Statement of Applicability ISO 42001:2023

Organisation: VamiSec GmbH
Version: 1.0
Approval status: To be approved in management review

For internal use (do not print this part for your official statement of applicability)

Nr.	Chapter	Topic	Control	Applicable to our organisation	Implemented in our organisation	Implementation		Control owner	Control type	InfoSec properties			CyberSec concepts	Operational capabilities	Security domains			
						How implemented	Further Evidences for implementation			Confidentiality	Integrity	Availability			Governance and Ecosystem	Protection	Defence	Resilience
				(Yes/No)	(Yes/No)													
A.2.2	Policies related to AI	AI policy	The organization shall document a policy for the development or use of AI systems.	Yes	Yes	The AI Policy was created in alignment with organizational objectives, approved by senior management, and published in the internal policy portal. It defines principles for AI development, integration, and responsible use. The policy is reviewed annually.	Final approved AI Policy (PDF) Cross-reference matrix aligning AI Policy with ISMS, and HR policies Version history showing past reviews	AI Officer	Preventive	X	X	X	Identify	Governance	X	X		
A.2.3	Policies related to AI	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.	Yes	Yes	A policy mapping exercise was conducted to identify intersections between AI objectives and existing policies (e.g. ISMS, Data Protection). Cross-references were documented, and relevant policies were updated to reflect AI-specific considerations where applicable. Ownership for policy alignment is defined.	AI Policy Mapping Matrix (shows which policies are linked) - Meeting minutes from policy alignment workshops - Updated versions of affected policies with AI sections - Internal memo assigning responsibility for policy coordination - Review logs showing policy alignment checked annually	AI Officer	Preventive	X	X		Identify	Governance	X			X
A.2.4	Policies related to AI	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.	Yes	Yes	A review schedule is set for the AI Policy (annually, or upon regulatory or operational change). A designated AI Governance Committee is assigned responsibility. Reviews are conducted based on changes in legislation, strategy, or technology. Updates are managed.	Documented review schedule (intranet) - Policy review log - Updated policy version with change log - Email or system-based acknowledgment receipts from staff	AI Officer	Preventive	X	X	X	Protect	Governance	X			
A.3.2	Internal organization	AI roles and responsibilities	Roles and responsibilities for AI shall be defined and allocated according to the needs of the organization.	Yes	Yes	All AI-related roles for development, deployment, and monitoring are defined in the AI Policy. Specific responsibilities are documented in the RACI Matrix and embedded in job descriptions. The AI Governance Committee ensures roles are kept up to date. Organizational charts and internal communications were updated to reflect role assignments.	Approved AI Policy section: "Roles and Responsibilities" - RACI Matrix for AI processes - Job descriptions with AI responsibilities (e.g., Data Scientist, AI Officer) - Updated organizational chart - Internal email or Teams announcement of roles	AI Officer	Preventive	X	X	X	Identify	Identity and access management	X			
A.3.3	Internal organization	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.	Yes	Yes	An AI Incident Reporting Procedure was created, including channels (email, webform) for raising concerns about the organization's role in AI systems. Responsibilities for intake, review, and resolution are clearly defined. The process is communicated through onboarding, awareness sessions, and internal communication channels. Reports are logged and handled promptly to ensure transparency and accountability.	AI Incident Management Procedure document Screenshot or URL of internal reporting form/email Training slides or onboarding materials mentioning reporting Record of reported issues (anonymized) Communication email or poster rollout (internal campaign)	AI Officer	Detective	X	X	X	Protect Respond Recover	Identity and access management	X		X	X
A.4.2	Resources for AI systems	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.	Yes	Yes	An AI Resource Inventory was created to list all relevant resources (technical, human, data, infrastructure) across the AI system life cycle: development, validation, deployment, operation, and retirement. Resources are categorized by type (e.g., model, dataset, compute, personnel) and usage. The inventory is reviewed quarterly and updated after significant changes (e.g., system upgrades, staffing shifts).	-AI Resource Inventory spreadsheet or tool export - Categorization schema with examples (data, models, infrastructure) -Version history/log of inventory updates - Meeting notes from inventory review sessions - Approval log for initial inventory creation	AI Officer	Preventive Corrective	X	X	X	Protect Recover	Asset management			X	
