AI Governance, Risk, Compliance & Culture

Helping you govern

Azhar Zia-ur-Rehman

MS BE

Certified in AI Governance

Certified Business Model Transformation Practitioner

Certified Information Systems Auditor

Certified Information Security Manager

Lead Cybersecurity Manager

Certified in Risk & Information Systems Control

Certified in ITIL

ISO27k Certified Lead Auditor

ISO20000 Lead Auditor

ISO22301 Lead Auditor

Certified Revenue Assurance Auditor

971 50 6139436

92 316 626 9792

azharzr@rehmaniyah.com

United Nations A/78/L.49

General Assembly

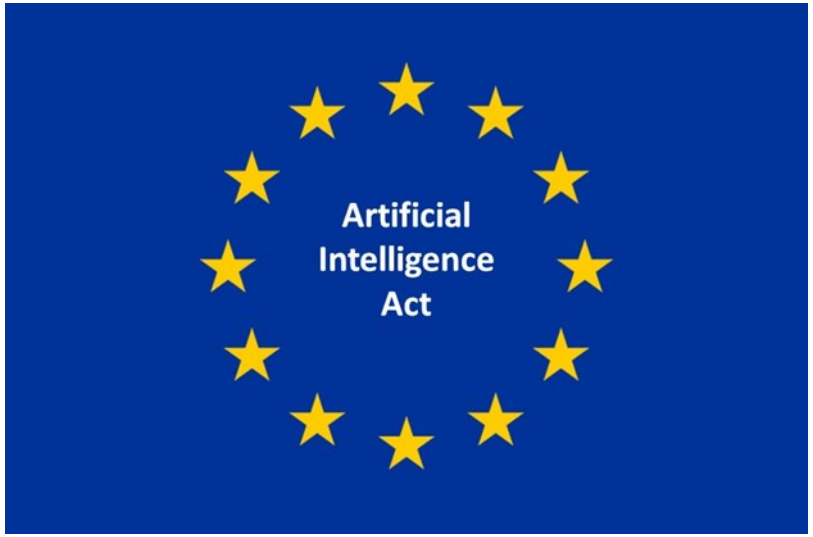
Distr.: Limited
11 March 2024

Original: English

Seventy-eighth session
Agenda item 13
Integrated and coordinated implementation of and follow-up to the outcomes of the major United Nations conferences and summits in the economic, social and related fields

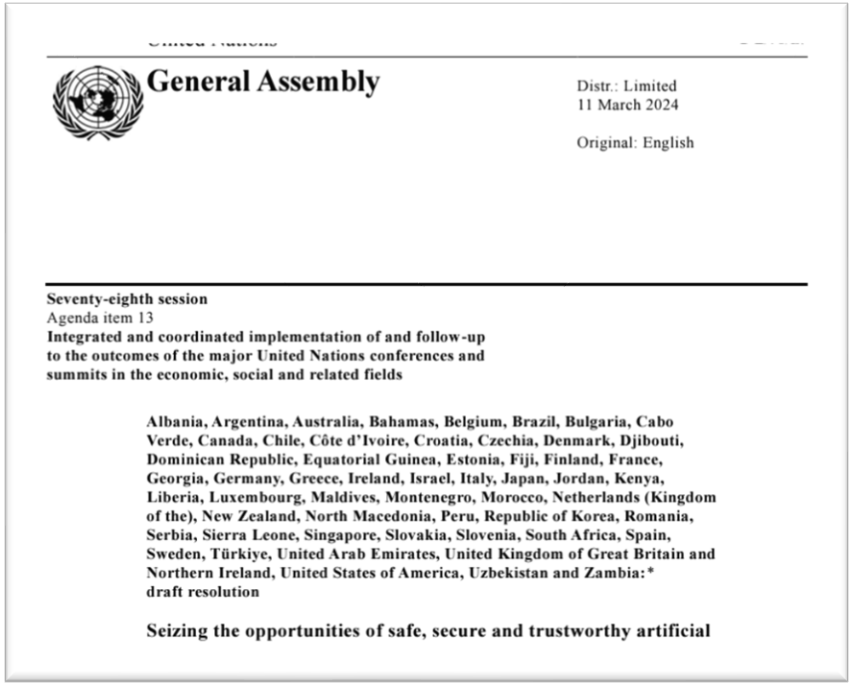
Albania, Argentina, Australia, Bahamas, Belgium, Brazil, Bulgaria, Cabo Verde, Canada, Chile, Côte d'Ivoire, Croatia, Czechia, Denmark, Djibouti, Dominican Republic, Equatorial Guinea, Estonia, Fiji, Finland, France, Georgia, Germany, Greece, Ireland, Israel, Italy, Japan, Jordan, Kenya, Liberia, Luxembourg, Maldives, Montenegro, Morocco, Netherlands (Kingdom of the), New Zealand, North Macedonia, Peru, Republic of Korea, Romania, Serbia, Sierra Leone, Singapore, Slovakia, Slovenia, South Africa, Spain, Sweden, Türkiye, United Arab Emirates, United Kingdom of Great Britain and Northern Ireland, United States of America, Uzbekistan and Zambia:*
draft resolution

