COMPANY AI Policy

NOTE: I AM EDITING THIS, PLEASE BEAR WITH ME AS I PREPARE THE NEXT VERSION

ISO Clauses 4.3 & 5.2, 6.1.2, 6.1.3, 6.1.4
ISO 42001 Controls

Version 0.1

Date 2025-01-07

1. ContextP

1.1 Scope & Boundaries

[COMPANY] defines the scope of this Policy (and, if applicable, the broader AI Management System) to cover its AI-related activities. This includes:

- Products or services that incorporate machine learning models and influence decision-making.
- Services where AI processes personal data of customers or other data subjects.
- Internal AI applications used by the organization (R&D, HR, finance, etc.).

Permissible Exclusions: Any functions or departments that do not handle AI in any form (if justified). Exclusions are detailed in the Statement of Applicability.

Updates to the Scope: The scope is reviewed periodically or whenever significant changes to AI use arise.

Examples:

- If you are **primarily an AI Developer**: “(i) The research, development, provision, maintenance, and ongoing improvement of AI technologies, models, and applications…”
- If you are **primarily an AI User**: “(ii) The use of internally developed and externally procured AI technologies across all business units and functions…”
-

***Tip**: Customize this template in a short document or table that you attach to the policy to clarify exactly which AI systems and organizational units are included.*

1.2 Purpose

This policy defines COMPANY’s overarching approach to responsibly develop, deploy, operate, and manage AI systems. It provides a concise description of the aims, objectives, and overall structure of any associated AI Management System.

Key Definitions

- **AI**: An engineered or machine-based system designed to operate with varying levels of autonomy, generating outputs such as predictions or recommendations.
- **AI Model**: A component that uses computational or statistical techniques to process inputs and produce outputs.
- **AI System**: A machine-based system that, for explicit or implicit objectives, infers from input data how to generate outputs influencing physical or virtual environments.

*If these definitions are needed strictly for EU AI Act or ISO 42001 compliance, see **Appendix A (Definitions)**.*

1.3 Objectives

It applies to the scope defined above (1.1)**.** COMPANY is committed to fulfilling legal, regulatory, and ethical requirements.

1.4 Location(s)

The scope of the AI Management system applies to the following geographical location:

[Address]

Add additional addresses if applicable.

Note: None of the Controls in 42001 Annex A require auditors to access physical spaces to verify the controls so in theory you can specify that point here. However, the systems that some Certification issuers use require the head office location to be specified on the Certificate so you may run into issues here at least in the short term. (This appears to be a problem in the UK for example). If you aren't being ISO-certified, you may delete this sub-section.

2. Policy Statement

2.1 General

This Company Manual and Management System are how the Organisation satisfies the requirements of [ISO/IEC 42001 (along with the relevant aspects of the other systems listed in section 5.2)]. It specifies the requirements for AI, Information Systems, and Quality controls customised to the needs of the Organisation or specific parts thereof. *(Tip: Delete references to specs. as required).*

We are committed to regularly reviewing this AI Policy to ensure it remains relevant, effective, and aligned with the latest developments in AI ethics and governance.

The Organisation has adopted a process approach for developing, implementing, maintaining and improving the effectiveness of its Management System in order to ensure that the following benefits are realised:

- **Responsible AI Practices**: Ensures ethical, transparent, fair, responsible, and secure methods in AI system development, procurement, usage, and monitoring.
- **Reputation management**: enhances trust in AI applications through transparency.
- **Legal, Regulatory, and Contractual Governance**: Supports COMPANY identification and compliance with legal and regulatory standards (see table in Section 3.3).
- **Ethical Principles**: COMPANY shall uphold principles such as e.g.,fairness, accountability, transparency, privacy, sustainability (See Section 3.4 for details.)

- **Practical guidance: Risk Management and Impact Assessment**: manages systematic AI risk effectively and appropriately (including through the use of system impact assessments).
- **Identifying opportunities**: Encourages innovation within a structured framework.

The organisation, in adopting a process approach, is committed to:

- Understanding Artificial Intelligence and the need to establish policies and objectives
- Implementing and operating controls in the context of managing the Organisation's overall organisation risk (including AI risks)
- The achievement of Management System objectives
- Monitoring and reviewing the performance and effectiveness of the Management System
- The fulfilment of legal and other compliance obligations
- Enhancement and continual improvement based on objective measures
- Communicating throughout the Organisation the importance of meeting all applicable requirements, including relevant statutory and regulatory requirements specifically related to its business activities
- Ensuring that adequate resources are determined and provided to monitor, maintain and improve the Management System.
- Ensuring that the internal and external issues and requirements of interested parties have been considered as part of this scope. This applies to the AI risks under the business' control, considering factors such as the context in which the business operates and the needs and expectations of its employees, contractors, customers and other interested parties.

