security Roles, Responsibilities, and Authorities for the ISMS and AIMS	2.1.0	24-Jul-26
	Fulcrum GT Structure and Reporting Lines for IT Resources	30-Jun-26	30-Jun-26
Information security risk assessment process	Fulcrum GT Risk Management Policy	2.0.1	21-Feb-26
	ISMS Information Security Objectives Plan	1.0.1	4-Mar-26
Information security risk treatment process	Fulcrum GT Risk Management Policy	2.0.1	21-Feb-26
	ISMS Information Security Objectives Plan	1.0.1	4-Mar-26
	IT Risk Assessment	18-Aug-26	18-Aug-26
Statement of Applicability	Fulcrum GT - ISMS Statement Of Applicability	2.0.1	3-Mar-26
Information security objectives	ISMS Information Security Objectives Plan	1.0.1	4-Mar-26
Planning of changes	Fulcrum GT Scope of the Information Security Management System (ISMS)	2.1.1	4-Mar-26
	Fulcrum GT Information Security Policy	2.0.1	4-Mar-26
	Fulcrum GT Policy Governance & Compliance Policy	2.0.1	4-Mar-26
	Fulcrum GT Operations Security Policy	2.0.1	21-Feb-26
	Fulcrum GT ISMS and AIMS Communication Policy	2.1.1	4-Mar-26

Evidence of Competence	Fulcrum GT Human Resource Security Policy	2.0.1	21-Feb-26
	Fulcrum GT Acceptable Use Policy for Information Technology and Artificial Intelligence	2.0.1	21-Feb-26
Security awareness	Security Awareness Training Matrix	27-Aug-26	27-Aug-26
	Fulcrum GT Human Resource Security Policy	2.0.1	21-Feb-26
	Fulcrum GT Acceptable Use Policy for Information Technology and Artificial Intelligence	2.0.1	21-Feb-26
Communications plan	ISMS Information Security Objectives Plan	1.0.1	4-Mar-26
	Fulcrum GT ISMS and AIMS Communication Policy	2.1.1	4-Mar-26
Documented Information Determined by the Organization as being Necessary for the Effectiveness of the ISMS	Fulcrum GT Scope of the Information Security Management System (ISMS)	2.1.1	4-Mar-26
	Fulcrum GT Information Security Policy	2.0.1	4-Mar-26
	Fulcrum GT Policy Governance & Compliance Policy	2.0.1	4-Mar-26
	Fulcrum GT Operations Security Policy	2.0.1	21-Feb-26
	ISMS Information Security Objectives Plan	1.0.1	4-Mar-26
	Fulcrum GT ISMS and AIMS Communication Policy	2.1.1	4-Mar-26
Operations Planning and Control	FGT Change Management Approval Workflow	28-Dec-25	28-Dec-25
	Fulcrum GT Change Management Policy	2.1.0	25-Jan-26
Results of the Information Security Risk Assessments	Fulcrum GT Risk Management Policy	2.0.1	21-Feb-26
	ISMS Information Security Objectives Plan	1.0.1	4-Mar-26
	IT Risk Assessment	18-Aug-26	18-Aug-26
Results of the Information Security Risk Treatment	Fulcrum GT Risk Management Policy	2.0.1	21-Feb-26
	ISMS Information Security Objectives Plan	1.0.1	4-Mar-26
	IT Risk Assessment	18-Aug-26	18-Aug-26
Evidence of the Monitoring and Measurement Results	ISO & CSA STAR Internal Audit	28-Aug-26	28-Aug-26
	ISMS Information Security Objectives Plan	1.0.1	4-Mar-26
Internal audit	ISO & CSA STAR Internal Audit	28-Aug-26	28-Aug-26
Internal audit program	ISO & CSA STAR Internal Audit	28-Aug-26	28-Aug-26
	Fulcrum GT - DRL Mapping to Controls - 2026 Internal Audit	20-Jul-26	20-Jul-26
Management review inputs	August 2026 Management Review of Fulcrum Information Security Management System and Artificial Intelligence Management System	28-Aug-26	28-Aug-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.

Evidence of the Results of the Management Reviews	August 2026 Management Review of Fulcrum Information Security Management System and Artificial Intelligence Management System	28-Aug-26	28-Aug-26
Nonconformity and corrective action	Fulcrum GT ISMS and AIMS Non-Conformities and Corrective Actions Register	3-Sep-26	3-Sep-26
Inventory of Information and Other Associated Asset	Fulcrum GT Asset Management Policy Vanta Inventory	2.0.1 4-Mar-26	21-Feb-26 4-Mar-26
Acceptable Use of Information And Other Associated Assets	Fulcrum GT Acceptable Use Policy for Information Technology and Artificial Intelligence	2.0.1	21-Feb-26
Access control	Not Selected - Surveillance	Not Selected - Surveillance	Not Selected - Surveillance
Information security in supplier relationships	Fulcrum GT Vendor Management Policy	1.5	8-Jul-26
Information Security for use of Cloud Services (New control)	Fulcrum GT Cloud Services Security Policy	1.2	24-Aug-26
Response to information security events	Compromised Credentials – Investigation Summary Report and Process Improvement Plan Fulcrum GT Incident Response Policy	21-Dec-26 3.1.1	21-Dec-26 24-Jul-26
Information and Communication Technology (ICT) Readiness for Business Continuity (New control)	Not Selected - Surveillance	Not Selected - Surveillance	Not Selected - Surveillance
Legal, Statutory, Regulatory, and Contractual Requirements	Not Selected - Surveillance	Not Selected - Surveillance	Not Selected - Surveillance

© 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.

Confidentiality / non-disclosure agreements	Not Selected - Surveillance	Not Selected - Surveillance	Not Selected - Surveillance
Configuration Management (New control)	Fulcrum GT Change Management Policy Infrastructure Changes Sample Code Changes Sample	2.1.0 19-Oct-26 19-Oct-26	25-Jan-26 19-Oct-26 19-Oct-26
Data Masking (New control)	Not Applicable - Excluded SoA	Not Applicable - Excluded SoA	Not Applicable - Excluded SoA
Monitoring Activities / Network Monitoring (New control)	Not Selected - Surveillance	Not Selected - Surveillance	Not Selected - Surveillance
Secure systems architecture and engineering principles	Not Selected - Surveillance	Not Selected - Surveillance	Not Selected - Surveillance
Secure Coding (New control)	Not Selected - Surveillance	Not Selected - Surveillance	Not Selected - Surveillance

© 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 42001 items	Evidence	Version	Date
Interested Parties and their Requirements	Fulcrum GT AIMS Scope Policy	1.1.1	24-Jul-26
Scope of the AIMS	Fulcrum GT AIMS Scope Policy	1.1.1	24-Jul-26
AI Policy	Fulcrum GT AI Policy	1.1.0	15-Jan-26
Evidence of roles, responsibilities and authorities assigned for the AIMS	FULCRUM GT AI Governance Charter	0.9	May-26
AI Risk Assessment Process	Fulcrum GT Risk Management Policy Risk Register	2.0.1 8-Sept-26	21-Feb-26 8-Sept-26
AI Risk Treatment Process	Fulcrum GT Risk Management Policy Risk Register	2.0.1 8-Sept-26	21-Feb-26 8-Sept-26
Statement of Applicability	FULCRUM GT - ISMS STATEMENT OF APPLICABILITY	2.0.1	3-Mar-26
AI System Impact Assessment Process	Fulcrum GT AIMS Impact Assessment Policy Fulcrum GT AI System Impact Assessment	1.1.0 1.1	15-Jan-26 17-Aug-26
AI Objectives	Fulcrum GT AI Policy	1.1.0	15-Jan-26
Evidence of Competence	Performance Evaluation Sample Performance Evaluation Template People Export	14-Apr-26 8-Jun-26 1-Sept-26	14-Apr-26 8-Jun-26 1-Sept-26
AI Awareness	People Export Fulcrum GT AI Policy	1-Sept-26 1.1.0	1-Sept-26 15-Jan-26
Documented Information Determined by the Organization as being Necessary for the Effectiveness of the AIMS	Fulcrum GT - ISO and CSA Star Internal Audit - Final Report Management Review of Fulcrum Information Security Management System and Artificial Intelligence Management System Risk Register Fulcrum GT AIMS Scope Policy	28-Aug-26 28-Aug-26 8-sept-26 1.1.1	28-Aug-26 28-Aug-26 8-sept-26 24-Jul-26
Operations Planning and Control	Fulcrum GT Risk Management Policy Risk Register	2.0.1 8-Sept-36	21-Feb-26 8-Sept-36
Results of the Information Security Risk Assessments	Fulcrum GT Risk Management Policy Risk Register	2.0.1	21-Feb-26 8-Sept-36

© 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-Sept-36	
Results of the Information Security Risk Treatment	Fulcrum GT Risk Management Policy Risk Register	2.0.1 8-Sept-36	21-Feb-26 8-Sept-36
Results of all AI system impact assessments	Fulcrum GT AIMS Impact Assessment Policy Fulcrum GT AI System Impact Assessment	1.1.0 1.1	15-Jan-26 17-Aug-26
Evidence of the Monitoring and Measurement Results	Fulcrum GT AI Policy Monthly Security Team Meeting Agenda	1.1.0 31-Jul-26	15-Jan-26 31-Jul-26
Internal Audit	Fulcrum GT - ISO and CSA Star Internal Audit - Final Report	28-Aug-26	28-Aug-26
Internal Audit Program	Fulcrum GT - ISO and CSA Star Internal Audit - Final Report	28-Aug-26	28-Aug-26
Management review inputs	Management Review of Fulcrum Information Security Management System and Artificial Intelligence Management System	28-Aug-26	28-Aug-26
Evidence of the Results of the Management Reviews	Management Review of Fulcrum Information Security Management System and Artificial Intelligence Management System	28-Aug-26	28-Aug-26
Nonconformity and corrective action	Fulcrum GT ISMS and AIMS Non-Conformities and Corrective Action	3-Sept-26	3-Sept-26
Documented information of relevant resources required for the activities at given AI system life cycle stages and other AI-related activities relevant for the organization.	Snap AIQ Architecture FULCRUM GT AI Governance Charter Vendor Export	20-Jul-26 0.9 1-Sept-26	20-Jul-26 May-26 1-Sept-26
Documented information about the data resources utilized for the AI system.	Fulcrum Snap AIQ™ Guidelines – Data Management Analysis Claude Enterprise - Data Management Google Gemini Enterprise - Data Management Analysis	1.0.0 1.0.0 1.0.0	21-Sept-26 22-Sept-26 22-Sept-26
Documented information about the tooling resources utilized for the AI system	Snap AIQ Architecture Vendor Export	20-Jul-26 1-Sept-26	20-Jul-26 1-Sept-26
Document information about the system and computing resources utilized for the AI system	Not Selected - Surveillance	Not Selected - Surveillance	Not Selected - Surveillance

© 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.