Seizing the opportunities of safe, secure and trustworthy artificial intelligence systems for sustainable development



Recognizing also that the improper or malicious design, development, deployment and use of artificial intelligence systems, such as without adequate safeguards or in a manner inconsistent with international law, pose **risks** that could hinder progress towards the achievement of the 2030 Agenda for Sustainable Development and its Sustainable Development Goals and undermine sustainable development in its three dimensions …

Recognizing also that the **governance of artificial intelligence** systems is an evolving area and the need for continued discussions on possible governance approaches that are appropriate, based on international law, interoperable, agile, adaptable, inclusive, responsive to the different needs and capacities of developed and developing countries alike and for the benefit of all, …



General Assembly

Distr.: Limited
11 March 2024

Original: English

Seventy-eighth session
Agenda item 13
Integrated and coordinated implementation of and follow-up to the outcomes of the major United Nations conferences and summits in the economic, social and related fields

Albania, Argentina, Australia, Bahamas, Belgium, Brazil, Bulgaria, Cabo Verde, Canada, Chile, Côte d'Ivoire, Croatia, Czechia, Denmark, Djibouti, Dominican Republic, Equatorial Guinea, Estonia, Fiji, Finland, France, Georgia, Germany, Greece, Ireland, Israel, Italy, Japan, Jordan, Kenya, Liberia, Luxembourg, Maldives, Montenegro, Morocco, Netherlands (Kingdom of the), New Zealand, North Macedonia, Peru, Republic of Korea, Romania, Serbia, Sierra Leone, Singapore, Slovakia, Slovenia, South Africa, Spain, Sweden, Türkiye, United Arab Emirates, United Kingdom of Great Britain and Northern Ireland, United States of America, Uzbekistan and Zambia:* draft resolution

Seizing the opportunities of safe, secure and trustworthy artificial

Acknowledges that the United Nations system, consistent with its mandate, uniquely contributes to reaching **global consensus on safe, secure and trustworthy artificial intelligence systems**, that is consistent with international law, in particular the Charter of the United Nations; the Universal Declaration of Human Rights; and the 2030 Agenda for Sustainable Development, including by promoting inclusive international cooperation and facilitating the inclusion, participation and representation of developing countries in deliberations.

Artificial Intelligence Standards

ISO 4213:2022 Assessment of machine learning classification performance
ISO 5338:2023 AI system life cycle processes
ISO 5339:2024 Guidance for AI applications
ISO 5392:2024 Reference architecture of knowledge engineering
ISO 5469:2024 Functional safety and AI systems
ISO 8183:2023 Data life cycle framework
ISO 20546:2019 Big data — Overview and vocabulary
ISO 20547-1:2020 Big data reference architecture — Part 1: Framework and application process
ISO 20547-2:2018 Big data reference architecture — Part 2: Use cases and derived requirements
ISO 20547-3:2020 Big data reference architecture — Part 3: Reference architecture
ISO 20547-5:2018 Big data reference architecture — Part 5: Standards roadmap
ISO 22989:2022 Artificial intelligence concepts and terminology
ISO 23053:2022 Framework for Artificial Intelligence (AI) Systems Using Machine Learning (ML)
ISO 23894:2023 Artificial intelligence — Guidance on risk management
ISO 24027:2021 Artificial intelligence (AI) — Bias in AI systems and AI aided decision making
ISO 24028:2020 Artificial intelligence — Overview of trustworthiness in artificial intelligence
ISO 24029-1:2021 Assessment of the robustness of neural networks — Part 1: Overview
ISO 24029-2:2023 Assessment of the robustness of neural networks — Part 2: Methodology for the use of formal methods
ISO 24030:2021 Artificial intelligence (AI) — Use cases
ISO 24368:2022 Artificial intelligence — Overview of ethical and societal concerns
ISO 24372:2021 Artificial intelligence (AI) — Overview of computational approaches for AI systems
ISO 24668:2022 Artificial intelligence — Process management framework for big data analytics
ISO 25058:2024 Guidance for quality evaluation of artificial intelligence (AI) systems
ISO 25059:2023 Quality model for AI systems
ISO 38507:2022 Governance implications of the use of artificial intelligence by organizations
ISO 42001:2023 Artificial intelligence — Management system