(optional) We are aware of the discussions circa September 2024 around the applicability of ISO/IEC 42001 within the EU, EEA, Switzerland and Turkey and the intention of the EU to develop an alternative standard to align with the EU AI Act. We are tracking developments with interest to ensure that we can comply with the EU AI Act and any alternative EU or international standard that emerges.

2.2 ISO/IEC 42001:2023

COMPANY is certified under and strives for compliance with the ISO/IEC 42001:2023 standard (the "**ISO Standard**").

To maintain compliance, COMPANY is committed in particular to:

- perform AI risk assessments and risk treatments in accordance with Clauses 6.1.2 and 6.1.3 of the ISO Standard respectively
- perform AI system impact assessments in accordance with Clause 6.1.4 of the ISO Standard
- Non-conformity, corrective action and continual improvement as described in sections 5.1 and 8 of this document and clauses 10.1 and 10.2 of the ISO Standard

- Monitoring, measurement, analysis & evaluation as described in sections 4.1 and 7.1 of this document and clause 9.1 of the ISO Standard
- Roles, responsibilities and authorities as described in sections 3.1 and 3.4 of this document and clause 5.3 of the ISO Standard
- The intended uses in appendix partially addresses ISO clauses 6.1.1 and 6.1.4 and controls 4.3, 5.3, 6.2.4, 6.2.6, 6.2.7, 6.2.8, 8.2, 9.3, 9.4

Tip: This clause is optional for companies certified under ISO/IEC 42001:2023.

3. Organization, Roles & Responsibilities

Roles and responsibilities have been defined and allocated to ensure accountability with respect to the AI Management System, AI objectives and AI risks; the Roles & Responsibilities Matrix is utilised to document this.

Responsibilities of the various roles are defined to the level appropriate for the individuals to perform their duties.

The relevant Contract of Employment, Job Description or Role Specification defines key staff's organisational roles, responsibilities and authorities.

The following are considered by the Organisation, and where required, their roles and responsibilities are defined:

3.1 Key Responsible Roles

Role/Committee	Individual(s)	Primary Responsibilities
Top Management (e.g. CEO, Board) In larger organisations, it may make sense to split the CEO and management team responsibilities.	Names and roles	The Management Team is responsible for maintaining the AI Management System, together with coordinating the following Management System activities: ● Operational responsibility for procedural matters, legal compliance, liaising with external organisations ● Approval of AI Policy ● Ensuring alignment with strategy

		• Allocating resources • Promotion of awareness and training • Internal auditing • Conducting Management Reviews • AI monitoring and measurement • Reporting nonconformances and ensuring corrective action takes place • Confirming the effectiveness of corrective action. • Ensuring documentation is maintained and updated • Management reporting
AI Steering Committee (if present) Management System Manager (if present)	Names and roles	Responsible for maintaining and coordinating the Management System and associated activities. These include conducting internal AI audits, coordinating risk assessments, risk treatments, and conducting impact assessments.
AI Development Lead	Names and roles	Oversees AI project lifecycle (design → deployment), ensures data quality.
Data Protection Officer (DPO)	Names and roles	Monitors privacy, data compliance, addresses data handling concerns, day-to-day responsibility for data protection
AI Ethics Officer (optional)	Names and roles	Advises on fairness and transparency issues, consults on ethical dilemmas.
Department/Business Unit Heads	Names and roles	Ensure departmental activities align with AI Policy, manage local risks, and allocate local resources.
ICT or DevOps Staff	Names and roles	Technical matters, including technical documentation, systems monitoring, technical incident investigation and liaison with technical contacts at external organisations.

All Personnel	All employees/contractors	Follow AI Policy and procedures, report incidents/nonconformities, complete required training.

***Template usage**: Adapt the table to your context (e.g., a small business may have only two or three named individuals). Update names and roles as needed. Where individual roles don't exist, ensure that the responsibilities are folded into another role (e.g. the Management Team or a specific department head may be made responsible for the responsibilities of the Management System manager).*

3.3 AI Role Definitions

AI Producers:	AI Producers are the individuals or teams responsible for creating AI models, algorithms and components that form the foundation of AI solutions. AI Producers ensure that the data used for training AI models is clean, accurate and ready for use whilst continuously monitoring and optimising AI models for optimal performance. They ensure these systems are built to meet ethical, technical, and regulatory standards, addressing risks and potential impacts throughout the AI lifecycle.
AI Providers:	AI Providers are responsible for deploying AI systems, models, or services to end users or other organizations, either as standalone products or integrated solutions. They ensure the accessibility, usability, and ongoing support of these systems while adhering to ethical, legal, and regulatory standards.
AI Users	AI Users are individuals or teams within an organisation who utilise AI tools, systems, services or insights. AI Users provide input data, interpret AI-generated insights and make informed decisions. They are responsible for ensuring the ethical and compliant use of AI, considering its potential impacts on stakeholders and adhering to relevant regulations and guidelines. AI systems that have been approved for use by the Organisation are documented within the AI Assets Register.