A.4.3	Resources for AI systems	Data resources	Information relating to information security threats shall be collected and analysed to produce threat intelligence.	Yes	Yes	The organization subscribes to external and internal threat intelligence sources (e.g. governmental CERTs, AI-specific vendor feeds, open-source communities). The security team collects, evaluates, and categorizes threats relevant to AI systems, including model misuse, data poisoning, and adversarial attacks. Threat intelligence is integrated into the AI risk register and shared with relevant technical teams to adapt controls or retrain models as necessary.	AI-specific threat feed subscription list (MITRE ATLAS) threat intel reports (internal monthly summaries) Entries in the AI risk register referring to threat trends Change logs in ML pipelines or security controls based on threat data SOC process document describing how threat intel is handled	AI Officer	Preventive Detective	X	X	X	Identify Detect	Threat intelligence		X	X	X
A.4.4	Resources for AI systems	Tooling resources	As part of resource identification, the organization shall document information about the tooling resources utilized for the AI system.	Yes	Yes	An AI Tooling Inventory was created to record all tools used in the AI life cycle, including development platforms, libraries, MLOps pipelines, and frameworks. The inventory includes tool name, version, license, configuration, usage purpose, and owner. The record is updated regularly when tools are introduced or modified, and linked to compliance and procurement processes.	AI Tooling Inventory spreadsheet or system export Tool configuration documentation (e.g. Terraform, Ansible, YAML) Version and license tracking table Change log showing tool additions and removals Review logs confirming quarterly updates	AI Officer	Preventive	X	X	X	Identify Protect	Asset management	X	X		
A.4.5	Resources for AI systems	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.	Yes	Yes	A dedicated inventory of computing resources (on-prem servers, cloud environments, GPUs, edge devices) used for AI systems has been created. The inventory includes specifications, performance metrics, capacity benchmarks, and ownership. Monitoring dashboards are used to assess real-time usage and detect bottlenecks. Updates are triggered by changes in infrastructure, usage patterns, or performance thresholds.	AI Computing Resource Inventory (Excel, CMDB export) Cloud dashboard screenshots (AWS, Azure, GCP usage reports) Resource monitoring logs (e.g., Prometheus, Datadog) Infrastructure-as-Code (IaC) definitions (Terraform, Ansible) Internal guidelines on resource scaling and allocation	AI Officer	Preventive	X	X	X	Identify	Asset management	X	X		
A.4.6	Resources for AI systems	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.	Yes	Yes	The organization maintains an up-to-date inventory of personnel involved in AI-related activities. Each role is described with its associated responsibilities and required competencies. A Competency Matrix is used to evaluate existing skills against defined requirements across the AI system life cycle. Identified gaps are addressed through targeted training or recruitment. This documentation is reviewed annually or as roles change.	Inventory of AI personnel (HR export, role registry) Competency Matrix (skills vs. roles mapping) Role descriptions with AI-related responsibilities Training plan addressing gaps in AI-related knowledge Recruitment strategy or job postings linked to competency needs	AI Officer	Preventive	X	X	X	Protect	Human resource security	X	X		
A.5.2	Assessing impacts of AI systems	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.	Yes	Yes	An AI Risk Assessment Policy has been created to define how the impacts of AI systems on individuals, groups, and society are identified, assessed, and documented. The process includes criteria such as fairness, discrimination, autonomy, and social consequences. Each AI project must conduct an assessment at the design phase, with updates during key lifecycle transitions. Results are reviewed by the AI Governance Committee.	AI Risk Assessment Policy document Completed AI Impact Assessment templates (e.g. for past projects) Review logs by AI Governance Committee Change log or lifecycle checklist showing reassessment points Awareness/training material for AI risk assessment	AI Officer	Preventive	X	X	X	Protect	Risk management		X		