Artificial Intelligence GRC&C Standards

ISO 38507:2022 Governance implications of the use of artificial intelligence by organizations

ISO 42001:2023 Artificial intelligence — Management system

ISO 23894:2023 Artificial intelligence — Guidance on risk management

ISO 24368:2022 Artificial intelligence — Overview of ethical and societal concerns

ISO 24027:2021 Artificial intelligence (AI) — Bias in AI systems and AI aided decision making

ISO 24028:2020 Artificial intelligence — Overview of trustworthiness in artificial intelligence

ISO 25058:2024 Guidance for quality evaluation of artificial intelligence (AI) systems

ISO 25059:2023 Quality model for AI systems

ISO 5469:2024 Functional safety and AI systems

ISO Standard for Artificial intelligence

ISO/IEC 42001:2023 AI Management System Standard

CertBetter

Artificial Intelligence Management System

What is Governance?

human-based system by which an organization is directed, overseen and held accountable for achieving its defined purpose

ISO 37000:2021

What is a Management System?

person or group of people that has its own functions with responsibilities, authorities and relationships to achieve its objectives

set of interrelated or interacting elements of an organization to establish policies and objectives, as well as processes to achieve those objectives

result to be achieved

ISO 42001:2023 3.4

What is Artificial Intelligence?

combination of interacting elements organized to achieve one or more stated purposes

capability of an engineered system to acquire, process and apply knowledge and skills

ISO/IEC 24028:2020

learned capacity to perform a task to a specified expectation

ISO 30428

meaningful data

knowledge are facts, information and skills acquired through experience or education

AI Management System

This document intends to help organizations responsibly perform their role with respect to AI systems (e.g. to use, develop, monitor or provide products or services that utilize AI).

This document provides requirements for establishing, implementing, maintaining and continually improving an AI management system within the context of an organization.


BS ISO/IEC 42001:2023

INTERNATIONAL STANDARD

ISO/IEC 42001

First edition
2023-12

Information technology — Artificial intelligence — Management system

Technologies de l'information — Intelligence artificielle — Système de management