Define the Organisation's role against the three definitions above. Example:

The Organisation's role is confirmed as an AI Producer, Provider and User.

3.4 Relevant Laws and Regulations, Relevant Authorities

*Below is a **placeholder table** listing the laws and regulations COMPANY is particularly dedicated to observing, and its role with respect to the relevant authorities. Some may or may not apply depending on your jurisdiction:*

Law/Regulation	Jurisdiction	Key Requirements for AI	Responsible Owner
EU AI Act	EU Member States	Risk categorization, transparency, safety, documentation	Names and roles
GDPR	EU	Data protection, privacy, consent	Data Protection Officer
The Digital Services Act (DSA)	EU	Regulates online platforms to ensure a safer digital space, protecting users and combating illegal content.	
The Digital Markets Act (DMA)	EU	Aims to prevent anti-competitive behavior by big tech "gatekeepers" in digital markets.	
The Cybersecurity Act	EU	Establishes EU-wide cybersecurity certification for products and services to enhance trust and resilience. Related to NIS2.	ICT or DevOps Staff
EU Product Liability Directive (PLD)	EU Member States	EU's Product Liability Directive. Sets out rules for holding manufacturers liable for defective products in the EU, including software and AI products.	
EU General Product Safety Regulation (GPSR)	EU	EU's General Product Safety Regulation. Ensures all consumer products meet high safety standards across the EU market.	
European Convention on		An international treaty that protects fundamental human rights and freedoms across its member states.	

Human Rights (ECHR)		Legally binding with the implementation of the Treaty of Lisbon in 2009. It applies specifically to EU institutions and member states when implementing EU law.	
Charter of Fundamental Rights of the European Union (EU Charter, CFR)		The CFR outlines a comprehensive set of fundamental rights that apply across the EU. Enforced by the European Court of Human Rights (ECtHR) in Strasbourg.	
IEEE Ethical Standards	International (e.g. US)	Ethical AI, design transparency	AI Development Lead
Local Consumer Protection Act	Your country	Requirements for fairness, disclaimers, user transparency	Legal Dept. / Compliance
Others as needed	Various	Briefly describe relevant AI aspects	Names and roles

Example table for UK organisations:

Law/Regulation	Jurisdiction	Responsible Owner
EU AI Act	EU Member States	Names and roles
GDPR	EU	Data Protection Officer
IEEE Ethical Standards	International (e.g. US)	AI Development Lead
Local Consumer Protection Act	Your country	Legal Dept. / Compliance
Others as needed	Various	Names and roles
Office for Artificial Intelligence	UK	Management System Manager

Health & Safety Executive	UK	Management System Manager
The National Cyber Security Centre	UK	Management System Manager
The Data Protection Act (2018) (DPA 2018) and associated UK General Data Protection Regulations (UK GDPR)	UK	Data Protection Officer
The Equality Act (2010)	UK	Legal Dept. / Compliance
The Human Rights Act (1998)	UK	Legal Dept. / Compliance
The Regulation of Investigatory Powers Act 2000 (RIPA)	UK	Legal Dept. / Compliance
The UK's National AI Strategy	UK	AI Development Lead
Health and Safety at Work etc. Act 1974	UK	CEO (unless delegated to HR Director, HSEQ Manager, etc)
The Financial Conduct Authority (FCA) Regulation	UK	Legal Dept. / Compliance
The Automated and Electric Vehicles Act 2018	UK	Legal Dept. / Compliance

Intellectual Property Laws	Various	Legal Dept. / Compliance
The Electronic Communications Act (2000)	UK	Legal Dept. / Compliance
The Computer Misuse Act (1990)	UK	Legal Dept. / Compliance
The Digital Economy Act (2010)	UK	Legal Dept. / Compliance
The Copyright, Designs and Patents Act 1988 and Trade Marks Act 1994	UK	Legal Dept. / Compliance

> ***Tip**: This table is dynamic. You might add or remove items and identify a "Regulatory Tracking Role" who is responsible for monitoring changes in laws and regulations.*

3.5 Ethical Principles

COMPANY commits to the following **ethical principles** for responsible AI usage:

1. **Fairness & Non-Discrimination**
    - Prevent biased outcomes by regularly evaluating training data, performance metrics, and user feedback.
    - Design systems that address potential adverse impacts on specific user groups. In scenarios where digital humans are used to represent culturally significant expressions, special care must be taken to preserve cultural integrity and authenticity.
    - (optional?) AI Systems should reflect the richness and diversity of linguistic and cultural expressions. They must prevent homogenization and dilution of language or cultural expression and must ensure that regional dialects and cultural

variations are accurately represented. Stewardship of diverse experiences must be supported rather than collapsed into a single 'standard' model.
    - AI Systems must ensure fairness in the representation and usage of language, preventing bias and discrimination based on attributes such as race, gender, disability, or cultural background. AI Systems must prioritize inclusivity, ensuring that all representations are accurate, respectful, and do not perpetuate harmful stereotypes.
    - (optional) Ensure individuals have agency in how they are compensated.
    - (optional) Ensuring that individuals retain control over their Name, Image & Likeness (NIL) helps prevent exploitation and ensures that they are appropriately compensated when their likeness generates revenue.
2. **Accountability**
    - Maintain clear lines of responsibility throughout the AI life cycle.
    - Document processes so that decisions made or influenced by AI can be traced back to responsible individuals or committees.
    - (optional?) **Accounting & Auditability**: Organizations creating and deploying AI Systems must maintain transparency in their *processes and accounting*, providing clear and accessible information about *when and where representations are used*. Furthermore, there must be mechanisms in place for *auditability*, allowing individuals to seek redress in cases where their Copyright, NIL, or Personal Data (PII) is misused or misrepresented.
    - (optional?) **Decision-making & Accountability**: Organizations creating and deploying AI Systems must maintain transparency in their *processes and decision-making*, providing clear and accessible information about *how AI Systems work*. Furthermore, there must be mechanisms in place for *accountability*, allowing individuals to seek redress in cases where their Copyright, NIL, or Personal Data (PII) is misused or misrepresented.
        i. This process, decision-making and AI system usage information must be available to (a) individuals licensing NIL, (b) individuals and organisations making pre-sales or post-sales enquiries about AI Systems, (c) end users, and (d) disclosed to the general public.
    -
3. **Transparency & Explainability**
    - End users must provide Informed Consent before interacting with the AI System.
    - Disclose when users are interacting with an AI system.
    - End users shall be included at every stage of the design, build, evaluation and auditing to ensure that AI tools meet the needs of end users.
    - Provide, whenever feasible, user-friendly explanations of how AI-generated decisions are reached.
    - (optional) AI Systems must have clear, explicit policies regarding their quality, including performance metrics, algorithmic biases, and data usage. This information shall be accessible to all interested parties, ensuring that users and clients are fully informed about the AI's capabilities and limitations.
4. **Privacy & Data Governance**

    - All AI systems shall safeguard human autonomy, identity, and dignity with respect to privacy to the fullest possible extend.
    - All AI systems must prevent potential harms to privacy which necessitates adequate data governance that covers the quality and integrity of data used
    - Collect, use, and store data responsibly, maintaining compliance with data protection laws and regulations.
    - Securely manage access to data and logs.
    - (optional?) Ethical AI development should include ongoing monitoring, ethical oversight, and impact assessments to ensure that the AI System is compliant with all relevant AI legislation, regulations, and codes of practice, and aligns with ethical guidelines throughout its lifecycle. This includes regular audits, red team testing, and risk assessments to proactively address potential ethical and safety concerns.
        i. This monitoring, ethical oversight, impact assessment, auditing and risk assessment information must be available to (a) individuals licensing NIL, (b) individuals and organisations making pre-sales or post-sales enquiries about AI Systems, (c) end users, and (d) disclosed to the general public.
5. **Security, Safety,Reliability, Robustness & Maintainability**
    - Individuals' data must be protected with the highest standards of security and privacy, ensuring that personal information—including NIL data—is safeguarded against unauthorized access, misuse, and breaches. Data protection must adhere to Privacy by Design principles, embedding privacy considerations throughout the AI lifecycle.
    - Implement rigorous testing and monitoring to ensure AI systems remain accurate, robust, and secure.
    - Promptly address faults or deviations.
    - (optional) Individuals must have agency in whether their NIL's representation meets the quality bar, and the ability to prevent representations that do not meet the quality bar.
6. **Environmental Sustainability** (optional)
    - Consider energy efficiency in AI training and inference.
    - Support broader corporate sustainability objectives.
7. **Agency** (optional)
    - Ensuring that individuals have agency in how, when, where, and under what circumstances/scenarios any representation of their Name, Image and Likeness is used.
    - Individuals have an inherent right to control how their identity is represented and used, especially in commercial contexts. This control over one’s personal identity is a matter of dignity, allowing individuals to determine how they are perceived by the public and to avoid exploitation. When AI technologies or companies use someone's NIL without informed consent, it can result in significant emotional, financial, and reputational harm, undermining an individual's personal agency.
8. **Informed Consent** (recommend including if operating under the EU AI Act, consider including for other jurisdictions)

