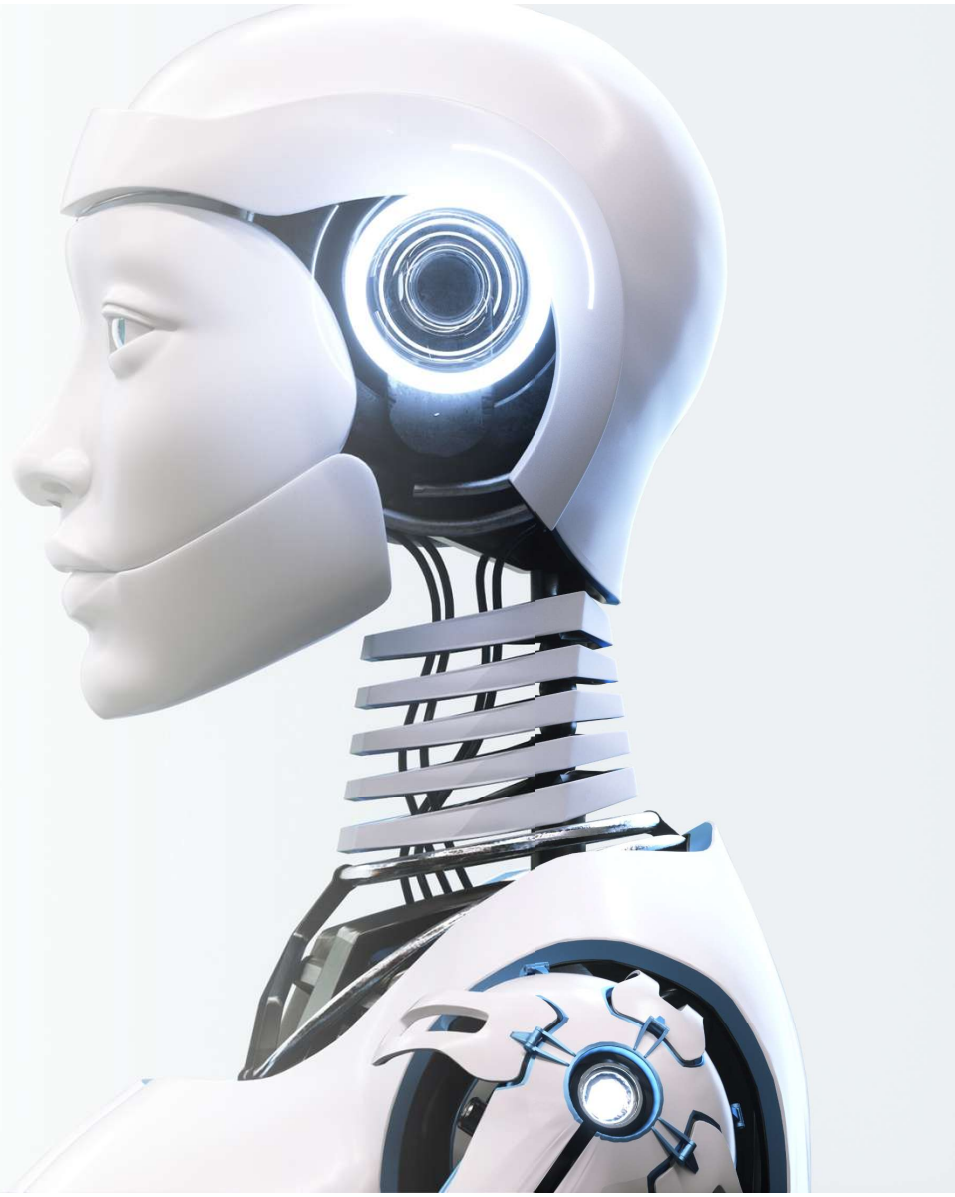
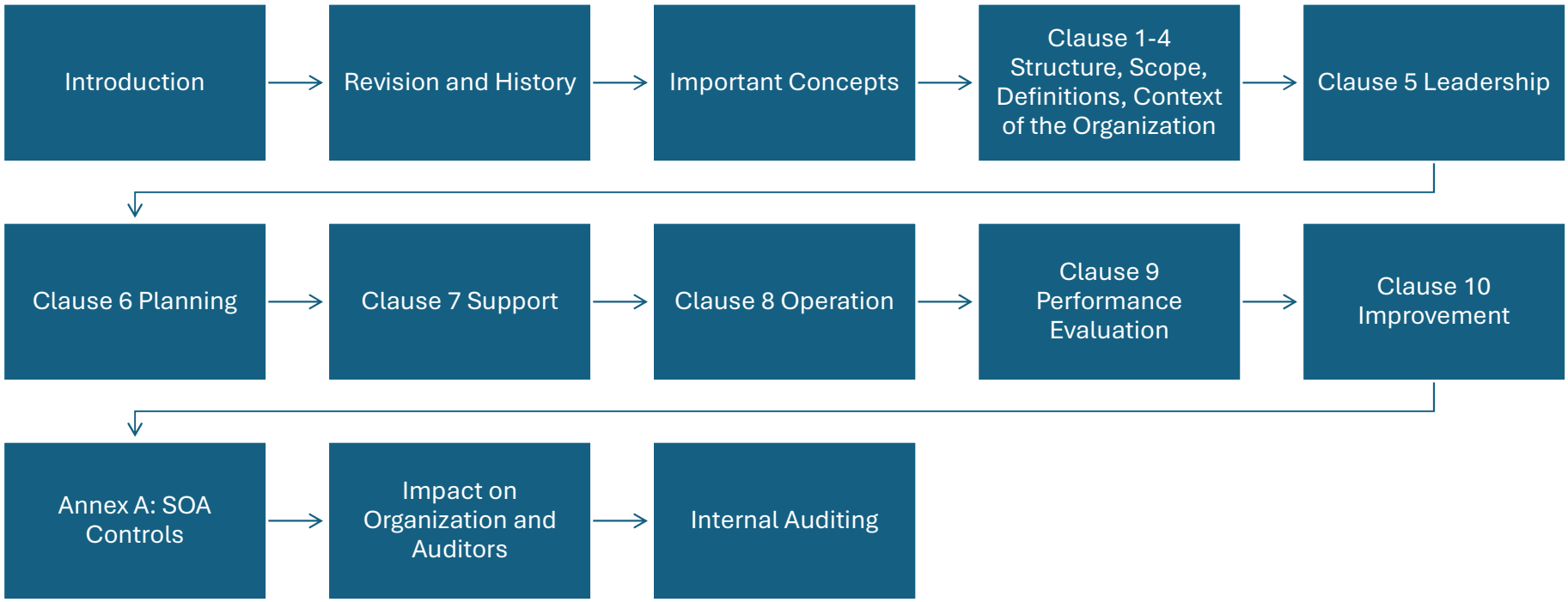
Free ISO 42001:2023 Internal Auditor Training

From Quality Asia Certifications Private Limited

QUALITY ASIA



Structure of the Course



QUALITY ASIA

Objectives of the course

- Gain a clear understanding of the clauses and AI-specific requirements of ISO 42001:2023.
- Interpret AIMS requirements and apply them within the organization's AI lifecycle and context.
- Understand how to assess the effectiveness of an AIMS in managing AI risks, ethics, and impacts.
- Learn auditing principles, techniques, and practices based on ISO 19011:2018 tailored for AI systems.
- Support the organization in ensuring responsible, transparent, and continual improvement in its AI systems.

Trainer Introduction

QUALITY ASIA

- **Mr. Atul Suri**
- BE (Electrical), MBA
- Certified Lead Auditor:
  - ISO 9001, 14001, 45001, 50001, 22000, 27001, 13485, and 26000
- BEE Certified Energy Auditor (CEA)
- Professional Experience:
  - 30+ Years in the industry, with a strong foundation in engineering and management.
  - 20+ Years as a seasoned Management Systems Auditor and Trainer, delivering expertise across multiple sectors.
- Worked with Various Top Notch Certification Bodies as a Lead Auditor and Reviewer like Quality Asia, Intertek, Apave, Moody International, IRQS, etc

About Quality Asia

QUALITY ASIA

Mission: To empower organizations with world-class quality standards and sustainable practices.