Document information about the human resources and their competences utilized for the development, deployment, operation, change management, maintenance, transfer and decommissioning, as well as verification and integration of the AI system	Not Selected - Surveillance	Not Selected - Surveillance	Not Selected - Surveillance
Document information of the results of AI system impact assessments and retain results for a defined period	Fulcrum GT AIMS Impact Assessment Policy Fulcrum GT AI System Impact Assessment	1.1.0 1.1	15-Jan-26 17-Aug-26
Documented information about the assessment of potential impacts of AI systems to individuals or groups of individuals throughout the system's life cycle	Fulcrum GT AIMS Impact Assessment Policy Fulcrum GT AI System Impact Assessment	1.1.0 1.1	15-Jan-26 17-Aug-26
Documented information about the potential societal impacts of their AI systems throughout their life cycle	Fulcrum GT AIMS Impact Assessment Policy Fulcrum GT AI System Impact Assessment	1.1.0 1.1	15-Jan-26 17-Aug-26
Documented information about the identification and documentation of objectives to guide the responsible development AI systems, and take those objectives into account and integrate measures to achieve them in the development life cycle.	Fulcrum GT AI Policy Fulcrum GT Secure Systems Development Policy	1.1.0 2.0.1	15-Jan-26 21-Feb-26
Documented information about the definition and documentation of the specific processes for the responsible design and development of the AI system.	Fulcrum GT AI Policy Fulcrum GT Secure Systems Development Policy	1.1.0 2.0.1	15-Jan-26 21-Feb-26
Documented information about the AI system design and development based on organizational objectives, documented requirements and specification criteria	Fulcrum GT AI Policy Fulcrum GT Secure Systems Development Policy	1.1.0 2.0.1	15-Jan-26 21-Feb-26
Documented information about the verification and validation measures for the AI system and specify criteria for their use.	Not Selected - Surveillance	Not Selected - Surveillance	Not Selected - Surveillance
Documented information about the deployment plan to ensure that appropriate requirements are met prior to deployment.	Not Selected - Surveillance	Not Selected -	Not Selected - Surveillance

© 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.

		Surveillance	
Documented information about the necessary elements for the ongoing operation of the AI system. At the minimum, this should include system and performance monitoring, repairs, updates and support.	Not Selected - Surveillance	Not Selected - Surveillance	Not Selected - Surveillance
Technical documentation needed for each relevant category of interested parties, such as users, partners, supervisory authorities, and provide the technical documentation to them in the appropriate form.	Not Selected - Surveillance	Not Selected - Surveillance	Not Selected - Surveillance
Documented information about the requirements for data quality used to develop and operate AI systems	Fulcrum Snap AIQ™ Guidelines – Data Management Analysis Claude Enterprise - Data Management Google Gemini Enterprise - Data Management Analysis	1.0.0 1.0.0 1.0.0	21-Sept-26 22-Sept-26 22-Sept-26
Evidence of data quality checks to ensure data quality standards are met	Fulcrum Snap AIQ™ Guidelines – Data Management Analysis Claude Enterprise - Data Management Google Gemini Enterprise - Data Management Analysis	1.0.0 1.0.0 1.0.0	21-Sept-26 22-Sept-26 22-Sept-26
Documented information about the process defined for recording the provenance of data used in AI systems over the life cycles of the data and the AI system.	Not Selected - Surveillance	Not Selected - Surveillance	Not Selected - Surveillance
Documented information about the criteria for selecting data preparations and the data preparation methods to be used.	Not Selected - Surveillance	Not Selected - Surveillance	Not Selected - Surveillance
Documented information about the plan for communicating incidents to users of the AI system.	Not Selected - Surveillance	Not Selected - Surveillance	Not Selected - Surveillance
Documented information about the organization's obligations to report information about the AI system to interested parties.	Not Selected - Surveillance	Not Selected - Surveillance	Not Selected - Surveillance
Documented information about the processes defined for the responsible use of AI systems.	Fulcrum GT AI Policy Fulcrum GT Acceptable Use Policy for	1.1.0 2.0.1	15-Jan-26 21-Feb-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 Technology and Artificial Intelligence Fulcrum Snap AIQ Epoch user training	18-Jun-26	18-Jun-26
Documented information about the identified objectives to guide the responsible use of AI systems.	Fulcrum GT AI Policy Fulcrum GT Acceptable Use Policy for Information Technology and Artificial Intelligence	1.1.0 2.0.1	15-Jan-26 21-Feb-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

Surveillance Requirements

Surveillance Requirements	Conformance Testing Result
All statements with respect to operations regarding the certified standard (e.g. promotional material, website, marketing)	Conforming
Most recent risk assessment (including the risk assessment report as well as the risk treatment plan)	Conforming
Most recent internal audit (including audit plan and audit results)	Conforming
Most recent management reviews (including required inputs and required outputs)	Conforming
Evidence of the nature of the nonconformity(ies) and any subsequent action(s) taken	Conforming
Evidence of the results of any corrective action	Conforming
Results from monitoring and measurement results for effectiveness of the MS	Conforming
Any complaints related to the ISO certification and the treatment of those complaints	Conforming
Review of any changes pertinent to the MS	Conforming
Evidence of the use of marks and/or any other reference to certification	Conforming
All current MS policies and procedures (specifically those required to support the ISMS)	Conforming
Current statement of applicability	Conforming
Progress of planned activities aimed at continual improvement	Conforming
Evidence of continuing operational control of the MS	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.

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
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

© 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.

5.2.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
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

© 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.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
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

© 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.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	Conforming
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	Conforming
7.5.3.f	retention and disposition.	Conforming
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

© 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.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
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	

© 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.

9.3.1.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:	Conforming
10.2.a.1	take action to control and correct it; and	Conforming
10.2.a.2	deal with the consequences;	Conforming
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:	Conforming
10.2.b.1	reviewing the nonconformity;	Conforming
10.2.b.2	determining the causes of the nonconformity; and	Conforming
10.2.b.3	determining if similar nonconformities exist, or could potentially occur;	Conforming
10.2.c	implement any action needed;	Conforming
10.2.d	review the effectiveness of any corrective action taken; and	Conforming
10.2.e	make changes to the information security management system, if necessary.	Conforming
Documented information shall be available as evidence of:		
10.2.f	the nature of the nonconformities and any subsequent actions taken, and	Conforming
10.2.g	the results of any corrective action.	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.

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

© 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.

5.15	Access Control	Rules to control physical and logical access to information and other associated assets shall be established and implemented based on business and information security requirements.	Not Selected for Surveillance
5.16	Identity management	The full life cycle of identities shall be managed.	Not Selected for Surveillance
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.	Not Selected for Surveillance
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.	Not Selected for Surveillance
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.	Not Selected for Surveillance
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.	Not Selected for Surveillance
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.	Not Selected for Surveillance

© 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.

5.28	Collection of evidence	The organization shall establish and implement procedures for the identification, collection, acquisition and preservation of evidence related to information security events.	Not Selected for Surveillance
5.29	Information security during disruption	The organization shall plan how to maintain information security at an appropriate level during disruption.	Not Selected for Surveillance
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.	Not Selected for Surveillance
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.	Not Selected for Surveillance
5.32	Intellectual property rights	The organization shall implement appropriate procedures to protect intellectual property rights.	Not Selected for Surveillance
5.33	Protection of records	Records shall be protected from loss, destruction, falsification, unauthorized access and unauthorized release.	Not Selected for Surveillance
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.	Not Selected for Surveillance
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.	Not Selected for Surveillance
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.	Not Selected for Surveillance
5.37	Documented operating procedures	Operating procedures for information processing facilities shall be documented and made available to personnel who need them.	Not Selected for Surveillance
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

© 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.

6.5	Responsibilities after termination or change of employment	Information security responsibilities and duties that remain valid after termination or change of employment shall be defined, enforced and communicated to relevant personnel and other interested parties.	Not Selected for Surveillance
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.	Not Selected for Surveillance
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.	Not Selected for Surveillance
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.	Not Selected for Surveillance
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.	Conforming
7.2	Physical entry	Secure areas shall be protected by appropriate entry controls and access points.	Conforming
7.3	Securing offices, rooms, and facilities	Physical security for offices, rooms and facilities shall be designed and implemented.	Conforming
7.4	Physical security monitoring	Premises shall be continuously monitored for unauthorized physical access.	Conforming
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.	Not Selected for Surveillance
7.6	Working in secure areas	Security measures for working in secure areas shall be designed and implemented.	Not Selected for Surveillance
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.	Not Selected for Surveillance
7.8	Equipment siting and protection	Equipment shall be sited securely and protected.	Not Selected for Surveillance
7.9	Security of assets off-premises	Off-site assets shall be protected.	Not Selected for Surveillance
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.	Not Selected for Surveillance
7.11	Supporting utilities	Information processing facilities shall be protected from power failures and other disruptions caused by failures in supporting utilities.	Not Selected for Surveillance
7.12	Cabling security	Cables carrying power, data or supporting information services shall be protected from interception, interference or damage.	Not Selected for Surveillance
7.13	Equipment maintenance	Equipment shall be maintained correctly to ensure availability, integrity and confidentiality of information.	Not Selected for Surveillance
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.	Not Selected for Surveillance
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.	Conforming
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.	Excluded per SoA
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.	Not Selected for Surveillance
8.16	Monitoring	Networks, systems and applications shall be monitored for anomalous behaviour and appropriate actions taken to evaluate potential information security incidents.	Not Selected for Surveillance
8.17	Clock synchronization	The clocks of information processing systems used by the organization shall be synchronized to approved time sources.	Not Selected for Surveillance
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.	Not Selected for Surveillance
8.19	Installation of software on	Procedures and measures shall be implemented to securely manage software installation on operational systems.	Not Selected for Surveillance