A.5.3	Assessing impacts of AI systems	Documentation of AI system im pact assessments	The organization shall document the results of AI system impact assessments and retain results for a defined peri od.	Yes	Yes	The results of AI impact assessments are documented using a standardized template that includes identified risks, affected stakeholders, and mitigation actions. Each assessment is approved by the responsible role noted in the AI RACI Matrix. Documents are stored in a controlled location with restricted access and retained for a period of five years (or longer, if required by law or contractual obligations).	Completed AI Impact Assessment reports (PDF/SharePoint) Retention schedule documented in Records Management Policy Access-controlled folder or document management system log AI RACI Matrix showing responsible roles Internal audit trail confirming availability of past assessments	AI Officer	Preventive	X	X	X	Identify	Risk management			X	
A.5.4	Assessing impacts of AI systems	Assessing AI system impact on in dividuals or groups of individuals	The organization shall assess and document the potential impacts of AI systems to individuals or groups of individu als throughout the system's life cycle.	Yes	Yes	The AI Impact Assessment template is used to evaluate potential effects on individuals or groups at each life cycle phase of the AI system. This includes social, ethical, privacy, and fairness considerations. Assessments are conducted during design and reviewed periodically or after major system changes. If significant impacts are identified, they are logged in the risk register and monitored.	Completed AI Impact Assessment forms Impact Assessment Template with criteria Schedule or calendar for reassessment cycles Risk Register entries derived from impact assessments Communication or training material for staff conducting assessments	AI Officer	Preventive	X	X	X	Protect	Risk management, compliance and audit		X	X	
A.5.5	Assessing impacts of AI systems	Assessing societal impacts of AI systems	The organization shall assess and document the potential societal impacts of their AI systems throughout their life cycle.	Yes	Yes	The AI Impact Assessment template includes a dedicated section to identify and evaluate potential societal impacts—such as effects on public trust, social cohesion, sustainability, or environmental harm. Assessments are conducted during design and reviewed regularly throughout the AI system's life cycle. Significant findings are documented and may be transferred to the organizational risk register for further tracking and action.	Completed AI Impact Assessment forms Impact Assessment Template with criteria Schedule or calendar for reassessment cycles Risk Register entries derived from impact assessments Communication or training material for staff conducting assessments	AI Officer	Preventive	X	X	X	Protect	Risk management, compliance and audit		X		
A.6.1.2	Organizational controls	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.	Yes	Yes	The organization defines responsible AI objectives addressing fairness, transparency, accountability, and societal impact. These objectives are documented and integrated into development plans, requirement documents, and process templates. They are communicated to all development teams and stakeholders. Adherence is monitored through regular reviews, audits, and design checkpoints across the AI lifecycle.	Responsible AI Objectives Document Development lifecycle policies referencing ethical objectives Evidence of integration in design, testing, and review workflows Meeting minutes or training sessions with development teams Internal review/audit reports checking adherence to objectives	AI Officer	Preventive	X	X	X	Protect	Policy and strategy management, risk management		X		
A.6.1.3	Organizational controls	Processes for responsible AI sys tem design and development	The organization shall define and document the specific processes for the responsible design and development of the AI system.	Yes	Yes	The organization has established documented procedures that integrate responsible AI principles—such as fairness, transparency, and accountability—into AI system design and development processes. These procedures are embedded into existing development lifecycle stages. All relevant staff are trained to apply these principles. The processes are reviewed and improved regularly based on internal feedback and external developments.	Responsible AI Design & Development Process Documentation AI development training attendance logs Ethics-by-design checklists or integrated lifecycle checkpoints Meeting minutes from periodic review sessions Records of updates made after review cycles	AI Officer	Preventive	X	X	X	Protect	System development lifecycle, quality assurance		X		