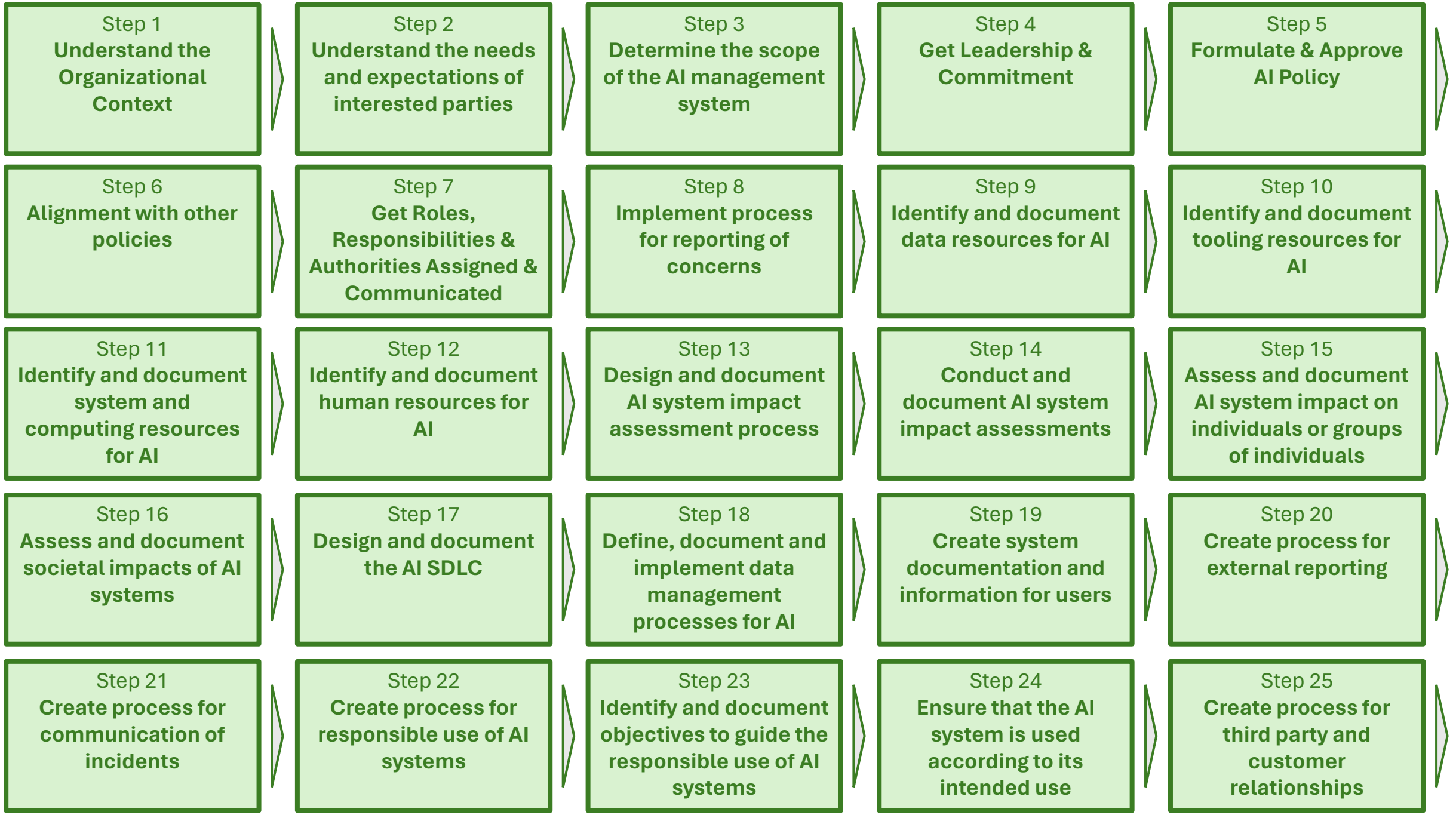
ISO IEC

Reference number
ISO/IEC 42001:2023(E)

Why an AI Management System?

To help the organization develop, provide or use AI systems responsibly in pursuing its objectives and meet applicable requirements, obligations related to interested parties and expectations from them.

Designing and implementing
an
AI Governance & Management System


Step 1
Understand the Organizational Context
Step 2
Understand the needs and expectations of interested parties
Step 3
Determine the scope of the AI management system
Step 4
Get Leadership & Commitment
Step 5
Formulate & Approve AI Policy
Step 6
Alignment with other policies
Step 7
Get Roles, Responsibilities & Authorities Assigned & Communicated
Step 8
Implement process for reporting of concerns
Step 9
Identify and document data resources for AI
Step 10
Identify and document tooling resources for AI
Step 11
Identify and document system and computing resources for AI
Step 12
Identify and document human resources for AI
Step 13
Design and document AI system impact assessment process
Step 14
Conduct and document AI system impact assessments
Step 15
Assess and document AI system impact on individuals or groups of individuals
Step 16
Assess and document societal impacts of AI systems
Step 17
Design and document the AI SDLC
Step 18
Define, document and implement data management processes for AI
Step 19
Create system documentation and information for users
Step 20
Create process for external reporting
Step 21
Create process for communication of incidents
Step 22
Create process for responsible use of AI systems
Step 23
Identify and document objectives to guide the responsible use of AI systems
Step 24
Ensure that the AI system is used according to its intended use
Step 25
Create process for third party and customer relationships

We will discuss the first six steps in brief.

Step 1 -- Understand the Organizational Context with respect to AI

- ✓ AI providers, including AI platform providers, AI product or service providers;
- ✓ AI producers, including AI developers, AI designers, AI operators, AI testers and evaluators, AI deployers, AI human factor professionals, domain experts, AI impact assessors, procurers, AI governance and oversight professionals;
- ✓ AI customers, including AI users;
- ✓ AI partners, including AI system integrators and data providers;
- ✓ AI subjects, including data subjects and other subjects;
- ✓ relevant authorities, including policymakers and regulators.