    - Ensuring that individuals (including end users and those whose training data is used) give informed consent before their copyright works, name, image and likeness, or other Personal Data is used. Informed consent includes the 10 steps defined in GDPR and ISO/IEC 29100.
9. **Ownership** (optional)
    - This principle reinforces the foundational concept that ownership rights are integral to ensuring fairness, dignity, and the protection of personal identity in AI Systems, aligning with broader ethical frameworks in AI governance, such as those outlined by the OECD and UNESCO.
        i. **Right to Ownership**: The principle that the individual should retain ownership of the AI System Source including any models or data that represent their NIL, significantly enhances their ability to assert their rights of control over how their digital representation is used, over QA, and fair compensation. This principle is grounded in international legal frameworks that emphasize personal autonomy and property rights, such as Article 17 of the Universal Declaration of Human Rights (right to property), as well as the Berne Convention for the Protection of Literary and Artistic Works, which protects the rights of creators over their work (including translation work).
        ii. **Transfer of Ownership**: Any transfer of ownership or rights must be done with Informed Consent, with clear communication explaining the implications of ceding ownership, particularly in terms of potential to create "unequal power dynamics" and potential inability to fully and effectively assert their rights of control over how their digital representation is used, over QA, and fair compensation.
10. **Education & Awareness** (required if operating under the EU AI Act. Required for employees/staff and supply/value chain if certified to ISO standards)
    - Promoting AI literacy and awareness within our organization, our value chain, and the communities we serve. We provide training and resources to ensure that individuals understand the ethical implications of AI and are equipped to contribute to responsible AI practices.
    - AI expertise internally and externally
    - Competence & training
11. Availability & quality of training data
    - AI systems based on ML need training, validation and test data in order to train and verify the systems for the intended behaviour.

If you have a Ethical AI Policy & Framework (e.g. have adopted a profile of the NIST framework), then replace this section with a reference to that document.

4. Planning and Metrics

4.1 AI Objectives and KPIs

Management System objectives are recorded in the Objectives Register with the following criteria:

- The status of progress towards achieving AI objectives is monitored and measured during the internal auditing process.
- The status of progress towards achieving AI objectives is evaluated during Management Review, where objectives may be added, enhanced or revised.

AI objectives consider the Ethical Principles (3.5).

Effective measurement of the defined objectives is achieved by applying all the procedures described in this system relating to recording, monitoring and analysing customer feedback and nonconformance issues.

The review of the AI objectives is an integral part of the AI Policy review as required by the procedures described in the AI Policy Process.

When setting **AI objectives**, COMPANY defines **Key Performance Indicators (KPIs)** or metrics to measure achievement. For instance:

- **Objective**: Achieve a maximum false-positive rate of 2% in a classification model.
    - **Metric**: Model's false-positive rate measured weekly on a validation dataset.
- **Objective**: Reduce bias in hiring recommendations.
    - **Metric**: e.g.Percentage difference in referral rates across demographic groups.

Where possible, objectives are based on the Specific, Measurable, Achievable, Realistic and Time-bound (SMART) methodology:

- **S - Specific** objectives must be clearly defined and clear
- **M - Measurable** objectives must be measurable through Key Performance Indicators (KPIs)
- **A - Achievable** objectives must be possible
- **R - Realistic** objectives must be realistic and in line with the Organisation's broader goals
- **T - Time-bound** objectives must have a defined time by which they will be achieved.

Template:

Objective	Metric / KPI	Target	Data Source	Review Frequency
Objective #1	E.g.error rate, usage stats, fair outcomes	Value/ Value %	Testset/logs Test set	Weekly/monthly/annual

Objective #2	Metric	Target	Data source	Frequency
Objective #3	Metric	Target	Data source	Frequency

5. Support & Documentation

5.1 Incident Management

- *COMPANY* references a separate **Incident Management Policy** (Document No. *xxxxxxxxx*) for all AI-related incidents, including data breaches, security vulnerabilities, system malfunctions, or ethical nonconformities.
- Responsible roles are defined for incident triage, escalation, root cause analysis, and corrective/preventive actions.

Placeholder:

- **Document name:** Document
- **Owner:** e.g. Security/ITDepartment
- **Department:** e.g.Security/ITDepartment
- **Escalation:** Describe escalation path, e.g.,AI Steering Committee
- **Example Timelines:** e.g., “24-hour initial report, 72-hour follow-up after analysis”

5.2 Integration with Other Management Systems

Use a **Cross-Reference Table** to show how AI procedures link to existing ISO or industry management system standards (e.g., ISO/IEC 27001 for security, ISO 9001 for quality, or ISO 27701 for privacy). For example:

Related Policy or Procedure	Reference Number	Area	AI Alignment
Information Security Policy (ISO 27001)	Doc ID	Data Security	Defines secure handling of AI system data, logs, and assets.
Privacy Management Procedures (ISO 27701)	Doc ID	Data Protection	Ensures AI data processing aligns with PII controllers.