A.6.2.2	AI system life cycle	AI system requirements and spec ification	The organization shall specify and document require ments for new AI systems or material enhancements to existing systems.	Yes	Yes	Requirements for new AI systems and major enhancements are gathered through stakeholder interviews and workshops. All functional, technical, legal, ethical, and performance requirements are documented in a structured Requirements Specification Document. Stakeholders review and validate the documented requirements to ensure completeness and accuracy before design and development begin.	Requirements Specification Document template and completed samples Stakeholder interview/workshop notes Requirements validation meeting records Change log for updates to requirements Traceability matrix linking requirements to implementation	AI Officer	Preventive	X	X	X	Protect	System development lifecycle	X	X		
A.6.2.3	AI system life cycle	Documentation of AI system design and development	The organization shall document the AI system design and development based on organizational objectives, docu mented requirements and specification criteria.	Yes	Yes	The AI system design is documented using architecture diagrams, algorithm specifications, and data flow charts. Development logs and version control (e.g., Git) are maintained throughout the lifecycle. Design documentation is aligned with functional and non-functional requirements and reviewed regularly by cross-functional teams to ensure it supports business objectives and regulatory compliance.	Design documentation (architecture diagrams, specifications) Version control system records (e.g., Git commits, tags) Development logs or issue trackers (e.g., *Jira*) Design review meeting records Traceability matrix mapping requirements to design components	AI Officer	Preventive	X	X	X	Protect	System development lifecycle		X		
A.6.2.4	AI system life cycle	AI system verification and valida tion	The organization shall define and document verification and validation measures for the AI system and specify criteria for their use.	Yes	Yes	For each AI system, a Verification and Validation Plan is created, covering testing scope, types (unit, integration, user acceptance), acceptance criteria, and responsible roles. The plan ensures that the AI system meets functional, security, and performance requirements before going live. Test results are reviewed, issues are tracked, and retesting is conducted where necessary.	Verification and Validation Plan (V&V Plan) Test execution reports and screenshots Acceptance criteria checklist Bug/issue logs and resolution history Sign-off documents from validation stakeholders	AI Officer	Preventive	X	X	X	Identify	Testing and quality assurance	X	X		
A.6.2.5	AI system life cycle	AI system deployment	The organization shall document a deployment plan and ensure that appropriate requirements are met prior to deployment.	Yes	Yes	A standardized AI Deployment Plan template is used for each AI system. It outlines the deployment steps, roles, responsibilities, technical conditions, pre-deployment checks, and risk mitigation. Prior to deployment, a review is conducted to confirm that operational, technical, and security criteria are met. The deployment is executed according to the plan and monitored for deviations or anomalies.	AI Deployment Plan template and completed project examples Pre-deployment review checklist Approval log before production go-live Monitoring dashboard screenshots during deployment Post-deployment review reports or lessons learned	AI Officer	Preventive	X	X	X	Identify	Change and deployment management	X	X		
A.6.2.6	AI system life cycle	AI system operation and monitoring	Processes and procedures shall be defined and implemented to manage the information security risks associated with the ICT products and services supply chain.	Yes	Yes	Operational procedures for AI systems are defined in standard operating procedure (SOP) documents. These include task schedules for monitoring, updates, backups, anomaly detection, and incident response. Monitoring tools are used to track system performance in real time. The response to system failures is integrated with the broader incident management process, ensuring minimal disruption and clear escalation paths.	AI System SOPs (operation, patching, support, etc.) Performance monitoring dashboard screenshots/logs Ticketing system records for support and repairs Incident Response Plan including AI-specific triggers Records of system updates and downtime reports	AI Officer	Preventive	X	X	X	Identify Protect	Monitoring and incident response	X	X		
A.6.2.7	AI system life cycle	AI system technical documentation	The organization shall determine what AI system techni cal 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.	Yes	Yes	Technical documentation is prepared for each relevant stakeholder group, including user manuals, API documentation, developer integration guides, compliance summaries, and regulatory fact sheets. Documentation is tailored in structure and language based on the target audience (e.g., business users vs. regulators). A documentation owner is assigned for each artifact, and updates are performed after major releases.	Documentation register mapping audience to document type Published samples (user guide, developer API doc, audit trail extract) Distribution logs (internal portal, external partner access) Document update log / change control record Style guide or template library for technical documentation	AI Officer	Preventive	X	X	X	Identify	Documentation management	X	X	X	