Step 1 -- Understand the Organizational Context with respect to AI

- ✓ Applicable legal requirements, including prohibited uses of AI;
- ✓ Policies, guidelines and decisions from regulators that have an impact on the interpretation or enforcement of legal requirements in the development and use of AI systems;
- ✓ Incentives or consequences associated with the intended purpose and the use of AI systems;
- ✓ Culture, traditions, values, norms and ethics with respect to development and use of AI;
- ✓ Competitive landscape and trends for new products and services using AI systems;
- ✓ Organizational context, governance, objectives, policies and procedures;
- ✓ Contractual obligations;
- ✓ Intended purpose of the AI system to be developed or used.

Step 2 -- Needs and expectations of interested parties

- ✓ The interested parties that are relevant to the AI management system;
- ✓ The relevant requirements of these interested parties;
- ✓ Which of these requirements will be addressed through the AI management system.

Step 3 -- Scope of the AI management system

The scope of the AI management system shall determine the organization’s activities related to the AI management system, leadership, planning, support, operation, performance, evaluation, improvement, controls and objectives.

Step 4 -- Leadership and Commitment to the AIMS

- ✓ Ensure that an **AI policy** and **AI objectives** are established and are compatible with the strategic direction of the organization;
- ✓ Ensure the integration of the AI management system requirements into the organization's business processes;
- ✓ Ensure that the resources needed for the AI management system are available;
- ✓ Communicate the importance of effective AI management and of conforming to the AI management system requirements;
- ✓ Ensure that the AI management system achieves its intended result(s);
- ✓ Direct and support persons to contribute to the effectiveness of the AI management system;
- ✓ Promote continual improvement;
- ✓ Support other relevant roles to demonstrate their leadership as it applies to their areas of responsibility.

Step 5
AI Policy 1/2

1. **Introduction**
    1. Overview of the organization's commitment to ethical and responsible AI.
    2. Purpose and scope of the AI Policy.
    3. Reference to ISO 42001:2023 compliance.
2. **Definition and Scope of Artificial Intelligence**
    1. Clear definition of artificial intelligence and related terms.
    2. Explanation of AI technologies and applications relevant to the organization.
3. **Ethical Principles and Values**
    1. Statement of ethical principles guiding the development and use of AI.
    2. Commitment to fairness, transparency, accountability, and privacy in AI systems.
    3. Alignment with internationally recognized ethical frameworks (e.g., IEEE, OECD).
4. **Governance and Accountability**
    1. Description of roles and responsibilities for AI governance.
    2. Establishment of oversight mechanisms for AI-related decision-making.
    3. Accountability mechanisms for addressing issues and ensuring compliance.
5. **Data Governance and Management**
    1. Policies and procedures for responsible data collection, storage, and usage.
    2. Data quality standards and validation processes for AI models.
    3. Data privacy and security measures to protect sensitive information.
6. **Algorithmic Transparency and Explainability**
    1. Requirements for transparent AI systems and algorithms.
    2. Guidelines for providing explanations and justifications for AI decisions.
    3. Measures to mitigate biases and ensure fairness in algorithmic outputs.