Vision: To be the leading provider of quality assurance and certification solutions in India.

NABCB accredited: Quality Asia is accredited by the National Accreditation Board for Certification Bodies (NABCB), which means that their certifications are recognized internationally.

Ethical Certifications: We are committed to providing 100% audit and compliance services, ensuring transparency and integrity in every certification we issue.

Comprehensive Expertise: We specialize in ISO 27001, ISO 9001, ISO 14001, and more, offering a full spectrum of certification services tailored to your organization's needs.

Free ISO Internal Auditor Training: We empower your team with free training, helping you build internal expertise and maintain compliance with international standards.

Global Reach, Local Touch: Serving clients across multiple Indian cities and international locations, we combine global expertise with personalized local service.

Commitment to Excellence: Our mission is to support businesses in achieving and maintaining their certification, unlocking new opportunities and improving operational efficiency.

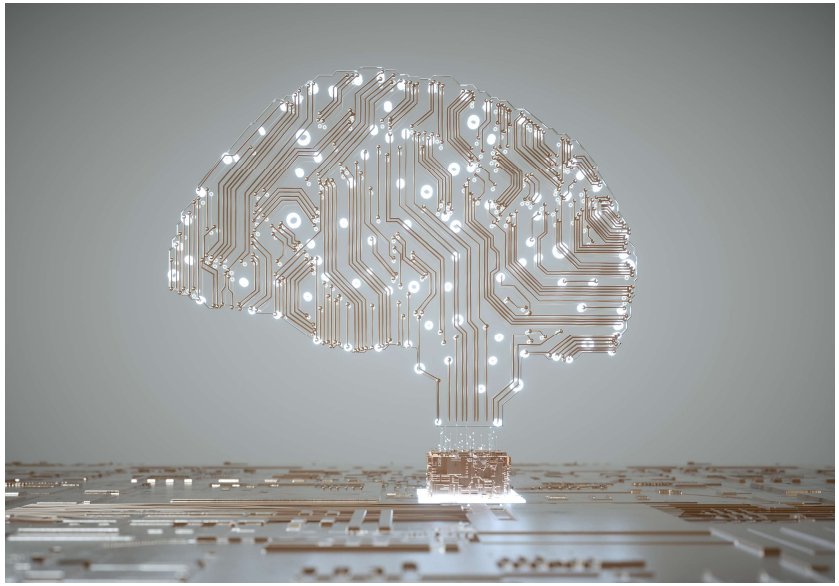
ABOUT FREE LIVE INTERNAL AUDITOR PROGRAM

QUALITY ASIA

Monthly Training Programs	We offer a focused training session on a different ISO standard each month, ensuring continuous learning and up-to-date knowledge for your team.
Flexible Learning Options	Missed a session? No problem! Our training programs are available for later viewing through the Quality Asia School on our website, allowing you to learn at your own pace. Log on to our Quality Asia website.
Our Mission	We are dedicated to increasing awareness about ISO standards and enhancing internal auditor competence. Our goal is to uplift industry operational standards by empowering professionals with the knowledge and skills they need to drive excellence in their organizations.

The Rise of AI

- **30th November 2022** is recognized as a canon event in the world of digital technology. It's the day when OpenAI's ChatGPT was launched, a free chatbot that presented a conversational form of artificial intelligence to the general public.
- The ability to easily interact with large language models has upended corporate strategies
  - introducing new business models and threatening existing ones
  - and has had a profound impact on jobs, entertainment, cybersecurity, and many other sectors of society.



QUALITY ASIA

Global Reactions and the Birth of ISO 42001

- The mix of opportunities and threats has expectedly triggered various reactions as people wonder whether generative AI will take over the world.
- The EU AI Act is one such reaction. Here, nations are seeking to regulate such technology in order to:
  - Drive responsible use.
  - Limit risks from the dangers it poses.
- The world's body of standards organizations has also not been left behind. In December 2023, the first AI management system standard was published: ISO 42001.

Purpose of ISO/IEC 42001:2023

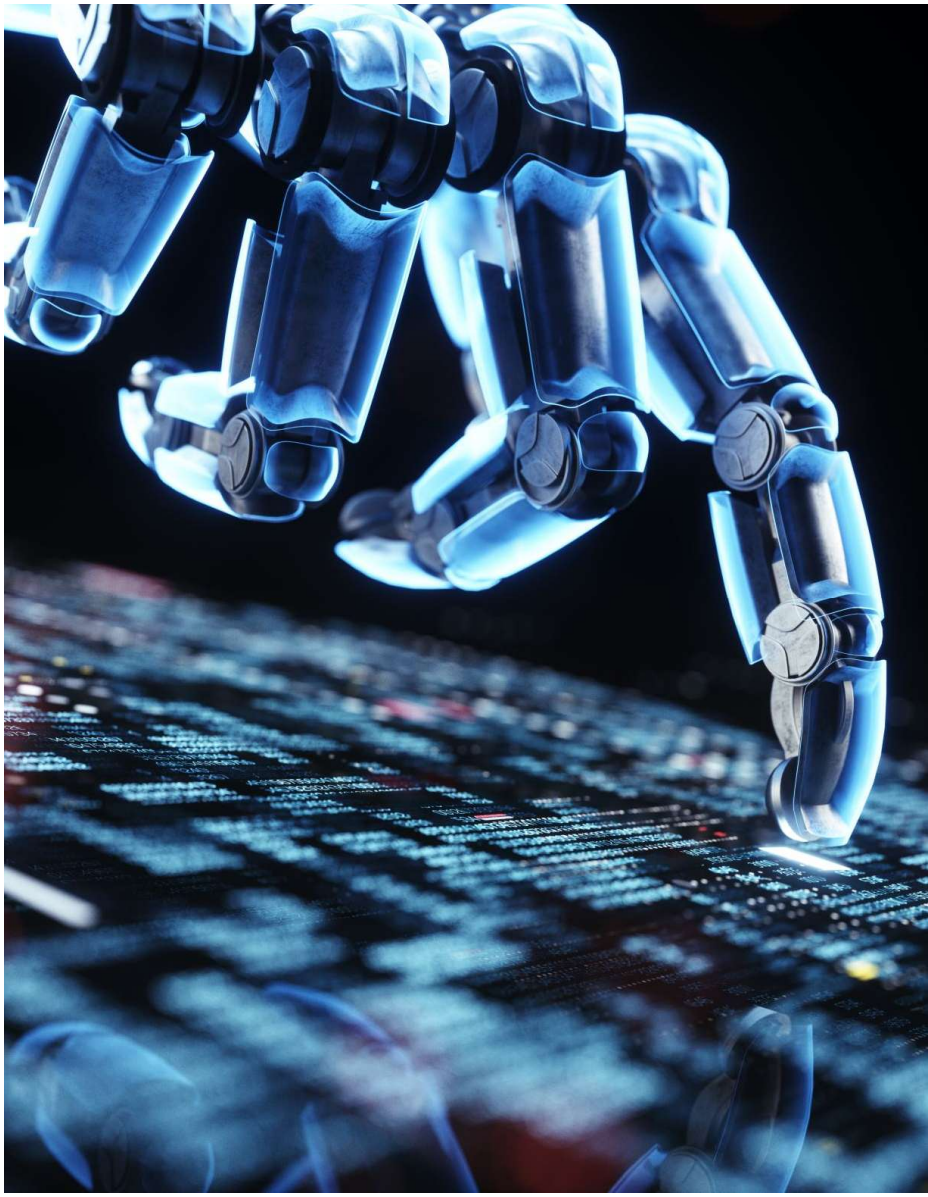
- Establish, implement, maintain, and continually improve an Artificial Intelligence Management System (AIMS).Balance innovation with governance.
- Address unique AI challenges such as:
  - Ethical considerations
  - Transparency
  - Continuous learning and improvement

ISO/IEC 42001:2023 Artificial Intelligence Management System

What is Artificial Intelligence?