A.6.2.8	AI system recording of event logs	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.	Yes	Yes	A Logging and Monitoring Policy has been established for AI systems, defining mandatory logging requirements during system operation and optionally during development, testing, and maintenance. Logging mechanisms are implemented using SIEM tools and platform-native solutions. Logs are reviewed regularly to detect anomalies, non-compliance, or security incidents. Responsibilities are defined in the AI RACI Matrix.	AI Logging and Monitoring Policy document, Log configuration files or screenshots of logging tools (e.g., ELK, Azure Monitor), Records of regular log reviews Anomaly detection rules or alerts AI RACI Matrix showing logging responsibility Audit trail from operational log retention system	AI Officer	Preventive	X	X	X	Protect	Monitoring and logging	X			
A.7.2	Data for AI systems	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.	Yes	Yes	VamiSec GmbH determines AI data requirements based on system functionality and objectives. All data sources are acquired through legal and ethical means. Acquisition methods, permissions, and provenance are documented to ensure transparency and traceability.	Data Acquisition Record Data Source Register Documented acquisition methods Consent or licensing agreements Ethical data sourcing guidelines	AI Officer	Corrective	X	X	X	Respond Recover	Data lifecycle management			X	
A.7.3	Data for AI systems	Acquisition of data	The organization shall determine and document details about the acquisition and selection of the data used in AI systems.	Yes	Yes	Data requirements for AI systems are determined based on functional and performance goals. All data acquisition activities follow a standardized and documented procedure to ensure legal and ethical sourcing. The organization maintains records of acquisition methods, data sources, provider details, and usage permissions in a centralized data acquisition register to ensure accountability and traceability.	Data Acquisition & Selection Procedure AI Data Acquisition Record (with source, method, and licensing details) Procurement or licensing agreements Internal checklists for ethical and legal validation Logs confirming ongoing traceability and updates to acquisition records	AI Officer	Detective	X	X	X	Detect Respond	Data sourcing and validation			X	
A.7.4	Data for AI systems	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.	Yes	Yes	A formal Data Quality Plan has been created using a standardized template. This plan defines quality criteria such as accuracy, completeness, consistency, and timeliness for all data used in AI systems. Responsibilities for ensuring data quality are assigned, and communication of data quality expectations is managed via scheduled activities. Effectiveness is monitored and improved through feedback loops and periodic review of data-related communications and outcomes.	Data Quality Requirements Document Completed Communication Plan including data quality scope Records of assigned responsibilities Meeting notes or communication logs Feedback reports or plan adjustments based on data quality monitoring	AI Officer	Corrective	X	X	X	Respond Recover	Data quality assurance			X	
A.7.5	Data for AI systems	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.	Yes	Yes	A documented process is in place to track and record the provenance of all data used in AI systems. This includes capturing information about data origin, providers, collection methods, acquisition dates, and usage purpose. Provenance records are stored securely and reviewed regularly to reflect any updates in data sources or usage. The process ensures traceability and supports auditability throughout the data and AI system lifecycle.	Data Provenance Procedure Data origin registry or catalog Acquisition logs and contracts with data providers Change history of data sets used Internal reviews or audits of provenance records	AI Officer	Preventive	X	X	X	Protect Identify	Data tracking and lineage			X	