© 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.	Not Selected for Surveillance
8.21	Security of network services	Security mechanisms, service levels and service requirements of network services shall be identified, implemented and monitored.	Not Selected for Surveillance
8.22	Segregation of networks	Groups of information services, users and information systems shall be segregated in the organization's networks.	Not Selected for Surveillance
8.23	Web filtering	Access to external websites shall be managed to reduce exposure to malicious content.	Not Selected for Surveillance
8.24	Use of cryptography	Rules for the effective use of cryptography, including cryptographic key management, shall be defined and implemented.	Not Selected for Surveillance
8.25	Secure development lifecycle	Rules for the secure development of software and systems shall be established and applied.	Not Selected for Surveillance
8.26	Application security requirements	Information security requirements shall be identified, specified and approved when developing or acquiring applications.	Not Selected for Surveillance
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.	Not Selected for Surveillance
8.28	Secure coding	Secure coding principles shall be applied to software development.	Not Selected for Surveillance
8.29	Security testing in development and acceptance	Security testing processes shall be defined and implemented in the development life cycle.	Not Selected for Surveillance
8.30	Outsourced development	The organization shall direct, monitor and review the activities related to outsourced system development.	Not Selected for Surveillance
8.31	Separation of development, test and production environments	Development, testing and production environments shall be separated and secured.	Not Selected for Surveillance
8.32	Change management	Changes to information processing facilities and information systems shall be subject to change management procedures.	Not Selected for Surveillance
8.33	Test information	Test information shall be appropriately selected, protected and managed.	Not Selected for Surveillance
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.	Not Selected for Surveillance

© 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 42001:2023 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 result(s) of its AI 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 AI 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 AI management system.	Conforming
4.3	Determining the scope of the AI management system	
The organization shall determine the boundaries and applicability of AI 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
4.4	The organization shall establish, implement, maintain and continually improve an AI 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 AI management system by:		
5.1.a	ensuring the AI policy and the AI objectives are established and are compatible with the strategic direction of the organization;	Conforming
5.1.b	ensuring the integration of the AI management system requirements into the organization's processes;	Conforming
5.1.c	ensuring that the resources needed for the AI management system are available;	Conforming
5.1.d	communicating the importance of effective AI management and of conforming to the AI management system requirements;	Conforming
5.1.e	ensuring that the AI management system achieves its intended outcome(s);	Conforming
5.1.f	directing and supporting persons to contribute to the effectiveness of the AI management system;	Conforming
5.1.g	promoting continual improvement; and	Conforming
5.1.h	supporting other relevant management roles to demonstrate their leadership as it applies to their areas of responsibility.	Conforming
5.2	AI Policy	
5.2.a	is appropriate to the purpose of the organization;	Conforming
5.2.b	provides a framework for setting AI objectives;	Conforming
5.2.c	includes a commitment to meet applicable requirements;	Conforming
5.2.d	includes a commitment to continual improvement of the AI management system.	Conforming
The information security policy shall:		
5.2.e	be available as documented information;	Conforming
5.2.f	provides a framework for setting AI objectives	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.

5.2.g	be communicated within the organization; and	Conforming
5.2.h	be available to interested parties, as appropriate.	Conforming
5.3	Roles, responsibilities and authorities	
Top management shall ensure that the responsibilities and authorities for relevant roles are assigned and communicated within the organization. Top management shall assign the responsibility and authority for:		
5.3.a	ensuring that the AI management system conforms to the requirements of this document;	Conforming
5.3.b	reporting on the performance of the AI management system to top management.	Conforming
Clause 6	**Planning**	
6.1	Actions to address risks and opportunities	
When planning for the AI 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 AI 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 establish and maintain AI risk criteria that support:		
6.1.1.d	distinguishing acceptable from non-acceptable risks;; and	Conforming
6.1.1.e.1	performing AI risk assessments; and	Conforming
6.1.1.e.2	conducting AI risk treatment; and	Conforming
6.1.1.e.3	assessing AI risk impacts.	
The organization shall determine the risks and opportunities according to:		
6.1.1.e.4	the domain and application context of an AI system;	Conforming
6.1.1.e.5	the intended use;	Conforming
6.1.1.e.6	the external and internal context described in 4.1.	Conforming
The organization shall plan:		
6.1.1.e.7	actions to address these risks and opportunities;	Conforming
6.1.1.e.7.1	how to: 1) integrate and implement the actions into its AI management system processes;	Conforming
6.1.1.e.7.2	2) evaluate the effectiveness of these actions.	Conforming
6.1.2	AI risk assessment	
The organization shall define and establish an AI risk assessment process that:		
6.1.2.a	is informed by and aligned with the AI policy (5.2) and AI objectives (6.2);	Conforming
6.1.2.b	is designed such that repeated AI risk assessments can produce consistent, valid and comparable results;	Conforming
6.1.2.c	identifies risks that aid or prevent achieving its AI objectives;	Conforming
6.1.2.d.1	analyses the AI risks to: 1) assess the potential consequences to the organization, individuals and societies that would result if the identified risks were to materialize;	Conforming
6.1.2.d.2	2) assess, where applicable, the realistic likelihood of the identified risks;	Conforming
6.1.2.d.3	3) determine the levels of risk;	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.e.1	evaluates the AI risks to: 1) compare the results of the risk analysis with the risk criteria (6.1.1);	Conforming
6.1.2.e.2	2) prioritize the assessed risks for risk treatment.	Conforming
6.1.3	AI risk treatment	
Taking the risk assessment results into account, the organization shall define an AI risk treatment process to:		
6.1.3.a	select appropriate AI risk treatment options;	Conforming
6.1.3.b	determine all controls that are necessary to implement the AI risk treatment options chosen and compare the controls with those in Annex A to verify that no necessary controls have been omitted;	Conforming
6.1.3.c	consider the controls from Annex A that are relevant for the implementation of the AI risk treatment options;	Conforming
6.1.3.d	identify if additional controls are necessary beyond those in Annex A in order to implement all risk treatment options;	Conforming
6.1.3.e	consider the guidance in Annex B for the implementation of controls determined in b) and c);	Conforming
6.1.3.f	produce a statement of applicability that contains the necessary controls [see b), c) and d)] and provide justification for inclusion and exclusion of controls. Justification for exclusion can include where the controls are not deemed necessary by the risk assessment and where they are not required by (or are subject to exceptions under) applicable external requirements.	Conforming
6.1.3.g.1	formulate an AI risk treatment plan. The organization shall obtain approval from the designated management for the AI risk treatment plan and for acceptance of the residual AI risks. The necessary controls shall be: aligned to the objectives in 6.2;	Conforming
6.1.3.g.2	available as documented information;	Conforming
6.1.3.g.3	communicated within the organization;	Conforming
6.1.3.g.4	available to interested parties, as appropriate.	Conforming
6.1.4	AI system impact assessment	
6.1.4.a	The organization shall define a process for assessing the potential consequences for individuals or groups of individuals, or both, and societies that can result from the development, provision or use of AI systems.	Conforming
6.1.4.b	The AI system impact assessment shall determine the potential consequences an AI system's deployment, intended use and foreseeable misuse has on individuals or groups of individuals, or both, and societies.	Conforming
6.1.4.c	The AI system impact assessment shall take into account the specific technical and societal context where the AI system is deployed and applicable jurisdictions.	Conforming
6.1.4.d	The result of the AI system impact assessment shall be documented. Where appropriate, the result of the system impact assessment can be made available to relevant interested parties as defined by the organization.	Conforming
6.1.4.e	The organization shall consider the results of the AI system impact assessment in the risk assessment (see 6.1.2). A.5 in Table A.1 provides controls for assessing impacts of AI systems.	Conforming
6.2	AI objectives and planning to achieve them	

© 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 shall establish AI objectives at relevant functions and levels. The AI objectives shall:		
6.2.a	be consistent with the AI policy (see 5.2);	Conforming
6.2.b	be measurable (if practicable);	Conforming
6.2.c	take into account applicable requirements;	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 AI 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 AI 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 AI management system.	Conforming
7.2	Competence	
The organization shall:		
7.2.a	determine the necessary competence of person(s) doing work under its control that affects its AI 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 AI policy;	Conforming
7.3.b	their contribution to the effectiveness of the AI management system, including the benefits of improved AI performance; and	Conforming
7.3.c	the implications of not conforming with the AI management system requirements.	Conforming
7.4	Communication	
The organization shall determine the need for internal and external communications relevant to the AI 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 AI management system shall include:		
7.5.1.a	documented information required by this document; 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.

7.5.1.b	documented information determined by the organization as being necessary for the effectiveness of the AI 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	Conforming
7.5.2.c	review and approval for suitability and adequacy.	Conforming
7.5.3	Control of documented information	
Documented information required by the AI 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	Conforming
7.5.3.f	retention and disposition.	Conforming
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	The organization shall implement the controls determined according to 6.1.3 that are related to the operation of the AI management system	Conforming
8.1.c	Documented information shall be available to the extent necessary to have confidence that the processes have been carried out as planned.	Conforming
8.1.d	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.e	The organization shall ensure that externally provided processes, products or services that are relevant to the AI management system are controlled.	Conforming
8.2	risk assessment	
8.2.a	The organization shall perform AI risk assessments in accordance with 6.1.2 at planned intervals or when significant changes are proposed or occur.	Conforming
8.2.b	The organization shall retain documented information of the results of all AI risk assessments.	Conforming
8.3	AI risk treatment	
8.3.a	The organization shall implement the AI risk treatment plan according to 6.1.3 and verify its effectiveness.	Conforming
8.3.b	When risk assessments identify new risks that require treatment, a risk treatment process in accordance with 6.1.3 shall be performed for these risks.	Conforming
8.3.c	When risk treatment options as defined by the risk treatment plan are not effective, these treatment options shall be reviewed 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.

	revalidated following the risk treatment process according to 6.1.3 and the risk treatment plan shall be updated.	
8.3.d	The organization shall retain documented information of the results of all AI risk treatments.	Conforming
8.4	AI system impact assessment	
8.4.a	The organization shall perform AI system impact assessments according to 6.1.4 at planned intervals or when significant changes are proposed to occur.	Conforming
8.4.b	The organization shall retain documented information of the results of all AI system impact assessments.	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;	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 AI management system:		
9.2.a.1	conforms to the organization's own requirements for its AI 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 objectives, criteria and scope for each audit;	Conforming
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
9.2.2.d	Documented information shall be available as evidence of the implementation of the audit programme(s) and the audit results.	Conforming
9.3	Management review	
9.3.1.a	Top management shall review the organization's AI 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 AImanagement system;	Conforming
9.3.2.c	changes in needs and expectations of interested parties that are relevant to the AI management system;	Conforming
9.3.2.d	information on the AI management system performance, including trends in:	Conforming
9.3.2.d.1	nonconformities and corrective actions;	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.