Artificial Intelligence (AI)

- AI refers to computer systems or machines that can perform tasks that normally require human intelligence. These tasks include:
  - Learning from data (Machine Learning)
  - Solving problems
  - Recognizing speech and images
  - Making decisions
  - Understanding and generating language
- **Examples**: Chatbots, recommendation systems (Netflix, Amazon), autonomous cars, AI assistants.



ISO 42001:2023 Artificial Intelligence Management System

- ISO 42001:2023 is the world's first international standard for managing Artificial Intelligence (AI) systems. It provides a framework for establishing, implementing, maintaining, and continually improving an AI Management System (AIMS). The standard ensures:
  - Responsible and ethical use of AI
  - Transparency, accountability, and human oversight
  - Management of AI-related risks and impacts

QUALITY ASIA

What is an AI Management System (AIMS)?

An **Artificial Intelligence Management System (AIMS)** is a structured framework that enables an organization to:

- **Design, develop, deploy, and manage AI systems** responsibly
- Address **ethical, legal, and social implications** of AI
- Ensure AI is **transparent, fair, secure, and auditable**
- It includes **policies, procedures, roles, risk controls**, and **monitoring mechanisms**.

Importance of ISO 42001:2023

- **First-ever ISO standard** specifically for managing AI risks and governance
- Enables **responsible use of AI** aligned with legal, societal, and customer expectations
- Builds **trust and accountability**
- Supports **compliance** with upcoming AI regulations (e.g., EU AI Act)
- Promotes **continual improvement** of AI systems

Roles of Organizations in an AI Ecosystem

Role Type	Examples & Responsibilities
AI Providers	Organizations that supply AI systems or platforms to others (e.g., AI SaaS providers, platform vendors)
AI Producers	Individuals or teams involved in the **design, development, testing, deployment, and maintenance** of AI systems. Includes: Developers, Designers, Operators, Evaluators, Human factor professionals, Impact assessors, Governance professionals.
AI Customers / Users	Organizations or individuals using AI in their business operations, products, or services. Responsible for proper use, monitoring, and human oversight.
AI Partners	System integrators, cloud hosts, data providers, annotation vendors — entities that support AI systems indirectly.
AI Subjects	Individuals affected by the AI system — such as **data subjects** or people impacted by AI-driven decisions (e.g., credit scoring, hiring).
Relevant Authorities	Policymakers, regulators, or statutory bodies overseeing AI compliance, ethics, or legal frameworks.

An organization may take on **multiple roles** simultaneously — e.g., a company might be an AI producer and user at the same time.

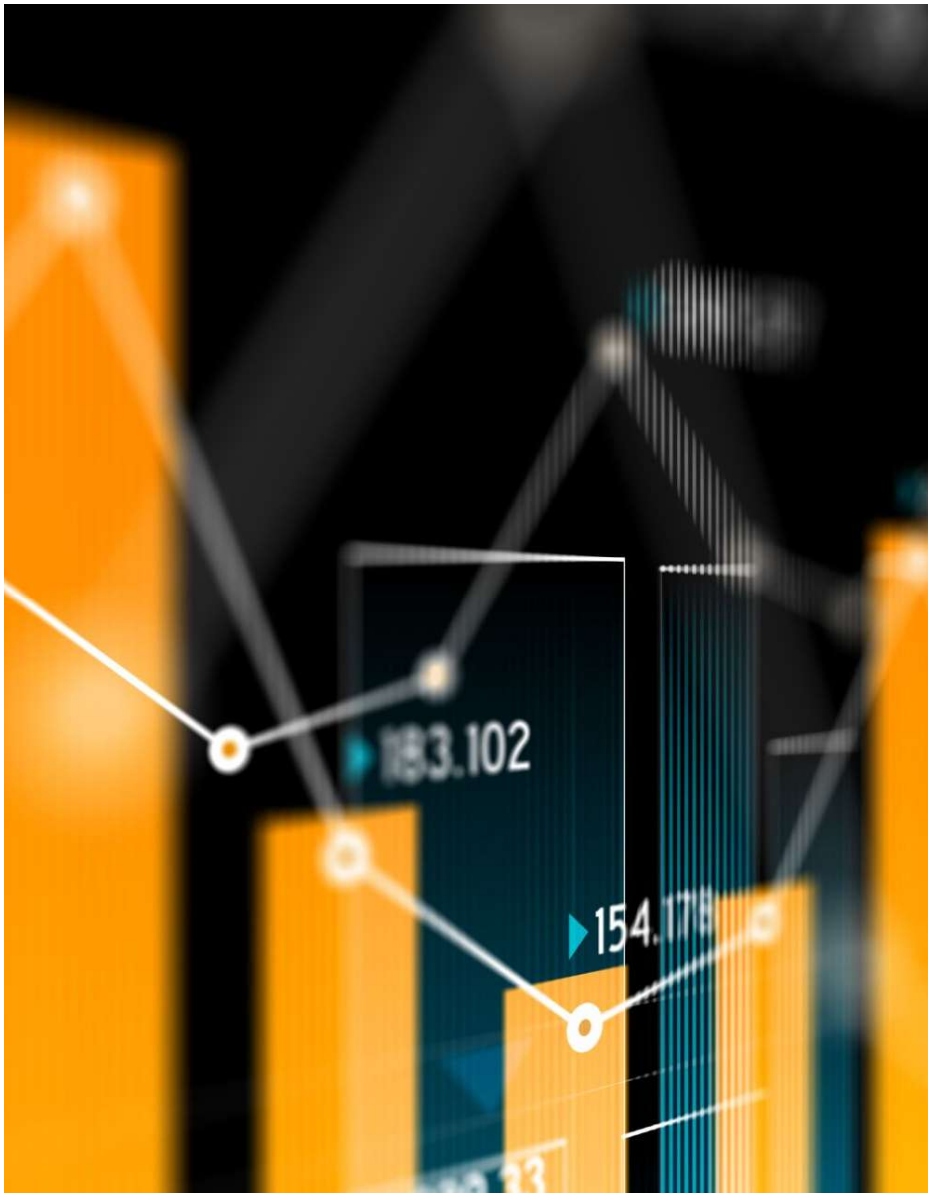
The EU AI Act – Overview

- First comprehensive AI-specific regulation introduced by the European Union.
  - To promote safe, trustworthy, and ethical AI across Europe and globally.
  - Covers the entire AI lifecycle — development, deployment, and use.
  - Categorizes AI systems into **unacceptable risk**, **high risk**, **limited risk**, and **minimal risk**.
  - Expected to set a **global benchmark** for AI governance, influencing other countries' regulations.

EU Artificial Intelligence Act

The AI Act classifies AI according to its risk:

- Unacceptable risk is prohibited (e.g. social scoring systems and manipulative AI).
- Most of the text addresses high-risk AI systems, which are regulated.
- A smaller section handles limited risk AI systems, subject to lighter transparency obligations: developers and deployers must ensure that end-users are aware that they are interacting with AI (chatbots and deepfakes).
- Minimal risk is unregulated (including the majority of AI applications currently available on the EU single market, such as AI enabled video games and spam filters – at least in 2021; this is changing with generative AI).



QUALITY ASIA

The majority of obligations fall on providers (developers) of high-risk AI systems

- Those that intend to place on the market or put into service high-risk AI systems in the EU, regardless of whether they are based in the EU or a third country.
- And also, third country providers where the high-risk AI system's output is used in the EU.

QUALITY ASIA

Deployers are natural or legal persons that deploy an AI system in a professional capacity, not affected end-users.

- Deployers of high-risk AI systems have some obligations, though less than providers (developers).
- This applies to deployers located in the EU, and third country users where the AI system's output is used in the EU.

General purpose AI (GPAI)

- All GPAI model providers must provide technical documentation, instructions for use, comply with the Copyright Directive and publish a summary about the content used for training.
- Free and open license GPAI model providers only need to comply with copyright and publish the training data summary, unless they present a systemic risk.
- All providers of GPAI models that present a systemic risk – open or closed – must also conduct model evaluations, adversarial testing, track and report serious incidents and ensure cybersecurity protections.

Examples of Prohibited AI Systems (Art. 5)

AI manipulating user behavior subliminally.