A.7.6	Data for AI systems	Data preparation	The organization shall define and document its criteria for selecting data preparations and the data preparation methods to be used.	Yes	Yes	A Data Preparation Procedure has been established and documented. It defines standardized criteria for data cleaning, transformation, formatting, and validation prior to use in AI systems. The procedure specifies tools, acceptable formats, and quality thresholds. It is applied consistently before any dataset is used in model training, tuning, or inference tasks.	Data Preparation Procedure Document Sample data preprocessing pipelines Logs or records of data preparation activities Validation reports confirming compliance with preparation criteria Audit records or QA checks on input data used in models	AI Officer	Detective Corrective	X	X	X	Detect Respond	Data preprocessing and quality control		X	X	
A.8.2	Information for interested parties of AI systems	System documentation and infor mation for users	The organization shall determine and provide the necessary information to users of the AI system.	Yes	Yes	VamiSec GmbH erstellt benutzerfreundliche Anleitungen, die spezifisch auf verschiedene Nutzergruppen zugeschnitten sind. Die Dokumentation enthält klare Nutzungsanweisungen, Systemeinschränkungen und Haftungsausschlüsse. Nutzerfeedback wird regelmäßig zur Optimierung der Unterlagen eingeholt und berücksichtigt.	Benutzerhandbücher und Anleitungen Dokumentierte Nutzungshinweise und Disclaimer Feedbackformulare und Auswertungsberichte Änderungsprotokolle zur Dokumentation	AI Officer	Preventive	X	X	X	Protect	User communication and documentation		X		X
A.8.3	Organizational controls	External reporting	The organization shall provide capabilities for interested parties to report adverse impacts of the AI system.	Yes	Yes	Accessible reporting channels have been established, including a dedicated email address and an online reporting form. These channels are communicated publicly via system documentation and the organization's website. Responsibilities for monitoring and responding to reports are clearly assigned.	Public documentation of reporting channels on website and in user manuals Communication policy referencing the reporting process Designation of responsible roles Records of submitted reports and response actions	AI Officer	Protective Corrective			X	Protect Respond	Reporting management		X		X
A.8.4	Communication of incidents	Communication of incidents	The organization shall determine and document a plan for communicating incidents to users of the AI system.	Yes	Yes	An Incident Communication Plan has been developed to define when and how affected users are to be informed. The plan includes responsibilities, communication channels (e.g., email, dashboard notifications), and predefined messaging. Designated staff receive regular training to ensure incident communication is timely and effective.	Incident Communication Plan document Record of staff training on incident protocols List of responsible roles and contact channels Audit logs of past incident notifications (if applicable)	AI Officer	Preventive	X	X	X	Identify	Incident communication	X			
A.8.5	Information for interested parties	Intellectual property rights	The organization shall determine and document their obligations to reporting information about the AI system to interested parties.	Yes	Yes	Legal, regulatory, and contractual requirements relevant to information disclosures about AI systems have been identified and documented. These obligations are incorporated into the Communication Plan. A dedicated section outlines what must be reported, to whom, under which circumstances, and by which roles.	Mapping of legal and contractual disclosure obligations Updated Communication Plan with information obligation section Role-based responsibility matrix Communication logs (if any disclosures performed)	AI Officer	Preventive	X	X	X	Identify	Legal and regulatory compliance	X			
A.9.2	Use of AI systems	Processes for responsible use of AI systems	The organization shall define and document the processes for the responsible use of AI systems.	Yes	Yes	Procedures for the responsible use of AI systems have been documented. These include ethical guidelines, acceptable use policies, and usage boundaries. The procedures are communicated to all relevant staff, and training is provided where necessary. Monitoring mechanisms are in place to ensure adherence through audits and user feedback.	Responsible Use Procedure Document Training materials and attendance records Audit reports User feedback summaries	AI Officer	Preventive Corrective	X	X	X	Identify Protect	AI governance processes		X	X	