ISO 22001	Doc ID		
ISO 22301	Doc ID		
Quality Management System (ISO 9001)	Doc ID	Quality Assurance	Aligns AI development with established QA processes.
ISO 14001	Doc ID		
B-Corp certification	Doc ID		
Add or remove as needed	Doc ID	AreaAreaArea	Alignment/Justification

5.3 Control of Documents of External Origin

Use a **Cross-Reference Table** to show how AI procedures link to other existing ISO or industry standards. For example:

Related Policy or Procedure	Reference Number	Area	AI Alignment
ISO 22989: AI Concepts and Terminology		Terminology	Provides foundational concepts and terminology to ensure consistent understanding and implementation within ISO 42001.
ISO 23894: AI Risk Management		Risk management	Aligns AI-specific risk management practices with ISO 42001's governance and operational requirements.
ISO 31000: Enterprise Risk Management		Risk management	Offers a general framework for enterprise risk management that

			complements ISO 42001's AI risk management processes.
ISO 42005: AI Impact Assessments		Impact assessments	Guides AI impact assessments, a critical component of ISO 42001's requirement to evaluate AI system effects.
ISO 5338: AI System Lifecycle Processes		Lifecycle processes	Defines lifecycle processes that ISO 42001 integrates for managing AI systems effectively across their lifecycle.
ISO 24368: AI Overview of Ethical and Societal Concerns		Ethics	Highlights ethical and societal concerns that ISO 42001 incorporates to ensure trustworthy and responsible AI.
ISO 38500: Governance of IT		IT Governance	Provides IT governance principles that underpin ISO 42001's alignment with organizational governance frameworks.
ISO 38507: Governance Implications of the use of AI		IT Governance	Addresses governance implications specific to AI, directly informing ISO 42001's governance requirements.
ISO/IEC 5259 - Data Quality for AI		Data Quality	Principles for managing and measuring data quality, preparing and governing data in AI.
Elements of valid Consent (draft)	Link	Consent	Consent/Assent for use of training data and for end users.
Add or remove as needed	Doc ID	AreaAreaArea	Alignment/Justification

6. Operation

Implementation of Controls:

- **Risk Assessment**: The Organisation has defined and established a Risk Assessment process that:

        - Considers AI risks
        - Aligns with the AI Policy and Organizational objectives (including AI objectives)
        - Assesses the realistic likelihood of the identified risk and determines a risk rating of Critical, High, Medium or Low.
        - Is designed to ensure repeated assessments produce consistent, valid and comparable results
        - Is periodically repeated or updated when major changes occur to the AI system
- Assesses the potential consequences to the Organisation, individuals and societies.**Risk Treatment**: The Organisation has defined and established a Risk Assessment process that:
    - Considers AI risk treatments
    - Selects risk treatment options, taking into consideration the results of the Risk Assessment.
        - Determines all necessary risk treatment controls and triggers and, when appropriate, documented and chosen options implemented.
        - Is periodically repeated or updated when major changes occur to the AI system
        - Reviews the Risk Treatment Plan and Statement of Applicability at least annually to verify that no necessary controls have been omitted.
        - Assesses the potential consequences to the Organisation, individuals and societies.
        - Requires authorisation of risk treatment plans by the Management Team before implementation commences. The Change Control Log retains a record detailing the approval status and completion.

    A Statement of Applicability has been documented that contains:

        - The necessary controls
        - Justification for inclusion or exclusion
        - Confirmation if the controls have been implemented.
- **System Impact Assessment**:
    - Where the Risk Assessment has identified the potential risk of medium or above, the Organisation assesses the impact of development, provision or use of AI Systems on individuals or society before introducing or substantially modifying AI systems. This is documented within the Impact Assessment.
    - Where appropriate, the results of the AI Impact Assessments are made available to relevant interested parties.
- **Controls (Annex A)**: COMPANY's Statement of Applicability (SoA) identifies which Annex A controls apply and whether additional custom controls are required.

    Tip*: The Controls and Assessments can be produced and maintained on an AI governance platform.*

    Tip*: The EU AI Act, ISO 42001 and NIST RMF* controls align and complement each other by promoting a unified framework for managing AI risks, ensuring compliance

with regulatory requirements, and embedding ethical and accountable practices for trustworthy AI systems.

Tip: The AI Management Essentials (AIME) provides an accessible resource for organizations to assess and improve their AI management systems and practices, by distilling key principles from existing AI regulations, standard and frameworks including the EU AI Act, ISO 42001 and NIST RMF.

7. Performance Evaluation

7.1 Monitoring, Measurement, Analysis and Evaluation

- : .

  The Management System is monitored, measured, analysed and evaluated through the application of the procedures documented in the Internal Audit and Management Review processes.