Social scoring systems.

Emotion recognition in workplaces and schools.

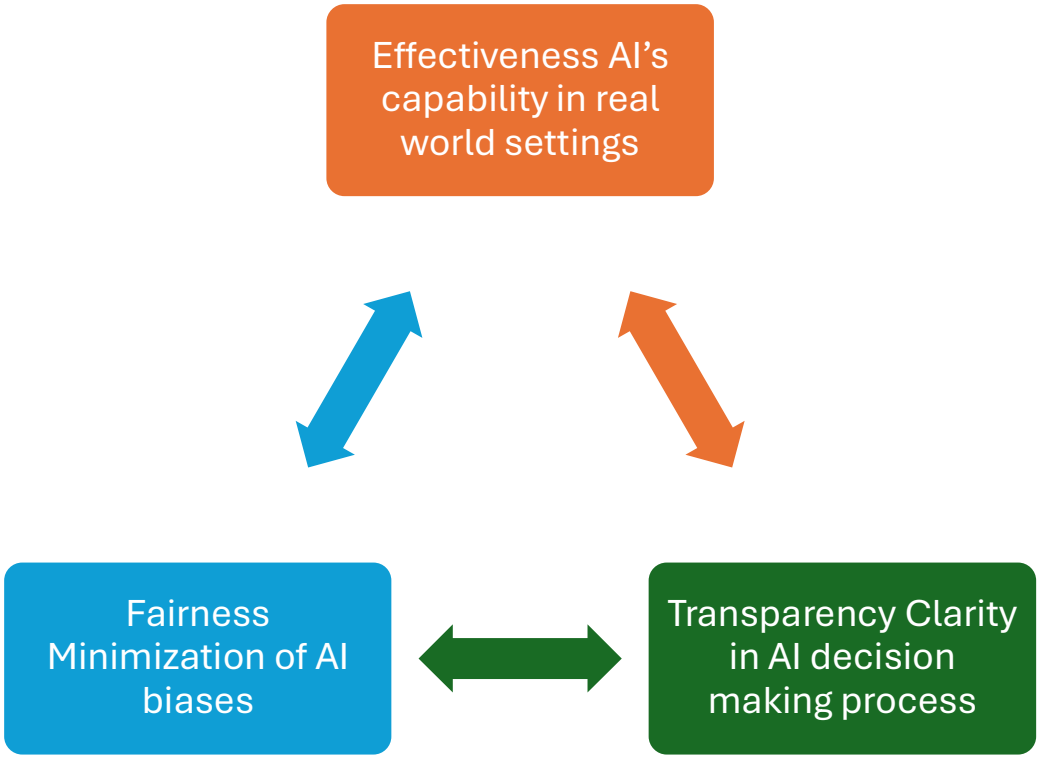
Unlawful real-time remote biometric identification in public spaces.

High Risk AI Systems (Annex III)

- Biometric identification systems
- Critical infrastructure management
- Education and vocational training assessments
- Employment and recruitment AI systems
- Law enforcement profiling
- Migration and border control decision-making
- Administration of justice AI applications

QUALITY ASIA

What are the benefits of implementing



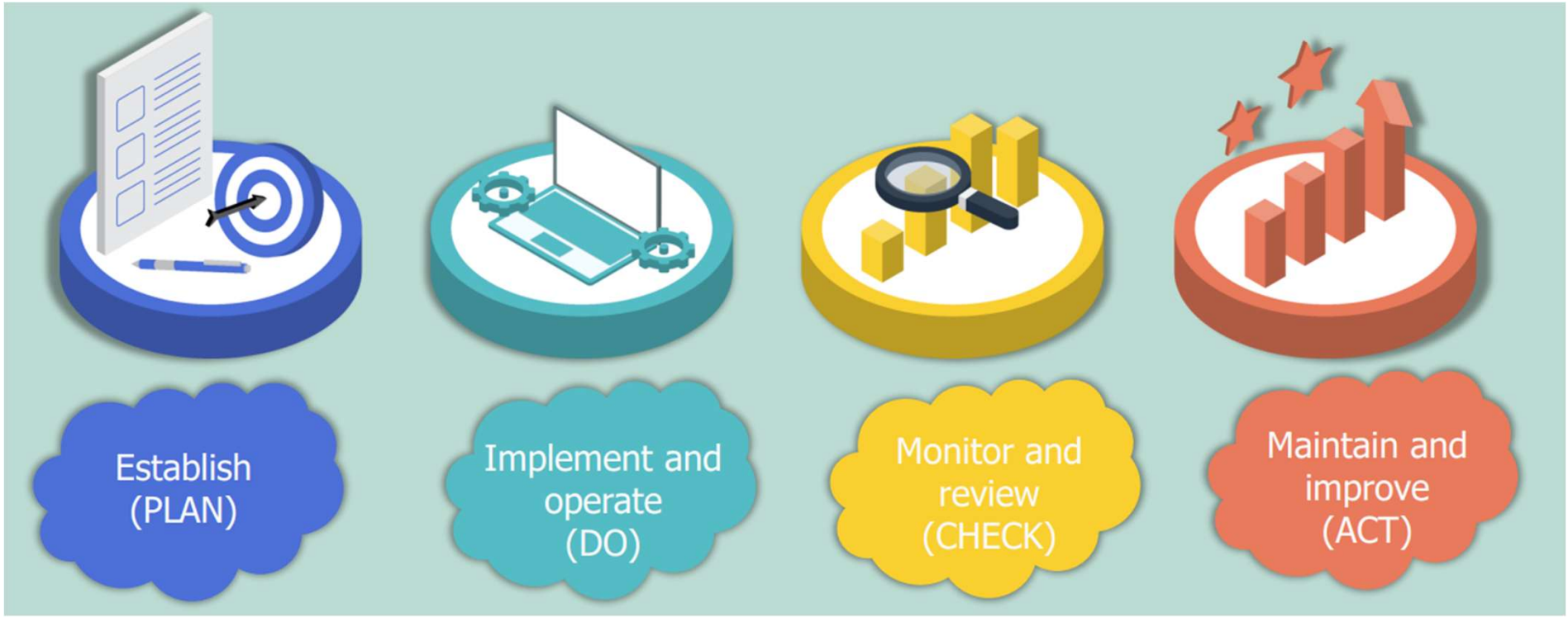
What do we mean by key benefits of an AIMS?

The benefits of effective, transparent and fair AIMS

- Brand strength
- Cost efficiency
- Customer loyalty
- Revenue and profit growth
- Employee morale
- Attracting new customers

Key concepts (1): Risk-based approach

- Effect
  - A deviation from the expected – positive or negative
- Uncertainty
  - Information related to knowledge of an event



PDCA and AIMS

Scan the QR or use link to join

Copy link

0 response submitted

What does AIMS stand for?

- Artificial Intelligence Management System
- Automated Internal Management System
- Advanced Innovation Monitoring System
- Artificial Integrated Management Service

Treemap | Bar

1 of 5

Show correct answer

Structure of ISO 42001

1. **Scope**
2. **Normative Reference**
3. **Terms and definitions**
4. **Context of the organization**
   (4.1 Understanding organization and its context, 4.2 Understanding the needs and expectations of interested parties, 4.3 Determining the scope of the AIMS, 4.4 Artificial Intelligence MS)
5. **Leadership**
   (5.1 Leadership and Commitment , 5.2 AI Policy, 5.3 Roles, responsibilities and authorities)
6. **Planning**
   (6.1 Actions to address risks and opportunities, 6.2 AI objectives and planning to achieve them, 6.3 Planning of changes)
7. **Support**
   (7.1 Resources, 7.2 Competence, 7.3 Awareness, 7.4 Communication, 7.5 Documented information)
8. **Operation**
   (8.1 Operational planning and control , 8.2 AI risk assessment, 8.3 AI risk treatment, 8.4 AI system impact assessment)
9. **Performance evaluation**
   (9.1 Monitoring, measurement, analysis and evaluation, 9.2 Internal audit, 9.3 Management review)
10. **Continual Improvement**
    (10.1 Continual improvement, 10.2 Nonconformity and corrective action)

Clause 1-3

Scope

- Establish, implement, maintain and continually improve an AIMS, Intended 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.