A.9.3	Use of AI systems	Objectives for responsible use of AI system	The organization shall identify and document objectives to guide the responsible use of AI systems.	Yes	Yes	Management reviews are scheduled at least annually. A structured template is used to prepare the agenda and gather relevant inputs, including audit results, performance data, and identified nonconformities. The meetings are documented, and action items and decisions are tracked.	Management Review Schedule Completed Management Review Templates Meeting Minutes Action Item Tracking Sheets	AI Officer	Preventive Corrective	X	X	X	Identify Protect	Strategic alignment and performance management				
A.9.4	Use of AI systems	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.	Yes	Yes	Intended use cases and system limitations are defined and documented in the technical and user documentation. Usage logs and metrics are monitored regularly to identify deviations or misuse and trigger corrective actions.	Documentation of Intended Use Usage Monitoring Reports Incident Reports related to misuse User Feedback Logs	AI Officer	Preventive Corrective	X	X	X	Identify	System documentation and monitoring	X			
A.10.2	Third-party and customer relationships	Allocating responsibilities	The organization shall ensure that responsibilities within their AI system life cycle are allocated between the organi zation, its partners, suppliers, customers and third parties.	Yes	Yes	Roles and responsibilities across all involved parties are clearly defined and contractually documented. Agreements cover obligations in each phase of the AI system life cycle. Stakeholders are informed through written communication and onboarding sessions.	Signed Responsibility Allocation Agreements Contractual Clauses defining roles Stakeholder Communication Records RACI Matrix or equivalent	AI Officer	Preventive	X	X	X	Protect	Contract and responsibility management	X	X		
A.10.3	Third-party and customer relationships	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.	Yes	Yes	Supplier evaluation criteria are defined to include compliance with responsible AI principles. All supplier contracts include specific clauses on AI ethics and transparency. Suppliers are regularly assessed for adherence to organizational AI requirements.	AI Supplier Management Policy Supplier audit reports Supplier contract templates with AI clauses Evaluation checklists or questionnaires	AI Officer	Preventive	X	X	X	Protect	Supplier and third-party management	X		X	
A.10.4	Third-party and customer relationships	Customers	The organization shall ensure that its responsible ap proach to the development and use of AI systems considers their customer expectations and needs.	Yes	Yes	Customer feedback is actively collected through surveys, interviews, and digital forms. This input is reviewed regularly and integrated into the design and enhancement of AI systems to better meet customer needs. Support channels are also in place to manage customer inquiries.	Survey results and feedback reports Feedback integration logs Change logs reflecting customer-driven updates Ticketing system records	AI Officer	Preventive	X	X	X	Protect	Customer engagement and feedback integration	X			

Version History			
Version	**Date**	**Changes**	**Name**
0.1	17/05/2025	Creation	Koral Yücel
1.0	5/20/2026	Review & Final	Valeri Milke

This template was created by the people of ICT Institute

You can find the latest version and other templates here:
https://ictinstitute.nl/free-templates/

You can use this template freely under the Create Commons Attribution license
https://creativecommons.org/licenses/by/4.0/

You can do the following with the templates:

Share. You can share the templates and any documents made with these templates freely, with any one that you want to share it with.
Adapt. You can make new documents based on the templates, make changes, add elements or delete elements as much as you want. You can even do this in commercial organisations of for commercial purposes.

If you are a customer, you do not have to mention ICT Institute anywhere
If you are not a customer, you must keep the text "create by the people of ICT Institute" somewhere

Note that the use of these templates is of course at your own risk.
Note also that the ISO standards are copyrighted. You must buy the standard from NEN or ISO before using it

Read also:
https://ictinstitute.nl/iso-27001-and-nen7510-support/
https://ictinstitute.nl/iso27002-explained-part-1/
https://ictinstitute.nl/iso27002-2022-explained-1/

_x000d_# This content is intended for public distribution.