  The following Key Performance Indicators (KPIs) are used to track and assess the performance of the Management System and its objectives, and produce regular performance reports to the AI Steering Committee or Management:

Objective - Metric / KPI	Data Source	Review Frequency
Monitoring and evaluating the accuracy of the AI system - output and impacts	Testset/logsTest set	Weekly/monthly/annual
Monitoring of AI system usage for all individuals, e.g. producers, developers, designers, operators, testers, customers, partners etc.	Data source	Frequency
AI system repairs, updates and support	Data source	Frequency
Competency and training in the development and use of AI systems	Training/CPD records	“
Development and implementation of AI systems	“	“

AI system performance monitoring and testing	“	“
Monitoring and evaluation of AI Risks and Treatment		Actioned continually. Reviewed at the Management Review.
Internal Audit results		Actioned continually. Reviewed at the Management Review.
Nonconformances/AI Incidents		Actioned continually. Reviewed at the Management Review.

***Tip**: These objectives can be monitored by the Management Review and internal audits.*

E.g.
“Management Reviews of the Management System are carried out following the relevant procedures described in this Management System and relevant documented information relating to reviews is maintained.

Analysis of the KPIs and objectives is regularly carried out. All significant actions resulting from this analysis are reviewed as part of the Management Review process.

Notification of any anomalies from other reports (system monitoring, impacts, Users etc.) is sent to the Management System Manager. All significant actions resulting from this analysis are reviewed.

Regular Internal Management System and Statement of Applicability Audits are pre-defined, conducted and regulated to monitor the critical control points defined in the Risk Assessment.”

7.2 Audits

Ensure compliance with the Management System through regular internal and external audits:

- **Internal Audits**: Conduct internal audits to assess adherence to the framework, effectiveness of risk controls, and compliance with relevant regulations and standards.
- **External Audits**: Engage third-party auditors to independently verify the effectiveness of the management process and ensure alignment with ISO requirements.
- **Audit Reports**: Maintain records of internal and external audits, including findings, recommendations, and corrective actions taken.

7.2.1 Internal Audits

A Management System Audit Programme ensures that the Management System is verified by conducting an Internal Audit on each of the following Management System processes:

- Planning & Risk Management
- Operations
- Training & Competence
- Monitoring, Measurement, Analysis & Evaluation
- Document Management
- Management System
- AI Policy
- Nonconformity, Corrective Action & Continual Improvement
- Audits
- Management Commitment & Management Review
- The ISO 42001:2023 Statement of Applicability.

The Audit Programme considers the importance of the process, with those critical areas being audited more frequently.

Internal Management System Audits are carried out according to the following procedures:

- At the beginning of each month, the Management System Internal Auditor consults the Management System Audit Programme and establishes which, if any, of the Management System processes are to be audited during the coming month
- A member of staff, when possible independent of the activity to be audited, is appointed by the Management System Manager/representative
- The Auditor refers to the Management System processes and determines the activities to be audited
- The Auditor selects a representative number of records to be audited on a random basis
- The Auditor advises any employees concerned that an Management System Audit is being undertaken and answers any questions they may have regarding the audit
- The Auditor examines the records selected to determine whether the activities identified above have been carried out correctly

- The Auditor keeps a record of the process and the findings of the Management System Audit
- The Management System Audit record and all other documents that relate to Internal Management System Audits are passed to the Management System Manager or representative
- The Management System Audit record and all other documents relating to Internal Management System Audits are retained for inspection by the Certification Body at the Annual Surveillance Audit of the Management System
- All issues arising from the Internal Management System Audit requiring immediate attention are discussed with the appropriate employees. A record is kept on an Management System Audit Report and added to the Nonconformance Log, as appropriate.

The Management Team ensures that the Management System Audit results are discussed at the next Management Review.

- Conduct scheduled audits to verify compliance with this AI Policy.

7.3 Management Review

Management Reviews are held at no greater than [12]-monthly intervals.

The agenda for such meetings includes but is not limited to the following:

- The status of actions from previous Management Reviews
- Changes in external and internal issues that are relevant to the Management System, including:
    - A review of the Organisation's AI Policy, objectives and goals to determine whether they remain relevant to the requirements of Users, Producers and Providers
    - A review of the Assets Register and the Risk Assessment including the Treatment Plans
    - A review of the Statement of Applicability
    - Changes in the Organisation's operational environment that could affect the AI Management System requirements for additional or revised resources
    - Fulfilment of AI objectives
    - A review of the effect of Climate Change on the ability to achieve the intended results of the AI Management System
- Changes in needs and expectations of interested parties that are relevant to the AI Management System
- Information on the Management System performance, including trends in:
    - Nonconformities and corrective actions
    - Monitoring and measurement results

- Internal and External Audit results
- Opportunities for continual improvement and changes required to continually improve the AI Management System:
    - Staff competence and awareness needs that relate to the AI system requirements.

Minutes of the Management Review are documented, including any actions, opportunities and results to continually improve the AI Management System.

- Top Management reviews audit results, performance metrics, incident reports, and external requirements, making decisions on policy or procedural updates.

8. Improvement

8.1 Management System

The Organisation has established and operates a Management System following the requirements of the International Standard through the defined processes and documented information that can be found in:

- The Management System
- The Organisation's Policies, processes and procedures.