Normative Reference

- Normative references cites ISO/IEC 22989 as indispensable for its application

Terms and Definitions

- Terms, definitions and concepts from ISO/IEC 22989 are used in ISO/IEC 42001

Clause 4 Context of the organization

4.1 Understanding organization and its context

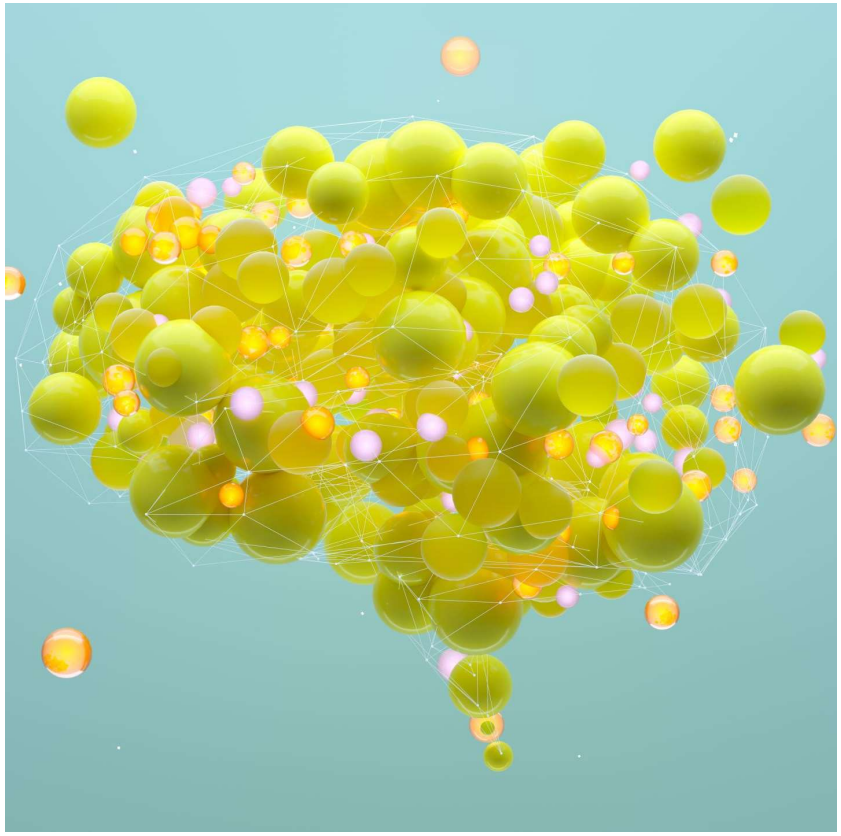
4.2 Understanding the needs and expectations of interested parties

4.3 Determining the scope of the AIMS

4.4 Artificial Intelligence MS)

4.1 Understanding organization and its context

- Identify **external and internal issues** relevant to your **purpose** and that impact the ability to achieve intended outcomes of the **AI Management System (AIMS)**.
- Consider the **intended purpose of AI systems** developed, provided, or used.
- Determine **organizational roles** related to AI systems.
- Both the external and the internal issues will change over time, the issues and their influence on the scope, constraints and requirements of the AIMS should be reviewed regularly



External Factors to Consider:

- **Legal Requirements:** Identify relevant laws or regulations governing AI use (e.g., restrictions on facial recognition, AI in finance or healthcare).
- **Regulatory Policies:** Stay updated with evolving policies and interpretations from regulators shaping AI practices and compliance obligations.
- **Ethical & Societal Norms:** Account for fairness, transparency, accountability, and cultural sensitivities in the deployment and use of AI.
- **Competitive Landscape:** Evaluate innovation trends and benchmark against peers to position AI capabilities strategically and responsibly.

QUALITY ASIA

Internal Factor to consider

- **Organizational Governance & Objectives:** Align AI governance frameworks, objectives, and policies with overall organizational goals to support responsible AI usage.
- **Contractual Obligations:** Ensure compliance with AI-related requirements in contracts with customers, vendors, or data partners (e.g., SLAs, security, or data ethics clauses).
- **Intended Purpose of AI Systems:** Define whether the AI is used for internal operations or offered externally as a product/service, which influences system design, risk, and oversight.

CLIMATE ACTION CHANGES

- The organization shall determine whether climate change is a relevant issue (for its context)

QUALITY ASIA

4.2 Understanding the needs and expectations of interested parties

The organization shall determine:

- The **interested parties** relevant to the AI Management System (AIMS)
- The **requirements** (needs/expectations) of these interested parties
- **Which requirements** will be addressed through the AIMS

QUALITY ASIA

Who Are Interested Parties?

- Customers and end-users
- AI subjects (data subjects, impacted individuals)
- Employees and AI developers
- Regulators and legal authorities
- Vendors, partners, and data providers
- Society/community
- Environmental stakeholders (for climate-related AI risks)

Examples of Needs & Expectations of Interested Parties

Interested Party	Needs & Expectations
Customers / Clients	Reliable and explainable AI outputs, privacy protection, fair outcomes, compliance with regulations
End-Users	Ease of use, transparency of AI decisions, ability to contest automated decisions, no discrimination
Regulators / Authorities	Legal compliance, ethical AI use, banned-use adherence, responsible data handling, climate impact disclosure
Employees / Developers	Clear responsibilities, training in AI ethics & risk, safe working environment
AI Subjects (e.g., data subjects)	Data privacy, opt-in/consent mechanisms, fair treatment, no bias or harm
Vendors / Data Providers	Contractual clarity, secure data exchange, defined AI integration scope
Community / Society	Environmentally safe AI use, social justice, avoidance of harmful AI deployment, **climate-friendly tech**
Top Management / Owners	AI aligned with business objectives, cost-effectiveness, reputation protection

CLIMATE ACTION CHANGES

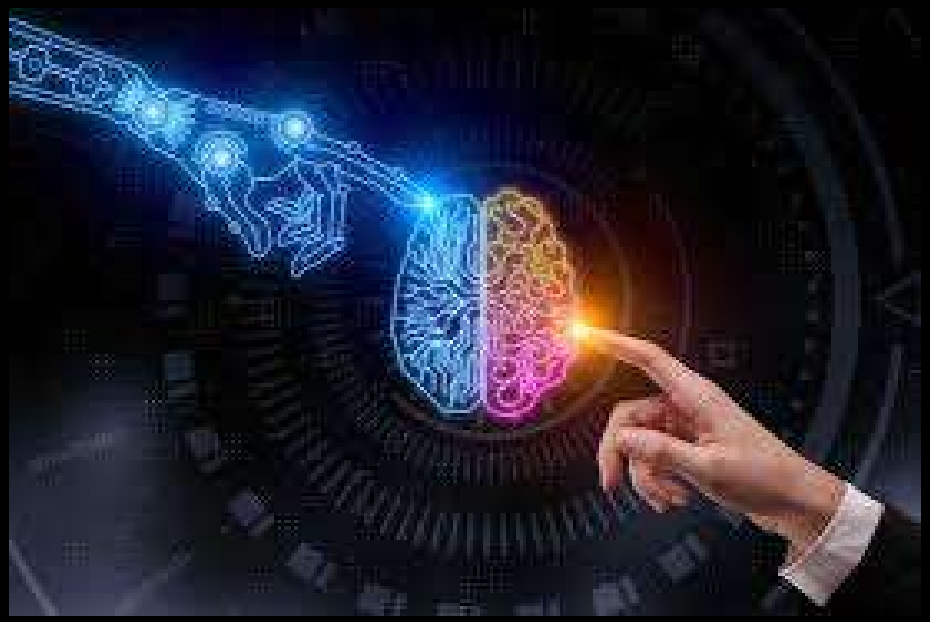
- Interested parties can have requirements related to climate change

4.3 Determining the scope of the AIMS

- Determined '**issues**' and '**requirements**' to be considered when determining the boundaries and applicability of its AIMS
- The **boundaries and applicability** of the AIMS
- The **AI systems**, processes, departments, and locations covered by the management system
- The **activities** involved (e.g., development, deployment, monitoring of AI systems)
- Be available as **documented information**