9.3.2.d.2	monitoring and measurement results;	Conforming
9.3.2.d.3	audit results;	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 AI 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 AI 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:	Conforming
10.2.a.1	take action to control and correct it; and	Conforming
10.2.a.2	deal with the consequences;	Conforming
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:	Conforming
10.2.b.1	reviewing the nonconformity;	Conforming
10.2.b.2	determining the causes of the nonconformity; and	Conforming
10.2.b.3	determining if similar nonconformities exist, or could potentially occur;	Conforming
10.2.c	implement any action needed;	Conforming
10.2.d	review the effectiveness of any corrective action taken; and	Conforming
10.2.e	make changes to the AI management system, if necessary.	Conforming
Documented information shall be available as evidence of:		
10.2.f	the nature of the nonconformities and any subsequent actions taken, and	Conforming
10.2.g	the results of any corrective action.	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.

ISO/IEC 42001:2023 Annex A Controls

A.2	**Policies related to AI:** To provide management direction and support for AI systems according to business requirements.		
A.2.2	AI policy	The organization shall document a policy for the development or use of AI systems.	Conforming
A.2.3	Alignment with other organizational policies	The organization shall determine where other policies can be affected by or apply to, the organization's objectives with respect to AI systems.	Conforming
A.2.4	Review of the AI policy	The AI policy shall be reviewed at planned intervals or additionally as needed to ensure its continuing suitability, adequacy and effectiveness.	Not Selected for Surveillance
A.3	**Internal organization:** To Establish accountability within the organization to uphold its responsible approach for the implementation, operation and management of AI systems.		
A.3.2	AI roles and responsibilities	Roles and responsibilities for AI shall be defined and allocated according to the needs of the organization	Conforming
A.3.3	Reporting of concerns	The organization shall define and put in place a process to report concerns about the organization's role with respect to an AI system throughout its life cycle.	Not Selected for Surveillance
A.4	**Resources for AI systems:** To ensure that the organization accounts for the resources (including AI system components and assets) of the AI system to fully understand and address risks and impacts.		
A.4.2	Resource documentation	The organization shall identify and document relevant resources required for the activities at given AI system life cycle stages and other AI-related activities relevant for the organization.	Conforming
A.4.3	Data resources	As part of resource identification, the organization shall document information about the data resources utilized for the AI system.	Conforming
A.4.4	Tooling resources	As part of resource identification, the organization shall document information about the tooling resources utilized for the AI system.	Conforming
A.4.5	System and computing resources	As part of resource identification, the organization shall document information about the system and computing resources utilized for the AI system.	Not Selected for Surveillance
A.4.6	Human resources	As part of resource identification, the organization shall document information about the human resources and their competences utilized for the development, deployment, operation, change management, maintenance, transfer and decommissioning, as well as verification and integration of the AI system.	Not Selected for Surveillance
A.5	**Assessing impacts of AI systems:** To assess AI system impacts to individuals or groups of individuals, or both, and societies affected by the AI system throughout its life cycle.		
A.5.2	AI system impact assessment process	The organization shall establish a process to assess the potential consequences for individuals or groups of individuals, or both, and societies that can result from the AI system throughout its life cycle.	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.

A.5.3	Documentation of AI system impact assessment	The organization shall document the results of AI system impact assessments and retain results for a defined period.	Conforming
A.5.4	Assessing AI system impact on individuals or groups of individuals	The organization shall assess and document the potential impacts of AI systems to individuals or groups of individuals throughout the system's life cycle	Not Selected for Surveillance
A.5.5	Assessing societal impacts of AI systems	The organization shall assess and document the potential societal impacts of their AI systems throughout their life cycle.	Not Selected for Surveillance
A.6	**AI system life cycle:**		
A.6.1	Management guidance for AI system development: To ensure that the organization identifies and documents objectives and implements processes for the responsible design and development of AI systems.		
A.6.1.2	Objectives for responsible development of AI system	The organization shall identify and document objectives to guide the responsible development AI systems, and take those objectives into account and integrate measures to achieve them in the development life cycle.	Conforming
A.6.1.3	Processes for responsible AI system design and development	The organization shall define and document the specific processes for the responsible design and development of the AI system.	Conforming
A.6.2	AI system life cycle To define the criteria and requirements for each stage of the AI system life cycle.		
A.6.2.2	AI system requirements and specifications	The organization shall specify and document requirements for new AI systems or material enhancements to existing systems.	Conforming
A.6.2.3	Documentation of AI system design and development	The organization shall document the AI system design and development based on organizational objectives, documented requirements and specification criteria.	Conforming
A.6.2.4	AI system verification and validation	The organization shall define and document verification and validation measures for the AI system and specify criteria for their use.	Not Selected for Surveillance
A.6.2.5	AI system deployment	The organization shall document a deployment plan and ensure that appropriate requirements are met prior to deployment.	Not Selected for Surveillance
A.6.2.6	AI system operation and monitoring	The organization shall define and document the necessary elements for the ongoing operation of the AI system. At the minimum, this should include system and performance monitoring, repairs, updates and support.	Not Selected for Surveillance
A.6.2.7	AI system technical documentation	The organization shall determine what AI system technical documentation is needed for each relevant category of interested parties, such as users, partners, supervisory authorities, and provide the technical documentation to them in the appropriate form.	Not Selected for Surveillance
A.6.2.8	AI system recording of event logs	The organization shall determine at which phases of the AI system life cycle, record keeping of event logs should be enabled, but at the minimum when the AI system is in use.	Not Selected for Surveillance
A.7	**Data for AI systems:** To ensure that the organization understands the role and impacts of data in AI systems in the application and development, provision or use of AI systems throughout their life cycles.		

© 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.

A.7.2	Data for development and enhancement of AI system	The organization shall define, document and implement data management processes related to the development of AI systems.	Conforming
A.7.3	Acquisition of data	The organization shall determine and document details about the acquisition and selection of the data used in AI systems.	Conforming
A.7.4	Quality of data for AI systems	The organization shall define and document requirements for data quality and ensure that data used to develop and operate the AI system meet those requirements.	Conforming
A.7.5	Data provenance	The organization shall define and document a process for recording the provenance of data used in its AI systems over the life cycles of the data and the AI system.	Not Selected for Surveillance
A.7.6	Data preparation	The organization shall define and document its criteria for selecting data preparations and the data preparation methods to be used.	Not Selected for Surveillance
A.8	**Information for interested parties of AI systems:** To ensure that relevant interested parties have the necessary information to understand and assess the risks and their impacts (both positive and negative).		
A.8.2	System documentation and information for users	The organization shall determine and provide the necessary information to users of the AI system.	Conforming
A.8.3	External reporting	The organization shall provide capabilities for interested parties to report adverse impacts of the AI system.	Conforming
A.8.4	Communication of incidents	The organization shall determine and document a plan for communicating incidents to users of the AI system.	Not Selected for Surveillance
A.8.5	Information for interested parties	The organization shall determine and document their obligations to reporting information about the AI system to interested parties.	Not Selected for Surveillance
A.9	**Use of AI systems:** To ensure that the organization uses AI systems responsibly and per organizational policies.		
A.9.2	Processes for responsible use of AI systems	The organization shall define and document the processes for the responsible use of AI systems.	Conforming
A.9.3	Objectives for responsible use of AI system	The organization shall identify and document objectives to guide the responsible use of AI systems.	Conforming
A.9.4	Intended use of the AI system	The organization shall ensure that the AI system is used according to the intended uses of the AI system and its accompanying documentation.	Not Selected for Surveillance
A.10	**Third-party and customer relationships** To ensure that the organization understands its responsibilities and remains accountable, and risks are appropriately apportioned when third parties are involved at any stage of the AI system life cycle.		
A.10.2	Allocating responsibilities	The organization shall ensure that responsibilities within their AI system life cycle are allocated between the organization, its partners, suppliers, customers and third parties	Conforming
A.10.3	Suppliers	The organization shall establish a process to ensure that its usage of services, products or materials provided by suppliers aligns with the organization's approach to the responsible development and use of AI systems.	Not Selected for Surveillance

© 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.

A.10.4	Customers	The organization shall ensure that its responsible approach to the development and use of AI systems considers their customer expectations and needs.	Not Selected for Surveillance

© 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.

CSA STAR CCM v4.1

Control Domain	Control Title	Control ID	Control Specification	Objective of the control confirmed by Auditor
Audit & Assurance (A&A)				
Audit & Assurance	Audit and Assurance Policy and Procedures	A&A-01	Establish, document, approve, communicate, apply, evaluate and maintain audit and assurance policies and procedures and standards. Review and update the policies and procedures at least annually, or upon significant changes.	Conforming
Audit & Assurance	Independent Assessments	A&A-02	Conduct independent audit and assurance assessments according to relevant standards at least annually.	Conforming
Audit & Assurance	Risk Based Planning Assessment	A&A-03	Perform independent audit and assurance assessments according to risk-based plans and policies,and in response to significant changes or emerging risks.	Conforming
Audit & Assurance	Requirements Compliance	A&A-04	Verify compliance with all relevant standards, regulations, legal/contractual, and statutory requirements applicable to the audit.	Conforming
Audit & Assurance	Audit Management Process	A&A-05	Define and implement an Audit Management process aligned with relevant auditing standards to support audit planning, risk analysis, security control assessment, conclusion, remediation schedules, report generation, and review of past reports and supporting evidence.	Conforming
Audit & Assurance	Remediation	A&A-06	Establish, document, approve, communicate, apply, evaluate and maintain a risk-based corrective action plan to remediate audit findings, regularly review and report remediation status to relevant stakeholders.	Conforming
Application & Interface Security (AIS)				
Application & Interface Security	Application and Interface Security Policy and Procedures	AIS-01	Establish, document, approve, communicate, apply, evaluate and maintain policies and procedures for application security. Review and update the policies and procedures at least annually, or upon significant changes.	Conforming
Application & Interface Security	Application Security Baseline Requirements	AIS-02	Establish, document and maintain baseline requirements for securing applications.	Conforming
Application & Interface Security	Application Security Metrics	AIS-03	Define and implement technical and operational metrics in alignment with business objectives, security requirements, and compliance obligations.	Conforming
Application & Interface Security	Secure Application Development Lifecycle	AIS-04	Define and implement a secure SDLC process for application requirements analysis, planning, design, development, testing, deployment, and operation in accordance with security requirements.	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.