The Organisation maintains and retains documented information where required by International Standards.

As part of the implementation of the Management System, the Organisation has identified and documented in this Management System:

- The processes needed for the Management System
- The sequence and interaction of these processes
- The criteria and methods used to ensure the effective operation and control of these processes, including responsibilities and authorities
- The means to ensure the availability of the resources and the information necessary to support the operation, monitoring and continual improvement of these processes, objectives and the provision or use of AI systems
- Risks and opportunities

- The processes used to measure, where applicable, monitor and analyse these processes, implement action necessary to achieve planned results and monitor continual improvement.

As part of the Management Review process, the Organisation reviews the Management System and, when required, makes changes to ensure that it continues to meet management requirements.

***Tip**: If you do not operate a Management System, section 8.1 and references to Management system may be omitted.*

- *If you plan to certify to an ISO management system standard (examples include ISO 9001, 14001, 20000, 22301, 27001, 27701, 31000, 37301, 42001, 45001, and 50001) then establishing and maintaining a Management System is a requirement.*
- *Similarly if you are subject to the EU AI Act **and** engage with high risk AI systems.*
- *NIST RMF requires a structured management process but does not explicitly require a management system in the way that ISO standards do.*

***Tip**: You can still choose to operate a lightweight Management System if you aren't required to and aren't planning to certify. You gain the advantages of improved organization, risk mitigation, and performance without the rigidity or cost of full compliance frameworks.*

8.2 Nonconformity, Corrective Actions & Continual Improvement

- **Nonconformities & Corrective Actions**: All nonconformities are documented in Nonconformity/Corrective Action Logs, Incident Logs, or Software Systems and investigated to establish root causes and apply proportionate measures.

  Nonconformances may consist of the following:

  - Nonconformance in relation to data security, such as incidents or breaches
  - Nonconformances of the IMS
  - AI system nonconformances, such as inaccuracies
  - AI system incidents, including concerns and events.

- **Corrective Action**: Corrective actions are appropriate to the effects of nonconformities encountered; any actions taken to correct activities not meeting the requirements of the Management System are recorded and further reviewed.

Corrective actions may be required as a result of AI-related incidents or concerns raised as outlined in the Statement of Applicability.

- **Continual Improvement**: Any actions taken to prevent recurrence are similarly recorded.

  The Organisation is committed to continually improving the suitability, adequacy and effectiveness of the IMS, which is demonstrated through the Nonconformity, Corrective Action & Continual Improvement, Internal Audit, Management Review and Risk Management processes and other initiatives such as staff awareness training (including awareness training on AI-related topics).

-

9. Version History

Law/Regulation	Version	Jurisdiction
Date	Version ID	Approver(s)
Date	Version ID	Approver(s)

***Tip**: As you edit the policy…*

License & Contributors

Contributors:

- Kevin Schawinski (Modulos)
- Thomas Kuster (LEXR)
- Michael Davey (Michael Davey Consulting Ltd)
- Plan-Do-Check-Act cycle diagram by Karn Bulsuk (http://www.bulsuk.com)
- *YOUR NAME*

© 2025 Modulos AG & Contributors. This work is licensed under CC BY 4.0.

Appendices

Below are **optional** or more **detailed** materials that certain organizations may wish to include, depending on jurisdiction and organizational complexity.

Appendix A: Definitions (EU AI Act, ISO 42001, etc.)

1. **AI** (EU AI Act definition): "…designed to operate with varying levels of autonomy…"
2. **AI System** (ISO 42001 definition): "A machine-based system…"
3. **More definitions as needed**.

Appendix B: ISO/IEC 42001-Specific References

- **Clause 6.1.2 & 6.1.3**: Details on AI risk assessment and treatment.
- **Clause 6.1.4**: Impact assessments.
- **Clause 10.1 & 10.2**: Corrective actions and continual improvement.

Appendix C: Region-Specific Laws

Law	Jurisdiction	Owner
The Data Protection Act (2018)	UK	Data Protection officer
The Equality Act (2010)	UK	Legal Dept. / Compliance
…	…	…

Appendix D: Optional Ethical or Cultural Requirements

- **Name, Image & Likeness (NIL)**
  - Ensuring individuals' agency over their likeness in AI-based usage.
  - Potential compensation or usage constraints.
- **Cultural Integrity & Linguistic Diversity**
  - AI systems to reflect local dialects, avoid cultural homogenization.
- **Informed Consent**
  - Extended clarifications on how you obtain, record, and maintain consent (GDPR, ISO 29100).

Appendix E: Example Prohibited Use Cases

If your organization needs to define certain "red lines" or prohibited AI usage scenarios (e.g., misuse of IP, biometric identification, gambling or weaponization), you can list them here. These might align with:

- EU AI Act's High-Risk or Prohibited Categories
- EULA terms or internal code of conduct
- Sector-specific constraints (medical, finance, etc.)