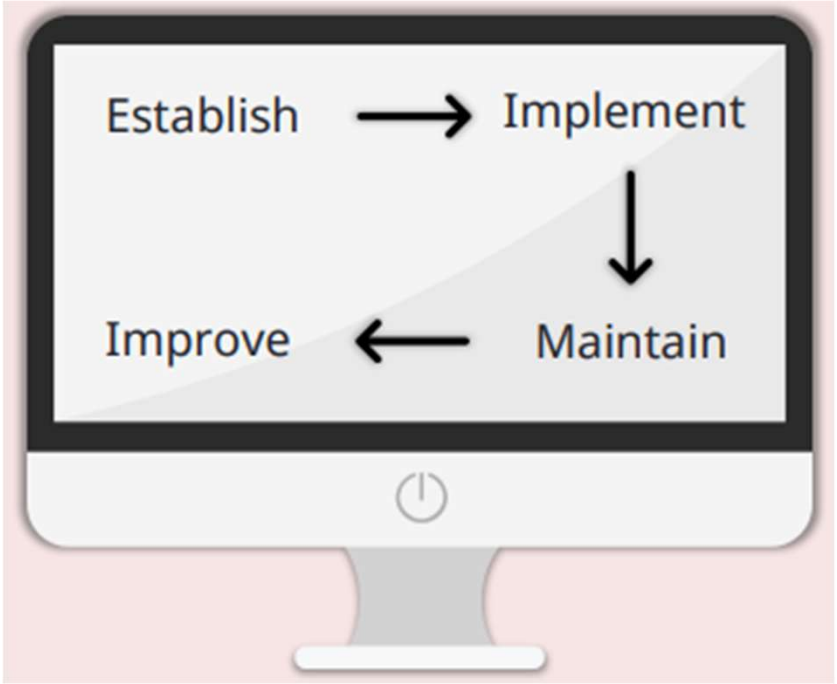
Sample Scope Statement

- “The AI Management System of XYZ Ltd. covers the development, deployment, and maintenance of AI-based financial decision systems across its Bangalore and Pune offices. It addresses risks, ethical use, data protection, and continuous monitoring of AI models.”



4.4 AI management system

- The organization shall establish, implement, maintain, continually improve and document an AI management system, including the processes needed and their interactions, in accordance with the requirements of this document.



Recapitulation – Clause 4

- **Identify Factors Influencing the AI Management System (AIMS):**
  Legal, regulatory, ethical, technological, market, and organizational factors impacting AI systems.
- **Recognize Relevant Interested Parties:**
  Customers, users, employees, regulators, suppliers, and society — and their AI-related needs and expectations, including privacy, transparency, fairness, and compliance.
- **Define the Scope and Applicability of the AIMS:**
  Determine the boundaries considering internal/external issues, compliance obligations, AI systems covered, and stakeholder requirements.
- **Commit to Continuous Improvement:**
  Establish, implement, maintain, and continually enhance the AIMS to achieve ethical AI objectives, risk management, and societal trust.

Scan the QR or use link to join

https://forms.office.com/r/aSWZnYz4Ap

Copy link

0 response submitted

What must an organization consider when understanding its context under ISO 42001?

Legal, regulatory, ethical, and competitive factors	Only financial and marketing strategies	Only product development speed	Only customer demographics

Treemap | Bar

1 of 5

Show correct answer

Clause 5
Leadership

5.1 Leadership and Commitment

5.2 AI Policy

5.3 Roles, responsibilities and authorities

5.1 Leadership and commitment

- Ensure that an **AI policy** and **AI objectives** are established and aligned with strategic direction.
- Integrate the **AI Management System** into core business processes.
- Ensure availability of **necessary resources** for the AIMS.
- **Communicate** the importance of effective AI management and compliance with requirements.
- Ensure the AIMS achieves its **intended results**.
- **Direct and support** people to contribute to the system's effectiveness.
- Promote **continual improvement** of the AIMS.
- **Support key roles** in demonstrating leadership relevant to their responsibilities.

5.2 AI Policy

- Appropriate to the **purpose of the organization**
- A framework for setting **AI objectives** (see Clause 6.2)
- A commitment to **applicable legal, regulatory, and ethical requirements**
- A commitment to **continual improvement** of the AI Management System

The AI Policy must:

- Be available as **documented information**
- Align with and **refer to other organizational policies**
- Be **communicated** within the organization
- Be **accessible to interested parties**, as appropriate

5.3 Roles, responsibilities and authorities

- The top management shall ensure that responsibilities and authorities for relevant AI roles are clearly assigned and properly communicated within the organization.
  - Ensuring the **AI Management System conforms** to ISO 42001 requirements.
  - **Reporting** on the performance of the AI Management System to top management.

Recapitulation – Clause 5

- **Demonstrate Leadership and Commitment:**
  Top management must actively promote AI governance, accountability, and responsible AI practices across the organization.
- **Establish AI Management System Policy:**
  Develop and communicate a clear AIMS Policy aligned with the organization's purpose, ensuring commitment to ethical use, continual improvement, and compliance with AI regulations.
- **Assign Organizational Roles and Responsibilities:**
  Define, assign, and communicate responsibilities and authorities for ensuring the AIMS meets its requirements, including roles for AI risk management, ethics, security, and impact assessments.
- **Promote Accountability and Resources:**
  Ensure availability of necessary resources, competencies, and mechanisms for AI governance, risk management, monitoring, and continual learning.

Scan the QR or use link to join

https://forms.office.com/r/r9Uen9vwjR

Copy link

0 response submitted

Who is responsible for demonstrating leadership and commitment for AIMS?

Treemap | Bar

1 of 5

Show correct answer

Clause 6
Planning

6.1 Actions to address risks and opportunities

6.2 AI objectives and planning to achieve them

6.3 Planning of changes

6.1 Actions to address risks and opportunities

- 6.1.1. General
- 6.1.2. AI risk assessment
- 6.1.3. AI risk treatment
- 6.1.4. AI system impact assessment

6.1.1. General

01

Help ascertain the risks and opportunities that must be addressed

- Guarantee the AIMS meets its intended objectives
  Mitigate or curb undesired impacts
  Foster ongoing improvement

02

Manage AI risk effectively

- Distinguish acceptable vs. non-acceptable risks
- Perform AI risk assessments
- Conduct risk treatment
- Assess AI-specific impacts

03

Determine the quantum and nature of risks

- Domain and context of the application
- Specific business requirements
- Internal and external contexts

General

- Determine risks and opportunities and plan actions to address them.

How to:

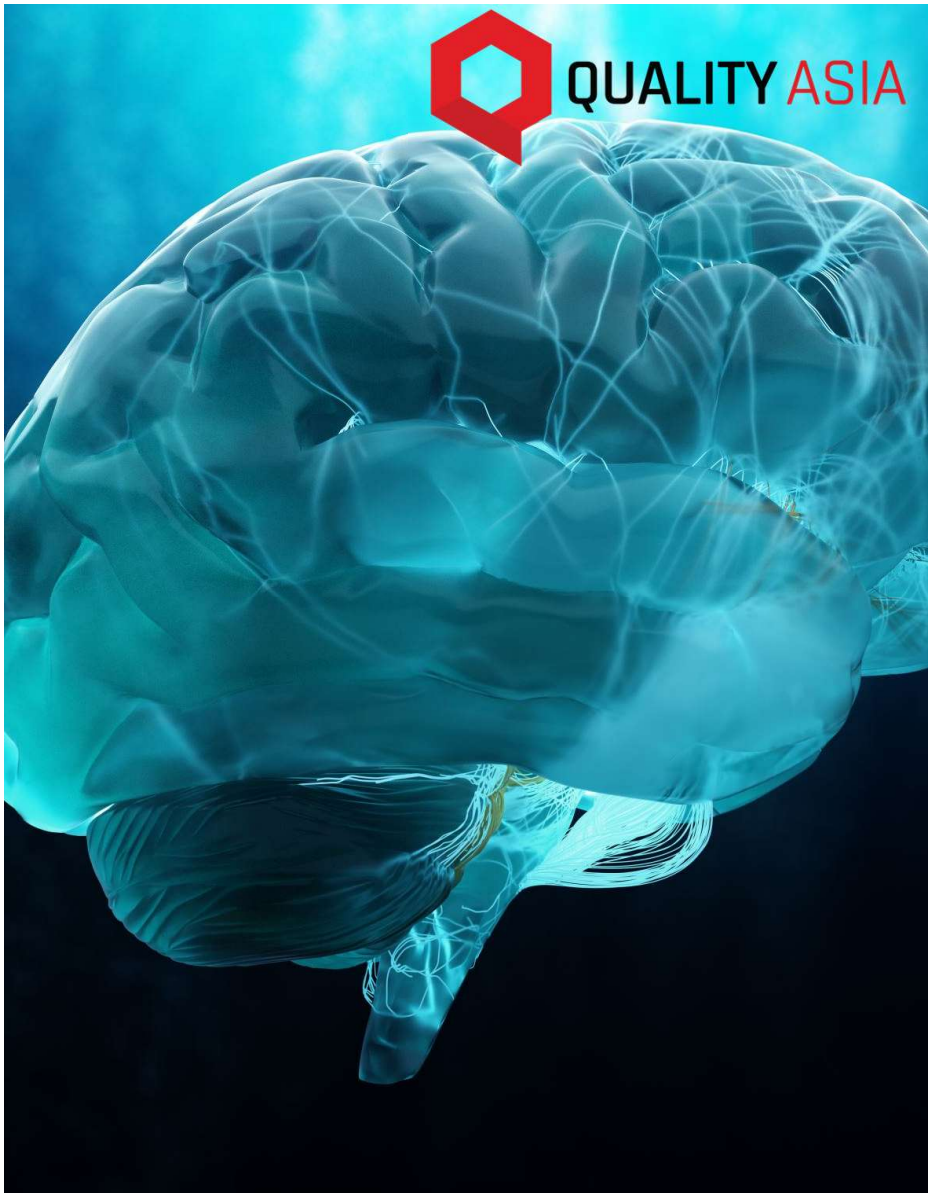
- Integrate these actions into AIMS processes
- **Evaluate** the effectiveness of actions taken
- The organization shall retain documented information on actions taken to identify and address Al risks and Al opportunities.

6.1.2. AI risk assessment

- Define and apply a structured process for **AI risk assessment**
- Align the process with the **AI policy** and **AI objectives**
- Designed to produce **consistent, valid, and comparable** results

AI Risk Assessment

- RISK = Consequences × Likelihood (AI Context)
- Risk assessment must consider:
  - Potential **impact** on the organization, individuals, and society
  - The **realistic likelihood** of the identified AI risks
- Define **criteria** to distinguish:
  - Acceptable vs. unacceptable AI risks



Consequences and Likelihood Definitions for AI

Consequence	Description (AI Context)
Catastrophic	Major harm to public safety, environment, or massive AI failure
Critical	Severe legal/regulatory breach or business disruption
Serious	Financial loss or high operational impact
Significant	Damage to reputation or partial process failure
Minor	Low-impact issues, quickly recoverable
Likelihood	**Description**
Almost certain	Will occur regularly during AI system operations
Very likely	Strong probability based on AI behavior/data patterns
Likely	Can occur under normal conditions
Rather unlikely	Possible but rare in controlled environments
Unlikely	Highly improbable given safeguards in place

Risk Matrix for AI Systems

Likelihood	Consequences				
	Catastrophic	Critical	Serious	Significant	Minor
Almost certain	Very high	Very high	High	High	Medium
Very likely	Very high	High	High	Medium	Medium
Likely	High	High	Medium	Medium	Medium
Rather unlikely	Medium	Medium	Medium	Medium	Low
Unlikely	Medium	Medium	Medium	Low	Low

Risk Identification in AIMS

- Repeated risk assessments should be:
  - **Consistent, Valid, Comparable**
- Use:
  - **Event-based** identification (e.g., AI model drift)
  - **System-based** (e.g., algorithm bias, data poisoning)
- Use AI Impact Assessments (AIIA) where applicable

Risk Ownership in AIMS

- Identify **risk owners**: individuals or functions accountable for monitoring, reporting, and treating AI risks
- Assign ownership across:
  - AI lifecycle stages (development → deployment)
  - Functions (compliance, tech, legal)

Risk Analysis & Evaluation

Risk Analysis:

- Evaluate **consequences** & **likelihood**
- Determine overall **AI risk level**

Risk Evaluation:

- Compare results to defined **AI risk criteria**
- Prioritize for **treatment or acceptance**

- Maintain documented information on the full AI risk assessment process.

6.1.3. AI risk treatment

- **Select** appropriate **AI risk treatment options**
- **Identify and compare** necessary controls (internal + from **Annex A**)
- **Implement** controls aligned with selected treatment options
- **Determine** if additional controls are needed beyond Annex A
- Use **Annex B** for guidance on implementation of controls

Risk treatment options

- Risk avoidance
- Risk acceptance
- Risk reduction or mitigation
- Risk transfer
- Risk increase or risk taking (in case of opportunities)

Developing the AI Risk Treatment Plan

- **Consider** controls from Annex A for implementing treatment options.
- **Consult Annex B** for practical implementation guidance.
- **Produce Statement of Applicability (SoA):**
  - List of necessary controls.
  - Justifications for exclusions and inclusions.
- **Formulate AI Risk Treatment Plan** aligned with objectives (Clause 6.2).

Requirements for the AI Risk Treatment Plan

The Risk Treatment Plan must be:

- Aligned with **organizational objectives** (6.2).
- Documented as **controlled information**.
- **Communicated** within the organization.
- **Available to interested parties**, as appropriate.

Statement of Applicability (SOA for AIMS)

- Document **which controls are included** and why
- Justify **exclusions**, especially if:
  - Risk is not relevant
  - Legal exemptions apply
- Controls may be custom-built or taken from other frameworks

Sample SOA

Control	Topic	Control Requirement	A?	Justification	Implementation Method	Status
A.2.2	AI Policy	The organization shall document a policy for the development or use of AI systems.	A	Required for governance and direction of AIMS.	AI Policy document approved by top management.	Implemented
A.2.3	Alignment with Other Policies	Organization shall determine where AI intersects with other business policies.	A	AI may affect data, ethics, and security policies.	Cross-referencing in Integrated Management System (IMS).	In Progress
A.2.4	Review of AI Policy	Review policy regularly for adequacy and effectiveness.	A	Required for continual improvement.	Annual review during Management Review Meeting.	Planned
A.3.2	AI Roles & Responsibilities	Define and allocate AI-specific roles.	A	Required for role clarity and accountability.	Defined in RACI Matrix and organizational chart.	Implemented
A.3.3	Reporting of Concerns	Process to raise AI-related ethical or safety concerns.	A	Needed for responsible AI use and compliance.	Ethics hotline and whistleblower procedure updated.	In Progress
A.4.2	Resource Documentation	Identify and document resources per AI lifecycle stage.	A	Enables effective planning and control.	AI resource inventory maintained in SharePoint.	Implemented
A.4.3	Data Resources	Document data used in AI systems.	A	Crucial for traceability and data governance.	Dataset logs with metadata maintained in project folders.	In Progress
A.4.4	Tooling Resources	Document AI development tools and platforms.	A	Required for version control and reproducibility.	Git-based tool repository with tool usage logs.	Planned
A.4.5	System & Computing Resources	Document systems and infrastructure used.	A	Required for operational stability and capacity planning.	Resource catalog in IT asset register.	Implemented
A.4.6	Human Resources	Document human competencies and availability.	A	Competency management is key to safe AI operations.	Skill matrix and training records in HRMS.	In Progress

6.1.4. AI system impact assessment

- Define a process to **assess the potential consequences** of AI systems.
- Cover the AI system's:
  - Deployment
  - Intended use
  - Foreseeable misuse

Elements of AI System Impact Assessment

- **Assess consequences** for individuals, groups, and society.
- **Consider technical and societal context** (e.g., laws, cultural impact).
- **Document** the results of the impact assessment.
- **Make available to stakeholders** if required.