Application & Interface Security	Application Security Testing	AIS-05	Implement a testing strategy, including criteria for acceptance of new information systems, upgrades and new versions, which provides application security assurance and maintains compliance while meeting organizational delivery goals. Automate when applicable and possible.	Conforming
Application & Interface Security	Secure Application Deployment	AIS-06	Establish and implement strategies and capabilities for secure, standardized, and compliant application deployment. Automate where possible.	Conforming
Application & Interface Security	Application Vulnerability Remediation	AIS-07	Define and implement a process to remediate application security vulnerabilities, automating remediation when possible.	Conforming
Application & Interface Security	API Security	AIS-08	Define and implement processes, procedures, and technical measures to secure APIs. Review and update for any improvements at least annually or upon significant changes.	Conforming
Business Continuity Management & Operational Resilience (BCR)				
Business Continuity Management and Operational Resilience	Control 1	BCR-01	Establish, document, approve, communicate, apply, evaluate and maintain business continuity management and operational resilience policies and procedures. Review and update the policies and procedures at least annually, or upon significant changes.	Conforming
Business Continuity Management and Operational Resilience	Control 2	BCR-02	Determine the impact of business disruptions and risks to establish criteria for developing business continuity and operational resilience strategies and capabilities. Review and update the risk assessment and impact analysis at least annually or upon significant changes.	Conforming
Business Continuity Management and Operational Resilience	Control 3	BCR-03	Establish strategies to reduce the impact of business disruptions, and improve resiliency and recovery from business disruptions.	Conforming
Business Continuity Management and Operational Resilience	Control 4	BCR-04	Establish, document, approve, communicate, apply, evaluate and maintain a business continuity plan based on the results of the operational resilience strategies and capabilities.	Conforming
Business Continuity Management and Operational Resilience	Control 5	BCR-05	Develop, identify, and acquire documentation, both internally and from external parties, that is relevant to support the business continuity and operational resilience plans. Make the documentation available to authorized	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.

			stakeholders and review at least annually or upon significant changes.	
Business Continuity Management and Operational Resilience	Control 6	BCR-06	Exercise and test business continuity and operational resilience plans at least annually or upon significant changes.	Conforming
Business Continuity Management and Operational Resilience	Control 7	BCR-07	Establish and maintain communication channels with all relevant stakeholders in the course of business continuity and resilience procedures.	Conforming
Business Continuity Management and Operational Resilience	Control 8	BCR-08	Periodically perform backups. Ensure the confidentiality, integrity and availability of the backup, and verify restoration from backup for resiliency.	Conforming
Business Continuity Management and Operational Resilience	Control 9	BCR-09	Establish, document, approve, communicate, apply, evaluate and maintain a disaster response plan to recover from natural and man-made disasters. Update the plan at least annually or upon significant changes.	Conforming
Business Continuity Management and Operational Resilience	Control 10	BCR-10	Exercise the disaster response plan annually or upon significant changes, including if possible, the participation of local emergency authorities.	Conforming
Business Continuity Management and Operational Resilience	Control 11	BCR-11	Supplement business-critical equipment with both locally redundant and geographically dispersed equipment located at a reasonable minimum distance in accordance with applicable industry standards.	Conforming
Change Control & Configuration Management (CCC)				
Change Control and Configuration Management	Control 1	CCC-01	Establish, document, approve, communicate, apply, evaluate and maintain policies and procedures for managing the risks associated with applying changes to assets owned, controlled or used by the organization. Review and update the policies and procedures at least annually, or upon significant changes.	Conforming
Change Control and Configuration Management	Control 2	CCC-02	Establish, maintain and implement a defined quality change control, approval and testing process incorporating baselines, testing, and release standards.	Conforming
Change Control and Configuration Management	Control 3	CCC-03	Implement a change management procedure to manage the risks associated with applying changes	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.

			to assets, owned, controlled or used by the organization.	
Change Control and Configuration Management	Control 4	CCC-04	Implement and enforce a procedure to authorize the addition, removal, update, and management of assets that are owned, controlled or used by the organization.	Conforming
Change Control and Configuration Management	Control 5	CCC-05	Include provisions limiting changes directly impacting service customers owned environments (tenants) to explicitly authorized requests within service level agreements.	Conforming
Change Control and Configuration Management	Control 6	CCC-06	Establish, document and implement change management and configuration baselines for all relevant authorized changes on organization assets. Review and update the baselines at least annually or upon significant changes.	Conforming
Change Control and Configuration Management	Control 7	CCC-07	Implement detection measures with proactive notification in case of changes deviating from the established baseline.	Conforming
Change Control and Configuration Management	Control 8	CCC-08	Implement a procedure for the management of exceptions, including emergencies, in the change and configuration process. Align the procedure with the requirements of GRC-04: Policy Exception Process.	Conforming
Change Control and Configuration Management	Control 9	CCC-09	Define and implement a process to proactively roll back changes to a previous known good state in case of errors or security concerns.	Conforming
Cryptography, Encryption & Key Management (CEK)				
Cryptography, Encryption & Key Management	Control 1	CEK-01	Establish, document, approve, communicate, apply, evaluate and maintain policies and procedures for Cryptography, Encryption and Key Management. Review and update the policies and procedures at least annually, or upon significant changes.	Conforming
Cryptography, Encryption & Key Management	Control 2	CEK-02	Define and implement cryptographic, encryption and key management roles and responsibilities.	Conforming
Cryptography, Encryption & Key Management	Control 3	CEK-03	Provide data protection at-rest, in-transit, and where applicable, in-use by using cryptographic libraries certified to approved standards.	Conforming
Cryptography, Encryption & Key Management	Control 4	CEK-04	Utilize encryption algorithms following industry standards for protecting data, based on the data classification and associated 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.

Cryptography, Encryption & Key Management	Control 5	CEK-05	Establish a standard change management procedure, to accommodate changes from internal and external sources, for review, approval, implementation and communication of cryptographic, encryption and key management technology changes.	Conforming
Cryptography, Encryption & Key Management	Control 6	CEK-06	Manage and adopt changes to cryptography-, encryption-, and key management-related systems (including policies and procedures) that fully account for downstream effects of proposed changes, including residual risk, cost, and benefits analysis.	Conforming
Cryptography, Encryption & Key Management	Control 7	CEK-07	Establish and maintain an encryption and key management risk program that includes provisions for risk assessment, risk treatment, risk context, monitoring, and feedback.	Conforming
Cryptography, Encryption & Key Management	Control 8	CEK-08	Service providers must provide the capability for service customers to manage their own data encryption keys.	Conforming
Cryptography, Encryption & Key Management	Control 9	CEK-09	Audit encryption and key management systems, policies, and processes with a frequency that is proportional to the risk exposure of the system with audit occurring preferably continuously but at least annually and upon any security event(s).	Conforming
Cryptography, Encryption & Key Management	Control 10	CEK-10	Generate Cryptographic keys using industry accepted cryptographic libraries specifying the algorithm strength and the random number generator used.	Conforming
Cryptography, Encryption & Key Management	Control 11	CEK-11	Manage cryptographic secret and private keys that are provisioned for a unique purpose.	Conforming
Cryptography, Encryption & Key Management	Control 12	CEK-12	Rotate cryptographic keys in accordance with the calculated cryptoperiod, which includes provisions for considering the risk of information disclosure and legal and regulatory requirements.	Conforming
Cryptography, Encryption & Key Management	Control 13	CEK-13	Define, implement and evaluate processes, procedures and technical measures to revoke and remove cryptographic keys prior to the end of its established cryptoperiod, when a key is compromised, or an entity is no longer part of the organization, which include provisions for legal and regulatory requirements.	Conforming
Cryptography, Encryption & Key Management	Control 14	CEK-14	Define, implement, and evaluate processes, procedures, and technical measures to securely destroy cryptographic keys when they are no longer needed, which include provisions for legal and regulatory requirements.	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.

Cryptography, Encryption & Key Management	Control 15	CEK-15	Define, implement and evaluate processes, procedures and technical measures to create keys in a pre-activated state when they have been generated but not authorized for use, which include provisions for legal and regulatory requirements.	Conforming
Cryptography, Encryption & Key Management	Control 16	CEK-16	Define, implement and evaluate processes, procedures and technical measures to monitor, review and approve key transitions from any state to/from suspension, which include provisions for legal and regulatory requirements.	Conforming
Cryptography, Encryption & Key Management	Control 17	CEK-17	Define, implement and evaluate processes, procedures and technical measures to deactivate keys at the time of their expiration date, which include provisions for legal and regulatory requirements.	Conforming
Cryptography, Encryption & Key Management	Control 18	CEK-18	Define, implement and evaluate processes, procedures and technical measures to manage archived keys in a secure repository requiring least privilege access, which include provisions for legal and regulatory requirements.	Conforming
Cryptography, Encryption & Key Management	Control 19	CEK-19	Define, implement and evaluate processes, procedures and technical measures to use compromised keys to encrypt information only in controlled circumstance, and thereafter exclusively for decrypting data and never for encrypting data, which include provisions for legal and regulatory requirements.	Conforming
Cryptography, Encryption & Key Management	Control 20	CEK-20	Define, implement and evaluate processes, procedures and technical measures to assess the risk to operational continuity versus the risk of the keying material and the information it protects being exposed if control of the keying material is lost, which include provisions for legal and regulatory requirements.	Conforming
Cryptography, Encryption & Key Management	Control 21	CEK-21	Define, implement and evaluate processes, procedures and technical measures in order for the key management system to track and report all cryptographic materials and changes in status, which include provisions for legal and regulatory requirements.	Conforming
Datacenter Security (DCS)				
Datacenter Security	Control 1	DCS-01	Establish, document, approve, communicate, apply, evaluate and maintain policies and procedures for physical and environmental security. Review and update the policies and procedures at least annually, or upon significant changes.	Excluded per CAIQ
Datacenter Security	Control 2	DCS-02	Establish, document, approve, communicate, apply, evaluate and maintain policies and procedures for the secure disposal of equipment used outside the organization's premises. If the equipment is	Excluded per CAIQ