Step 5
AI Policy 2/2

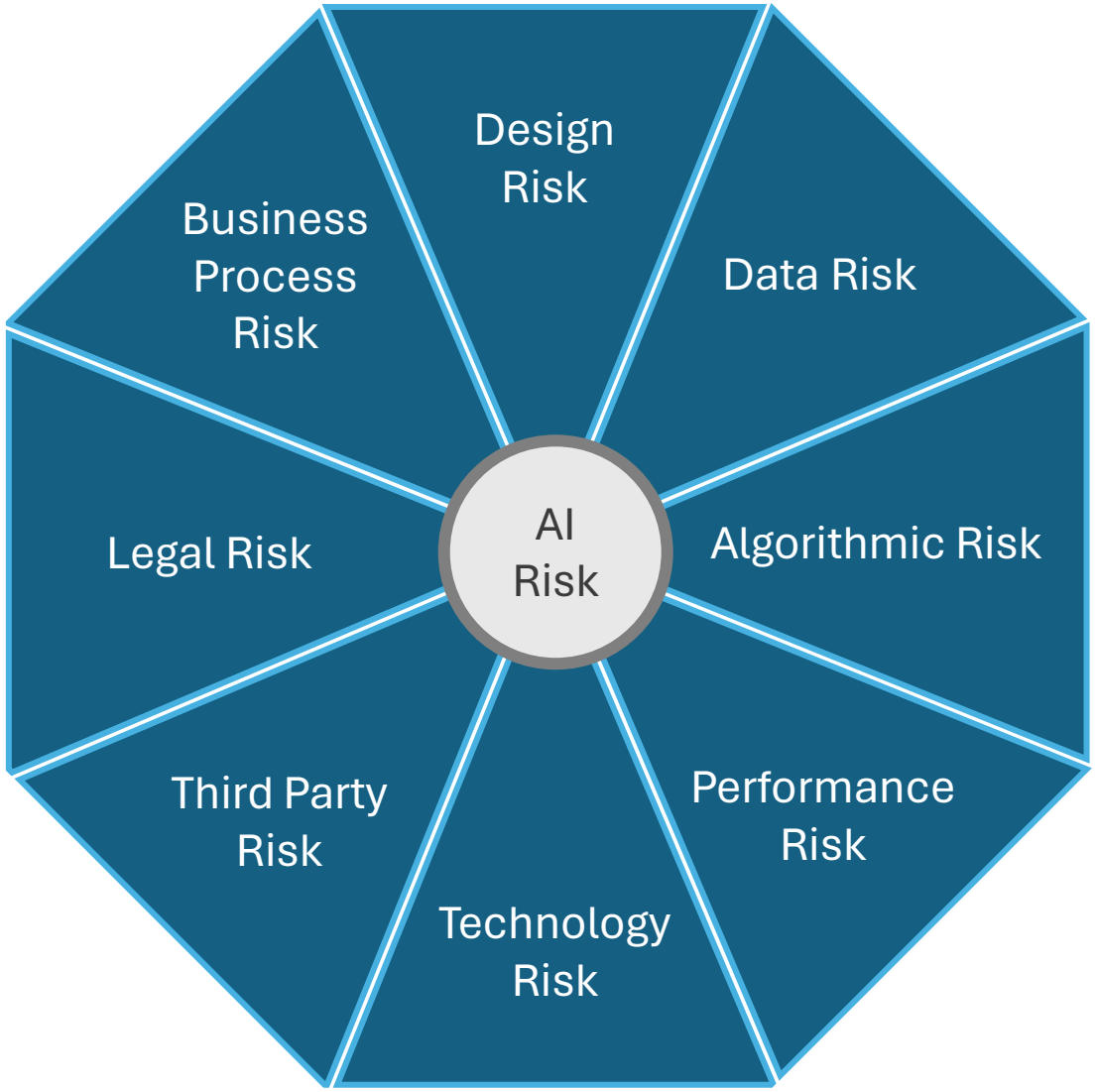
7. **Risk Management**
    1. Identification and assessment of risks associated with AI deployment.
    2. Risk mitigation strategies and controls for AI-related risks.
    3. Monitoring and review mechanisms for ongoing risk management.
8. **Compliance and Legal Considerations**
    1. Compliance with relevant laws, regulations, and industry standards.
    2. Legal considerations related to intellectual property, liability, and accountability.
    3. Measures to ensure AI systems adhere to legal and regulatory requirements.
9. **Training and Awareness**
    1. Training programs for employees involved in AI development and deployment.
    2. Awareness campaigns to educate stakeholders about AI ethics and best practices.
    3. Continuous learning initiatives to stay updated on emerging AI trends and issues.
10. **Stakeholder Engagement and Transparency**
    1. Engagement strategies for involving stakeholders in AI-related decisions.
    2. Transparency measures for communicating AI capabilities, limitations, and risks.
    3. Channels for receiving feedback and addressing stakeholder concerns.
11. **Monitoring and Continuous Improvement**
    1. Monitoring mechanisms to assess the performance and impact of AI systems.
    2. Feedback loops for capturing lessons learned and improving AI practices.
    3. Commitment to continuous improvement in AI governance and ethics.
12. **Documentation and Reporting**
    1. Documentation requirements for AI development processes and decisions.
    2. Reporting obligations for AI-related activities, risks, and performance.