© 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.

			not physically destroyed a data destruction procedure that renders recovery of information impossible must be applied. Review and update the policies and procedures at least annually, or upon significant changes.	
Datacenter Security	Control 3	DCS-03	Establish, document, approve, communicate, apply, evaluate and maintain policies and procedures for the relocation or transfer of hardware, software, or data/information to an offsite or alternate location. The relocation or transfer request requires the written or cryptographically verifiable authorization. Review and update the policies and procedures at least annually, or upon significant changes.	Excluded per CAIQ
Datacenter Security	Control 4	DCS-04	Establish, document, approve, communicate, apply, evaluate and maintain policies and procedures for maintaining a safe and secure working environment in offices, rooms, and facilities. Review and update the policies and procedures at least annually, or upon significant changes.	Excluded per CAIQ
Datacenter Security	Control 5	DCS-05	Establish, document, approve, communicate, apply, evaluate and maintain policies and procedures for the secure transportation of physical media. Review and update the policies and procedures at least annually, or upon significant changes.	Excluded per CAIQ
Datacenter Security	Control 6	DCS-06	Classify and document the physical, and logical assets (e.g., applications) based on the organizational business risk. Review and update the assets' classification at least annually, or upon significant changes.	Excluded per CAIQ
Datacenter Security	Control 7	DCS-07	Catalogue and track all relevant physical and logical assets located at all of the service provider's sites within a secured system. Review and update the catalogue at least annually or upon significant changes.	Excluded per CAIQ
Datacenter Security	Control 8	DCS-08	Design and implement physical security perimeters to safeguard personnel, data, and information systems.	Excluded per CAIQ
Datacenter Security	Control 9	DCS-09	Use equipment identification as a method for connection authentication.	Excluded per CAIQ
Datacenter Security	Control 10	DCS-10	Allow only authorized personnel access to secure areas, with all ingress and egress points restricted, documented, and monitored by physical access control mechanisms. Retain access control records on a periodic basis as deemed appropriate by the organization.	Excluded per CAIQ
Datacenter Security	Control 11	DCS-11	Implement, maintain, and operate datacenter surveillance systems at the external perimeter and at all the ingress and egress points to detect unauthorized ingress and egress attempts.	Excluded per CAIQ

© 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.

Datacenter Security	Control 12	DCS-12	Train datacenter personnel to safely manage adverse events, including but not limited to unauthorized ingress and egress attempts.	Excluded per CAIQ
Datacenter Security	Control 13	DCS-13	Define, implement and evaluate processes, procedures and technical measures that ensure a risk-based protection of power and telecommunication cables from a threat of interception, interference or damage at all facilities, offices and rooms.	Excluded per CAIQ
Datacenter Security	Control 14	DCS-14	Implement and maintain data center environmental control systems that monitor, maintain and test for continual effectiveness the temperature and humidity conditions within accepted industry standards.	Excluded per CAIQ
Datacenter Security	Control 15	DCS-15	Secure, monitor, maintain, and test utilities services for continual effectiveness at planned intervals.	Excluded per CAIQ
Datacenter Security	Control 16	DCS-16	Keep business-critical equipment away from locations subject to high probability for environmental risk events.	Excluded per CAIQ
Datacenter Security	Control 17	DCS-17	Establish, monitor and report datacenter security metrics to secure data center assets and services.	Excluded per CAIQ
Datacenter Security	Control 18	DCS-18	Define, implement and evaluate processes, procedures and technical measures to ensure continuous operations.	Excluded per CAIQ
Data Security & Privacy Lifecycle Management (DSP)				
Data Security and Privacy Lifecycle Management	Control 1	DSP-01	Establish, document, approve, communicate, apply, evaluate and maintain policies and procedures for the preparation, classification, protection and handling of data throughout its lifecycle, and according to all applicable laws and regulations, standards, and risk level. Review and update the policies and procedures at least annually, or upon significant changes.	Conforming
Data Security and Privacy Lifecycle Management	Control 2	DSP-02	Apply industry accepted methods for the secure disposal of data from storage media such that data is not recoverable by any forensic means.	Conforming
Data Security and Privacy Lifecycle Management	Control 3	DSP-03	Create and maintain a data inventory, at least for any sensitive, regulated and personal data. Review and update the inventory at least annually or upon significant changes.	Conforming
Data Security and Privacy Lifecycle Management	Control 4	DSP-04	Classify data according to its type, criticality and sensitivity level.	Conforming
Data Security and Privacy Lifecycle Management	Control 5	DSP-05	Create data flow documentation to identify what data is processed, stored or transmitted where. Review data flow documentation at defined intervals, at least annually, or upon significant changes.	Conforming
Data Security and Privacy Lifecycle Management	Control 6	DSP-06	Document ownership and stewardship of all relevant documented personal and sensitive data. Perform review at least annually.	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.

Data Security and Privacy Lifecycle Management	Control 7	DSP-07	Develop systems, products, and business practices based upon a principle of security by design and industry best practices.	Conforming
Data Security and Privacy Lifecycle Management	Control 8	DSP-08	Develop systems, products, and business practices based upon a principle of privacy by design and industry best practices. Ensure that systems' privacy settings are configured by default, according to all applicable laws and regulations.	Conforming
Data Security and Privacy Lifecycle Management	Control 9	DSP-09	Conduct a Data Protection Impact Assessment (DPIA) to evaluate the origin, nature, particularity and severity of the risks upon the processing of personal data, according to any applicable laws, regulations and industry best practices.	Conforming
Data Security and Privacy Lifecycle Management	Control 10	DSP-10	Define, implement and evaluate processes, procedures and technical measures that ensure any transfer of personal or sensitive data is protected from unauthorized access and only processed within scope as permitted by the respective laws and regulations.	Conforming
Data Security and Privacy Lifecycle Management	Control 11	DSP-11	Define and implement, processes, procedures and technical measures to enable data subjects to request access to, modification, or deletion of their personal data, according to any applicable laws and regulations.	Conforming
Data Security and Privacy Lifecycle Management	Control 12	DSP-12	Define, implement and evaluate processes, procedures and technical measures to ensure that personal data is processed according to any applicable laws and regulations and for the purposes declared to the data subject.	Conforming
Data Security and Privacy Lifecycle Management	Control 13	DSP-13	Define, implement and evaluate processes, procedures and technical measures for the transfer and sub-processing of personal data within the service supply chain, according to any applicable laws and regulations.	Conforming
Data Security and Privacy Lifecycle Management	Control 14	DSP-14	Define, implement and evaluate processes, procedures and technical measures to disclose the details of any personal or sensitive data access by sub-processors to the data owner prior to initiation of that processing.	Conforming
Data Security and Privacy Lifecycle Management	Control 15	DSP-15	Obtain authorization from data owners, and manage associated risk before replicating or using production data in non-production environments.	Conforming
Data Security and Privacy Lifecycle Management	Control 16	DSP-16	Data retention, archiving and deletion is managed in accordance with business requirements, applicable laws and regulations.	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.

Data Security and Privacy Lifecycle Management	Control 17	DSP-17	Define and implement, processes, procedures and technical measures to protect sensitive data throughout it's lifecycle.	Conforming
Data Security and Privacy Lifecycle Management	Control 18	DSP-18	The service provider must implement and describe to service customers the procedure to manage and respond to requests for disclosure of Personal Data by Law Enforcement Authorities according to applicable laws and regulations	Conforming
Data Security and Privacy Lifecycle Management	Control 19	DSP-19	Define and implement, processes, procedures and technical measures to specify and document the physical locations of data, including any locations in which data is processed or backed up.	Conforming
Governance, Risk & Compliance (GRC)				
Governance, Risk and Compliance	Control 1	GRC-01	Establish, document, approve, communicate, apply, evaluate and maintain policies and procedures for an information governance program, which is sponsored by the leadership of the organization. Review and update the policies and procedures at least annually, or upon significant changes.	Conforming
Governance, Risk and Compliance	Control 2	GRC-02	Establish and maintain a formal, documented, and leadership-sponsored Enterprise Risk Management (ERM) program that includes policies and procedures for identification, evaluation, ownership, treatment, and acceptance of risks.	Conforming
Governance, Risk and Compliance	Control 3	GRC-03	Review all relevant organizational policies and associated procedures at least annually or when a substantial change occurs within the organization.	Conforming
Governance, Risk and Compliance	Control 4	GRC-04	Establish and follow an approved exception process as mandated by the governance program whenever a deviation from an established policy occurs.	Conforming
Governance, Risk and Compliance	Control 5	GRC-05	Develop and implement an Information Security Program, which includes programs for all the relevant domains of the CCM.	Conforming
Governance, Risk and Compliance	Control 6	GRC-06	Define and document roles and responsibilities for planning, implementing, operating, assessing, and improving governance programs.	Conforming
Governance, Risk and Compliance	Control 7	GRC-07	Identify and document all relevant standards, regulations, legal/contractual, and statutory requirements, which are applicable to your organization. Review at least annually or upon significant changes.	Conforming
Governance, Risk and Compliance	Control 8	GRC-08	Establish and maintain contact with cloud-related special interest groups and other relevant entities in line with business context.	Conforming
Human Resources (HRS)				
Human Resources	Control 1	HRS-01	Establish, document, approve, communicate, apply, evaluate and maintain policies and procedures for background	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.

			verification of all new employees (including but not limited to remote employees, contractors, and third parties) according to local laws, regulations, ethics, and contractual constraints and proportional to the data classification to be accessed, the business requirements, and acceptable risk. Review and update the policies and procedures at least annually, or upon significant changes.	
Human Resources	Control 2	HRS-02	Establish, document, approve, communicate, apply, evaluate and maintain policies and procedures for defining allowances and conditions for the acceptable use of organizationally-owned or managed assets. Review and update the policies and procedures at least annually, or upon significant changes.	Conforming
Human Resources	Control 3	HRS-03	Establish, document, approve, communicate, apply, evaluate and maintain policies and procedures that require unattended workspaces to not have openly visible confidential data. Review and update the policies and procedures at least annually, or upon significant changes.	Conforming
Human Resources	Control 4	HRS-04	Establish, document, approve, communicate, apply, evaluate and maintain policies and procedures to protect information accessed, processed or stored at remote sites and locations. Review and update the policies and procedures at least annually, or upon significant changes.	Conforming
Human Resources	Control 5	HRS-05	Establish and document procedures for the return of organization-owned assets by terminated employees, contractors and third parties.	Conforming
Human Resources	Control 6	HRS-06	Establish, document, and communicate to all relevant personnel the procedures outlining the roles and responsibilities concerning changes in employment.	Conforming
Human Resources	Control 7	HRS-07	Employees sign the employee agreement prior to being granted access to organizational information systems, resources and assets.	Conforming
Human Resources	Control 8	HRS-08	The organization includes within the employment agreements provisions and/or terms for adherence to established information governance and security policies.	Conforming
Human Resources	Control 9	HRS-09	Establish, document and communicate roles and responsibilities of employees, as they relate to information assets' security and privacy.	Conforming
Human Resources	Control 10	HRS-10	Identify, document, and review, at planned intervals, requirements for non-disclosure/confidentiality agreements reflecting the organization's needs for the protection of data and operational details.	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.

Human Resources	Control 11	HRS-11	Establish, document, approve, communicate, apply, evaluate and maintain a security awareness training program for all employees of the organization and provide regular training updates.	Conforming
Human Resources	Control 12	HRS-12	Provide employees with access to sensitive organizational and personal data with appropriate security awareness training and regular updates in organizational procedures, processes, and policies relating to their professional function relative to the organization.	Conforming
Human Resources	Control 13	HRS-13	Make employees aware of their roles and responsibilities for maintaining awareness and compliance with established policies and procedures and applicable legal, statutory, or regulatory compliance obligations.	Conforming
Identity & Access Management (IAM)				
Identity & Access Management	Control 1	IAM-01	Establish, document, approve, communicate, implement, apply, evaluate, and maintain policies and procedures for identity and access management. Review and update the policies and procedures at least annually, or upon significant changes.	Conforming
Identity & Access Management	Control 2	IAM-02	Establish, document, approve, communicate, implement, apply, evaluate, and maintain policies and procedures for the management of authentication credentials, including passwords. Review and update the policies and procedures at least annually, or upon significant changes.	Conforming
Identity & Access Management	Control 3	IAM-03	Manage, store, and regularly review the inventory of identities, and monitor their level of access.	Conforming
Identity & Access Management	Control 4	IAM-04	Employ the separation of duties principle when implementing information system access.	Conforming
Identity & Access Management	Control 5	IAM-05	Employ the least privilege principle when implementing information system access.	Conforming
Identity & Access Management	Control 6	IAM-06	Define and implement an identity access provisioning process which authorizes, records, and communicates access changes to data and assets.	Conforming
Identity & Access Management	Control 7	IAM-07	De-provision or modify identity access in a timely manner.	Conforming
Identity & Access Management	Control 8	IAM-08	Review and revalidate identity access for least privilege and separation of duties with a frequency that is commensurate with organizational risk tolerance, and at least annually or upon significant changes.	Conforming
Identity & Access Management	Control 9	IAM-09	Define, implement and evaluate processes, procedures and technical measures for the segregation of privileged access roles.	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.

Identity & Access Management	Control 10	IAM-10	Define and implement an access process to ensure privileged access roles and rights are granted for a time limited period, and implement procedures to prevent the accumulation of segregated privileged access.	Conforming
Identity & Access Management	Control 11	IAM-11	Define, implement and evaluate processes and procedures for service customers to participate, where applicable, in the granting of access for agreed, high risk (as defined by the organizational risk assessment) privileged access roles.	Conforming
Identity & Access Management	Control 12	IAM-12	Define, implement and evaluate processes, procedures and technical measures that ensure identities' activities are identifiable through uniquely associated IDs.	Conforming
Identity & Access Management	Control 13	IAM-13	Define, implement and evaluate processes, procedures and technical measures for authenticating access to systems, application and data assets, including multifactor authentication for at least privileged user and sensitive data access. Adopt digital certificates or alternatives which achieve an equivalent level of security for system identities.	Conforming
Identity & Access Management	Control 14	IAM-14	Define, implement and evaluate processes, procedures and technical measures for the secure management of authentication credentials, including passwords.	Conforming
Identity & Access Management	Control 15	IAM-15	Define, implement and evaluate processes, procedures and technical measures to verify access to data and system functions is authorized.	Conforming
Interoperability & Portability (IPY)				
Interoperability & Portability	Control 1	IPY-01	Establish, document, approve, communicate, apply, evaluate and maintain policies and procedures for interoperability and portability including requirements for: a. Communications between application interfaces b. Information processing interoperability c. Application development portability d. Information/Data exchange, usage, portability, integrity, and persistence Review and update the policies and procedures at least annually, or upon significant changes.	Conforming
Interoperability & Portability	Control 2	IPY-02	Provide application interface(s) to service customers so that they programmatically retrieve their data to enable interoperability and portability.	Conforming
Interoperability & Portability	Control 3	IPY-03	Implement cryptographically secure network protocols for the management, import and export of data, according to industry standards.	Conforming
Interoperability & Portability	Control 4	IPY-04	Agreements must include provisions specifying service customers' access to data upon contract termination and will include: a. Data format	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.

			b. Length of time the data will be stored c. Scope of the data retained and made available to the service customers d. Data deletion policy	
Infrastructure Security (I&S)				
Infrastructure Security	Control 1	I&S-01	Establish, document, approve, communicate, apply, evaluate and maintain policies and procedures for infrastructure and virtualization security. Review and update the policies and procedures at least annually, or upon significant changes.	Conforming
Infrastructure Security	Control 2	I&S-02	Plan and monitor the availability, quality, and adequate capacity of resources in order to deliver the required system performance as determined by the business.	Conforming
Infrastructure Security	Control 3	I&S-03	Monitor, encrypt and restrict communications between environments, services, and applications to only authenticated and authorized connections, as justified by the business. Review these configurations at least annually, and support them by a documented justification of all allowed services, protocols, ports, and compensating controls.	Conforming
Infrastructure Security	Control 4	I&S-04	Harden host and guest OS, hypervisor or infrastructure control plane according to their respective best practices, and supported by technical controls, as part of a security baseline.	Conforming
Infrastructure Security	Control 5	I&S-05	Separate production and non-production environments to reduce the risk of sensitive production data being used in non-production environments. Production data is sanitized or protected before any authorized non-production use.	Conforming
Infrastructure Security	Control 6	I&S-06	Design, develop, deploy and configure applications and infrastructures such that service customer (tenant) access is appropriately segmented and segregated, monitored and restricted.	Conforming
Infrastructure Security	Control 7	I&S-07	Use secure and encrypted communication channels when migrating servers, services, applications, or data to cloud environments. Such channels must include only up-to-date and approved protocols.	Conforming
Infrastructure Security	Control 8	I&S-08	Identify and document high-risk environments based on data sensitivity, threat exposure, and business impact.	Conforming
Infrastructure Security	Control 9	I&S-09	Define, implement and evaluate processes, procedures and defense-in-depth techniques for protection, detection, and timely response to network-based attacks.	Conforming
Logging & Monitoring (LOG)				
Logging and Monitoring	Control 1	LOG-01	Establish, document, approve, communicate, apply, evaluate and maintain policies and procedures for logging and monitoring. Review and update the policies and procedures at least annually, or upon significant changes.	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.

Logging and Monitoring	Control 2	LOG-02	Define, implement and evaluate processes, procedures and technical measures to ensure the security and retention of audit logs.	Conforming
Logging and Monitoring	Control 3	LOG-03	Identify and monitor security-related events within applications and the underlying infrastructure. Define and implement a system to generate alerts to responsible stakeholders based on such events and corresponding metrics.	Conforming
Logging and Monitoring	Control 4	LOG-04	Restrict audit log access to authorized identities and maintain records of that access.	Conforming
Logging and Monitoring	Control 5	LOG-05	Implement and maintain capabilities to correlate and monitor security audit logs for the detection of suspicious or anomalous activity that deviates from typical or expected patterns. Establish and follow a defined process to review and take appropriate and timely actions on detected anomalies.	Conforming
Logging and Monitoring	Control 6	LOG-06	Use a reliable time source across all relevant information processing systems.	Conforming
Logging and Monitoring	Control 7	LOG-07	Establish, document and implement which information meta/data system events should be logged. Review and update the scope at least annually or whenever there is a change in the threat environment, and as per relevant regulatory requirements.	Conforming
Logging and Monitoring	Control 8	LOG-08	Define, implement and evaluate technical measures for service customers to detect and scrub or tokenize sensitive data from logs to prevent unauthorized exposure, as per applicable laws and regulations.	Conforming
Logging and Monitoring	Control 9	LOG-09	Generate audit records containing relevant security information.	Conforming
Logging and Monitoring	Control 10	LOG-10	Protect audit records from unauthorized access, modification, and deletion.	Conforming
Logging and Monitoring	Control 11	LOG-11	Establish and maintain a monitoring and internal reporting capability over the operations of cryptographic, encryption and key management policies, processes, procedures, and controls.	Conforming
Logging and Monitoring	Control 12	LOG-12	Log and monitor key lifecycle management events to enable auditing and reporting on usage of cryptographic keys.	Conforming
Logging and Monitoring	Control 13	LOG-13	Monitor and log physical access using an auditable access control system.	Conforming
Logging and Monitoring	Control 14	LOG-14	Define, implement and evaluate processes, procedures and technical measures for the reporting of anomalies and failures of the monitoring system and provide immediate notification to the accountable party.	Conforming
Security Incident Management, E-Discovery & Cloud Forensics (SEF)				

© 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.