Step 6 – Alignment With Other Policies

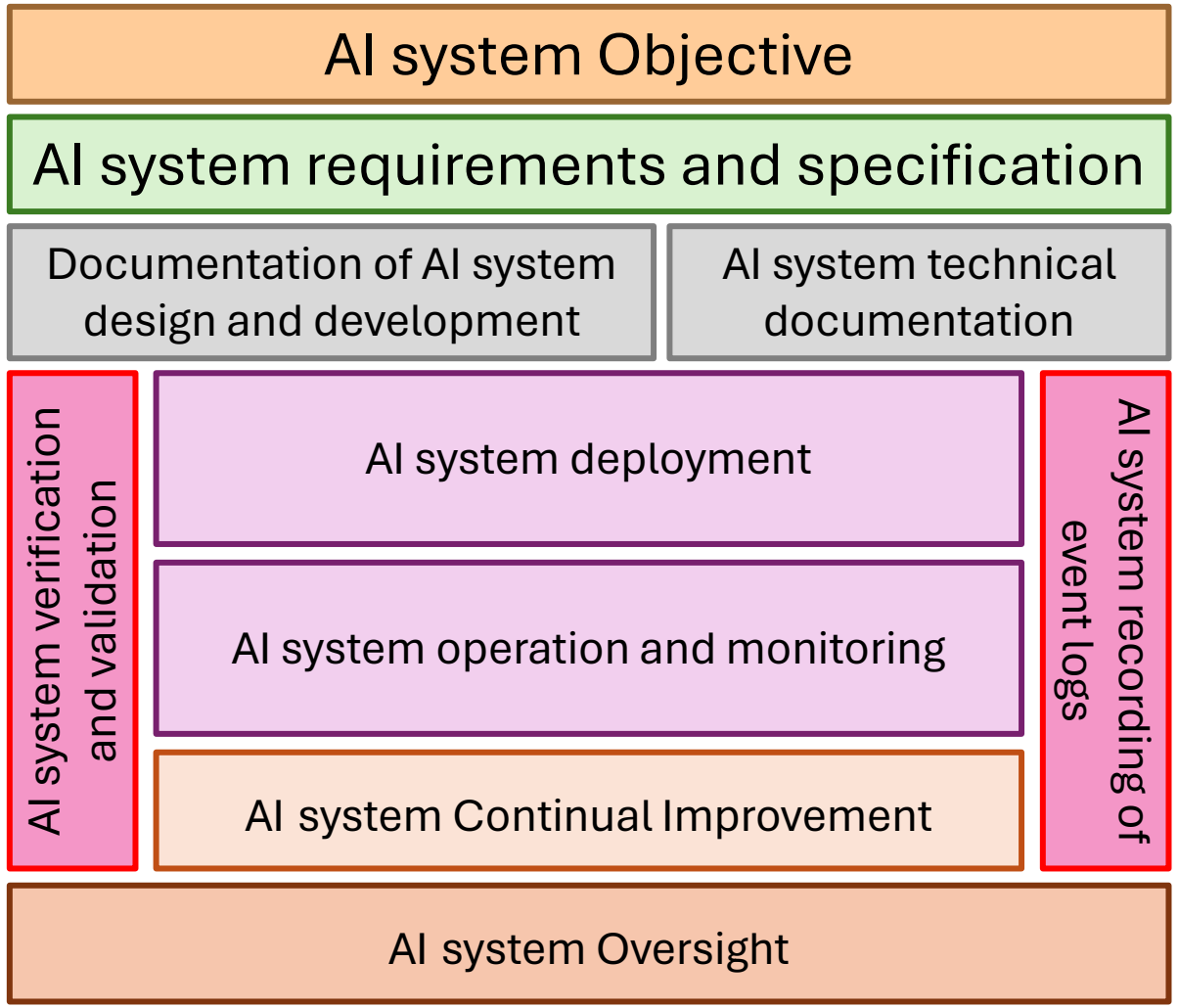
1. Data Privacy and Protection Policies
2. Security Policies
3. Ethical Guidelines
4. Compliance and Regulatory Policies
5. Intellectual Property (IP) Policies
6. Human Resources (HR) Policies
7. Risk Management Policies
8. Corporate Governance Policies
9. Data Governance Policy
10. Procurement and Vendor Management Policies
11. Sustainability and Environmental Policies

AI Poses Risks

©Azhar Zia-ur-Rehman



AI System Lifecycle



AI & Corporate Culture

Job Displacement and Anxiety
AI can automate tasks that were previously performed by humans, leading to job losses and creating anxiety among employees about job security. This can lead to decreased morale and increased resistance to AI initiatives.

Reduced Human Interaction
Over-reliance on AI can reduce face-to-face interactions among employees, potentially weakening team cohesion, communication, and collaboration.

Bias and Fairness Issues
AI systems can perpetuate or even exacerbate existing biases if they are trained on biased data. This can lead to unfair treatment of certain groups of employees, affecting workplace equity and inclusion.

Loss of Human Touch
AI-driven processes can lack empathy and the human touch, which are crucial in certain areas like HR, customer service, and conflict resolution. This can lead to dissatisfaction among both employees and customers.

Skill Gaps
The rapid adoption of AI can outpace employees' ability to learn new skills, leading to a skills gap. Companies might struggle to find employees with the necessary skills to work alongside AI.

Data Privacy Concerns
The use of AI often involves collecting and analysing large amounts of data, raising concerns about data privacy and security. This can lead to distrust among employees regarding how their data is being used.

Overdependence on AI
Relying too heavily on AI can lead to overdependence, reducing employees' critical thinking and problem-solving abilities. It can also lead to complacency in decision-making processes.

Ethical Dilemmas
The deployment of AI can raise ethical questions, such as the extent of AI's decision-making power and its impact on human autonomy. These dilemmas can create tension within the corporate culture.

Resistance to Change
Employees may resist adopting AI technologies due to fear of the unknown or discomfort with change. This resistance can hinder the successful implementation of AI initiatives.

AI & Domestic Culture

Privacy Invasion
AI-powered devices often collect vast amounts of personal data, which can raise significant privacy concerns. The constant monitoring by smart home devices can make individuals feel their privacy is being invaded.

Overreliance on Technology
Increased dependence on AI for daily tasks can lead to a reduction in essential skills, such as cooking, cleaning, or managing household affairs without technological assistance.

Decreased Human Interaction
The use of AI can reduce face-to-face interactions among family members. For instance, children might prefer interacting with AI-driven devices over spending time with family members, leading to a sense of isolation.

Loss of Autonomy
Relying on AI for decision-making, even in mundane tasks, can reduce individuals' sense of autonomy and agency in their own lives.

Security Risks
AI devices connected to the internet can be vulnerable to hacking and cyberattacks, posing security risks to personal data and home safety.

Erosion of Traditional Skills
As AI takes over various household chores, traditional skills and crafts may become less common, leading to a loss of cultural heritage and practical knowledge passed down through generations.

Digital Divide
The benefits of AI are often not equally distributed. Households with higher incomes can afford advanced AI technologies, while lower-income families may be left behind, exacerbating social inequalities.

Addiction and Screen Time
AI-powered entertainment and social media can be highly addictive, leading to excessive screen time. This can negatively impact physical health, mental well-being, and family relationships.

Ethical and Moral Concerns
The deployment of AI in homes can raise ethical questions, such as how much control AI should have over personal choices and the extent to which individuals should allow AI to influence their lives.

Cultural Homogenization
AI technologies are often developed with a specific cultural context in mind, typically Western. This can lead to the erosion of local customs and practices, contributing to cultural homogenization.

Parental Challenge
AI in the form of virtual assistants or educational tools can change the dynamics of parenting, with parents needing to balance the benefits of these tools against the potential for reduced direct interaction with their children.

AI & Religion

Dilution of Religious Practices
AI-driven automation can reduce the need for human involvement in religious rituals and practices, potentially leading to a dilution of the spiritual experience and a weakening of traditional religious practices.

Moral and Ethical Dilemmas
AI can present moral and ethical challenges that might conflict with religious teachings. For instance, decisions made by AI in healthcare or law enforcement can raise questions about accountability, justice, and the sanctity of life.

Erosion of Community
The communal aspect of religion, which involves gathering for worship, rituals, and social support, could be undermined if AI-driven virtual services replace in-person religious gatherings.

Challenges to Authority
AI can challenge traditional religious authorities by providing alternative interpretations of religious texts or by facilitating new forms of religious expression that may not align with established doctrines.

Loss of Human Connection
The personal and emotional aspects of religious counselling and guidance might be compromised if replaced by AI-driven chatbots or virtual assistants, which lack the ability to provide genuine empathy and understanding.

Secularization
The integration of AI into daily life can contribute to a more secular worldview, where reliance on technology reduces the perceived need for spiritual guidance and religious belief.

Data Privacy Concerns
The use of AI in religious contexts, such as apps for meditation, prayer, or religious study, can raise concerns about the privacy of sensitive religious data and how it might be used or misused.

Artificial Spirituality
The development of AI that simulates spiritual experiences or offers pseudo-religious services can create a superficial form of spirituality that lacks the depth and authenticity of traditional religious experiences.

Impact on Religious Leaders
AI could undermine the role of religious leaders by providing automated responses to religious questions, potentially diminishing the perceived value and authority of these leaders.