Security Incident Management, E-Discovery, & Cloud Forensics	Control 1	SEF-01	Establish, document, approve, communicate, apply, evaluate and maintain policies and procedures for Security Incident Management, E-Discovery, and Cloud Forensics. Review and update the policies and procedures at least annually, or upon significant changes.	Conforming
Security Incident Management, E-Discovery, & Cloud Forensics	Control 2	SEF-02	Establish, document, approve, communicate, apply, evaluate and maintain policies and procedures for the timely management of security incidents. Review and update the policies and procedures at least annually, or upon significant changes.	Conforming
Security Incident Management, E-Discovery, & Cloud Forensics	Control 3	SEF-03	Establish, document, approve, communicate, apply, evaluate and maintain a security incident response plan, which includes but is not limited to: a communication strategy for notifying relevant internal departments, impacted service customers, and other business critical relationships (such as supply-chain) that may be impacted.	Conforming
Security Incident Management, E-Discovery, & Cloud Forensics	Control 4	SEF-04	Exercise the incident response plans at planned intervals or upon significant changes.	Conforming
Security Incident Management, E-Discovery, & Cloud Forensics	Control 5	SEF-05	Establish, monitor and report information security incident metrics.	Conforming
Security Incident Management, E-Discovery, & Cloud Forensics	Control 6	SEF-06	Define, implement and evaluate processes, procedures and technical measures supporting business processes to triage security-related events.	Conforming
Security Incident Management, E-Discovery, & Cloud Forensics	Control 7	SEF-07	Define, implement and evaluate processes, procedures and technical measures for timely and effective response to security incidents in accordance with incident categories and severity levels. Review, update, and test processes and procedures at least annually.	Conforming
Security Incident Management, E-Discovery, & Cloud Forensics	Control 8	SEF-08	Define and implement processes, procedures and technical measures for security breach notifications. Report material security breaches including any relevant supply chain breaches, as per applicable SLAs, laws and regulations.	Conforming
Security Incident Management, E-Discovery, & Cloud Forensics	Control 9	SEF-09	Establish and maintain a secure repository of security incident records. Regularly review the incident records to identify patterns, root causes, and systemic vulnerabilities, and implement relevant corrective measures.	Conforming
Security Incident Management, E-Discovery, & Cloud Forensics	Control 10	SEF-10	Maintain points of contact for applicable regulation authorities, national and local law enforcement, and other legal jurisdictional authorities. Review and update the points of contact at least annually.	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.

Supply Chain Management, Transparency & Accountability (STA)				
Supply Chain Management, Transparency, and Accountability	Control 1	STA-01	Establish, document, approve, communicate, apply, evaluate, and maintain policies and procedures for supply chain risk management. Review and update the policies and procedures at least annually, or upon significant changes.	Conforming
Supply Chain Management, Transparency, and Accountability	Control 2	STA-02	Establish, document, approve, communicate, apply, evaluate and maintain policies and procedures for the application of the Shared Security Responsibility Model (SSRM) within the organization. Review and update the policies and procedures at least annually, or upon significant changes.	Conforming
Supply Chain Management, Transparency, and Accountability	Control 3	STA-03	Apply, document, implement and manage the SSRM throughout the supply chain.	Conforming
Supply Chain Management, Transparency, and Accountability	Control 4	STA-04	Provide SSRM Guidance to the service customers detailing information about the SSRM applicability throughout the supply chain.	Conforming
Supply Chain Management, Transparency, and Accountability	Control 5	STA-05	Delineate the shared ownership and applicability of all CSA CCM controls according to the SSRM.	Conforming
Supply Chain Management, Transparency, and Accountability	Control 6	STA-06	Review and validate the SSRM documentation.	Conforming
Supply Chain Management, Transparency, and Accountability	Control 7	STA-07	Implement, operate, and audit or assess the portions of the SSRM which the organization is responsible for.	Conforming
Supply Chain Management, Transparency, and Accountability	Control 8	STA-08	Develop and maintain an inventory of all supply chain relationships.	Conforming
Supply Chain Management, Transparency, and Accountability	Control 9	STA-09	Define, implement, and enforce a process for establishing a Bill of Material for the service supply chain. Review and update the Bill of Material at least annually or upon significant changes.	Conforming
Supply Chain Management, Transparency, and Accountability	Control 10	STA-10	Periodically review risk factors associated with supply chain relationships.	Conforming
Supply Chain Management, Transparency,	Control 11	STA-11	Establish, document, approve, communicate, apply, evaluate, and maintain policies and procedures for supply chain risk management. Review and update the policies	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.

and Accountability			and procedures at least annually, or upon significant changes.	
Supply Chain Management, Transparency, and Accountability	Control 12	STA-12	Establish, document, approve, communicate, apply, evaluate and maintain policies and procedures for the application of the Shared Security Responsibility Model (SSRM) within the organization. Review and update the policies and procedures at least annually, or upon significant changes.	Conforming
Supply Chain Management, Transparency, and Accountability	Control 13	STA-13	Apply, document, implement and manage the SSRM throughout the supply chain.	Conforming
Supply Chain Management, Transparency, and Accountability	Control 14	STA-14	Provide SSRM Guidance to the service customers detailing information about the SSRM applicability throughout the supply chain.	Conforming
Supply Chain Management, Transparency, and Accountability	Control 15	STA-15	Delineate the shared ownership and applicability of all CSA CCM controls according to the SSRM.	Conforming
Supply Chain Management, Transparency, and Accountability	Control 16	STA-16	Review and validate the SSRM documentation.	Conforming
Threat & Vulnerability Management (TVM)				
Threat & Vulnerability Management	Control 1	TVM-01	Establish, document, approve, communicate, apply, evaluate and maintain policies and procedures to identify, report and prioritize the remediation of vulnerabilities and threats, in order to protect systems against vulnerability exploitation. Review and update the policies and procedures at least annually, or upon significant changes.	Conforming
Threat & Vulnerability Management	Control 2	TVM-02	Establish, document, approve, communicate, apply, evaluate and maintain policies and procedures to protect against malware and malicious instructions. Review and update the policies and procedures at least annually, or upon significant changes.	Conforming
Threat & Vulnerability Management	Control 3	TVM-03	Define, implement and evaluate processes, procedures and technical measures for the detection of vulnerabilities on organizationally managed assets at least monthly.	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.

Threat & Vulnerability Management	Control 4	TVM-04	Define, implement, and evaluate a threat analysis process and procedures to identify, assess and review the threat landscape for cloud systems. Build threat models according to industry best practices to inform the risk mitigation strategy.	Conforming
Threat & Vulnerability Management	Control 5	TVM-05	Define, implement and evaluate processes, procedures and technical measures to update detection tools, threat signatures, and indicators of compromise on a weekly, or more frequent basis.	Conforming
Threat & Vulnerability Management	Control 6	TVM-06	Define, implement and evaluate processes, procedures and technical measures to identify updates for applications which use third party or open source libraries according to the organization's vulnerability management policy.	Conforming
Threat & Vulnerability Management	Control 7	TVM-07	Define, implement and evaluate processes, procedures and technical measures for the periodic performance of penetration testing by independent third parties.	Conforming
Threat & Vulnerability Management	Control 8	TVM-08	Define, implement and evaluate processes, procedures and technical measures based on identified risks to support scheduled and emergency responses to vulnerability identification.	Conforming
Threat & Vulnerability Management	Control 9	TVM-09	Use a risk-based method for effective prioritization of vulnerability remediation using an industry recognized framework.	Conforming
Threat & Vulnerability Management	Control 10	TVM-10	Use a risk-based method for the prioritization and mitigation of threats, leveraging an industry-recognized framework to guide threat decision-making and protection measures.	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.

Threat & Vulnerability Management	Control 11	TVM-11	Define and implement a process for tracking and reporting vulnerability identification and remediation activities that includes stakeholder notification.	Conforming
Threat & Vulnerability Management	Control 12	TVM-12	Establish, monitor and report metrics for vulnerability identification and remediation at defined intervals.	Conforming
Universal Endpoint Management (UEM)				
Universal Endpoint Management	Control 1	UEM-01	Establish, document, approve, communicate, apply, evaluate and maintain policies and procedures for all endpoints. Review and update the policies and procedures at least annually, or upon significant changes.	Conforming
Universal Endpoint Management	Control 2	UEM-02	Define, document, apply and evaluate a list of approved services, applications and sources of applications (stores) acceptable for use by endpoints when accessing or storing organization-managed data.	Conforming
Universal Endpoint Management	Control 3	UEM-03	Define and implement a process for the validation of the endpoint device's compatibility with operating systems and applications.	Conforming
Universal Endpoint Management	Control 4	UEM-04	Maintain an inventory of all endpoints used to store, access and process company data.	Conforming
Universal Endpoint Management	Control 5	UEM-05	Define, implement and evaluate processes, procedures and technical measures to enforce policies and controls for all endpoints permitted to access systems and/or store, transmit, or process organizational data.	Conforming
Universal Endpoint Management	Control 6	UEM-06	Configure all relevant interactive-use endpoints to require an automatic lock screen.	Conforming
Universal Endpoint Management	Control 7	UEM-07	Manage changes to endpoint operating systems, patch levels, and/or applications through the company's change management processes.	Conforming
Universal Endpoint Management	Control 8	UEM-08	Protect information from unauthorized disclosure on managed endpoint devices with storage encryption.	Conforming
Universal Endpoint Management	Control 9	UEM-09	Configure managed endpoints with anti-malware detection and prevention technology and services.	Conforming
Universal Endpoint Management	Control 10	UEM-10	Configure managed endpoints with properly configured software firewalls.	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.

Universal Endpoint Management	Control 11	UEM-11	Configure managed endpoints with Data Loss Prevention (DLP) technologies and rules in accordance with a risk assessment.	Conforming
Universal Endpoint Management	Control 12	UEM-12	Enable remote geo-location capabilities for all managed mobile endpoints, according to all applicable laws and regulations.	Conforming
Universal Endpoint Management	Control 13	UEM-13	Define, implement and evaluate processes, procedures and technical measures to enable the deletion of company data remotely on managed endpoint devices.	Conforming
Universal Endpoint Management	Control 14	UEM-14	Define, implement and evaluate processes, procedures and technical and/or contractual measures to maintain proper security of third-party endpoints with access to organizational assets.	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

No nonconformities identified in the current certification cycle.

© 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.