Key Requirements

Document	Make	Integrate
Document the impact assessment results	Make results available to interested parties if appropriate	Integrate findings into overall risk assessment (see 6.1.2)

Integration with Risk Management

The AI system impact assessment feeds into the **AI risk assessment** (refer to 6.1.2).

Refer to Table A.1 (e.g., A.5) for relevant controls.

In critical sectors (safety, privacy), perform **specialized impact assessments** as part of overall risk management.

QUALITY ASIA

6.2 AI objectives and planning to achieve them

- Establish **AI objectives** at relevant functions and levels.
- Ensure objectives are:
  - **Consistent** with the AI policy (see 5.2)
  - **Measurable**, where practicable
  - Aligned with **applicable requirements**
  - **Monitored, communicated**, and **updated** as needed
  - Available as **documented information**

Planning to Achieve AI Objectives

- **What** will be done
- **What resources** are required
- **Who** will be responsible
- **When** it will be completed
- **How** results will be evaluated
- Ensure all objective plans are documented and reviewed regularly.

Sample AI Objectives – ISO 42001:2023

S. No.	AI Objective	Target	Timeline	Responsible Person	Remarks
1	Ensure 100% of AI systems undergo risk assessment before deployment	100% coverage of new systems	Ongoing	Risk & Compliance Officer	As per Clause 6.1.2
2	Conduct bias testing and mitigation for all AI models handling personal data	100% of applicable models	Quarterly	Ethical AI Officer	Aligned with fairness and non-discrimination
3	Maintain AI incident log and ensure reporting within 48 hours of detection	100% of incidents logged	Continuous	Information Security Officer	Linked to Clause 8.2 & 10.1
4	Train all AI development team members on responsible AI principles	100% trained with records	Annually	HR & L&D Team	Supports competence and awareness
5	Achieve stakeholder satisfaction score of 90%+ on AI system usability and trust	≥90% positive feedback	Annual survey	Product Owner	Relevant to Clause 9.1
6	Ensure compliance of AI projects with applicable legal and regulatory requirements	100% legal review before go-live	Project-specific	Legal & Compliance	Per Clause 4.2 & 6.1.3

6.3 Planning of changes

- Changes to the AIMS shall be carried out in a **planned manner**, to avoid unwanted consequences.

Recapitulation – Clause 6

Address Risks and Opportunities : Identify risks and opportunities that could impact the achievement of intended outcomes of the AI Management System (AIMS) and take necessary actions to manage them.

Establish AI Objectives : Set measurable, clear, and consistent objectives for the AIMS, ensuring they align with the AIMS Policy, ethical AI principles, and compliance requirements.

Plan Actions for Objectives : Define what will be done, what resources will be required, who will be responsible, timelines, and how results will be evaluated to achieve AIMS objectives.

Plan AI Risk Management : Conduct AI risk assessments, treatments, and impact assessments (such as AI system impact assessment), and retain documented information as evidence of risk handling.

Prepare for Changes : Plan and manage changes to the AIMS proactively, ensuring continuity, compliance, and continuous improvement.

Scan the QR or use link to join

https://forms.office.com/r/aKQXjd0eQP

Copy link

0 response submitted

What must organizations identify when planning for AIMS?

Treemap | Bar

1 of 5

Show correct answer

Clause 7
Support

- 7.1 Resources
- 7.2 Competence
- 7.3 Awareness
- 7.4 Communication
- 7.5 Documented information

7.1 Resources

- Determine and provide the resources needed for the establishment, implementation, maintenance and continual improvement of the AIMS

Types of AI Resources May Include:

- **Human resources** (AI developers, ethics reviewers)
- **Computing infrastructure** (GPU clusters, cloud environments)
- **Data resources** (datasets, sources, data governance tools)
- **Tooling resources** (frameworks like TensorFlow, PyTorch)
- **Financial resources** (budget allocation for responsible AI)

7.2 Competence

- **Define the necessary competence** for personnel performing tasks that affect AI system performance
- Ensure competence through appropriate **education, training, or experience**
- Take actions, where needed, to **acquire or improve competence**, and evaluate the **effectiveness** of these actions
- Retain **documented evidence of competence**

7.3 Awareness

Personnel working under the organization's control shall be aware of:

- The **AI policy** (refer Clause 5.2)
- Their **contribution** to the effectiveness of the AI management system – including benefits such as improved AI performance and responsible use
- The **implications of not conforming** to the AI management system requirements

7.4 Communication

- Determine the need for internal and external communications relevant for the AIMS, including
- **On what?**
- **When?**
- **With whom?**
- **How?**

7.5 Documented information

The AI Management System documentation shall include:

- **Documents required** by ISO/IEC 42001:2023
- **Documents determined necessary** by the organization for the effective functioning of AIMS

Extent of documentation may vary based on:

- The size and complexity of the organization
- The nature of AI activities, products, and services
- The competence of personnel involved

7.5.2 Creating and Updating AIMS Documents

Ensure proper creation and maintenance of documents:

- **Identification and description** (e.g. title, date, reference number)
- **Format and media** (e.g. language, software version, paper/electronic)
- **Review and approval** for **suitability** and **adequacy**

7.5.3 Control of Documented Information

Control measures shall ensure that information is:

- **Available and suitable** when and where needed
- **Protected** against loss of confidentiality, improper use, or integrity issues

Control of documented information

- Distribution
- Access
- Retrieval
- Use
- Storage and preservation
- Version control
- Retention
- Secure disposition

Recapitulation – Clause 7

- **Resources Management:**
  Determine and provide adequate resources (people, infrastructure, technology) for establishing, implementing, maintaining, and continually improving the AI Management System (AIMS).
- **Competence:**
  Ensure personnel involved in AI-related tasks are competent based on education, training, and experience. Provide additional training where needed.
- **Awareness:**
  Make employees aware of the AIMS policy, objectives, their contribution to its success, and the consequences of not conforming.
- **Communication:**
  Define and implement effective internal and external communication relevant to the AI Management System, including what to communicate, when, with whom, and how.
- **Documented Information:**
  Maintain necessary documents (like policies, procedures, risk assessments) to support the AIMS, ensure appropriate control of documents (creation, update, protection, retention, disposal), and maintain evidence of operational effectiveness.

Scan the QR or use link to join

https://forms.office.com/r/Z3NT7849Py

Copy link

0 response submitted

What must the organization ensure regarding the competence of personnel?

That they know all products	That they are trained and experienced for AI-related tasks	That they have marketing degrees	That they can operate forklifts

Treemap | Bar

1 of 5

Show correct answer

Clause 8
Operation

8.1 Operational planning and control

8.2 AI risk assessment

8.3 AI risk treatment

8.4 AI system impact assessment

8.1 Operational planning and control

- Plan, implement, and control the processes required to meet AIMS requirements.
- Establish **criteria** for AI-related processes.
- Implement **controls** as per Clause 6 and **evaluate their effectiveness**.
- Maintain documented information to confirm activities were carried out as planned.
- Apply controls to:
  - **AI system development**
  - **AI system usage** across its life cycle
- Address and mitigate unintended consequences of planned changes.
- **Control changes** in the processes or AI system operations.
- **Control externally provided processes, products, or services** relevant to the AI management system.
- Apply **Annex A & B** for reference controls and implementation guidance.

8.2 AI risk assessment

- **Conduct AI risk assessments** at planned intervals (e.g., annually), and whenever significant changes are proposed or occur in the AI system.
- Ensure the AI risk assessment process follows the framework established in **Clause 6.1.2** (AI risk assessment methodology).
- **Document** the results of all AI risk assessments.

AI Risk Assessment – Introduction

- **AI offers major societal benefits**, but it also presents unique risks.
- Regulatory bodies (e.g., **EU AI Act**) emphasize **risk management** as a core of AI governance.
- ISO/IEC 42001:2023 Clause 8.2 requires organizations to:
  - Perform AI risk assessments **at planned intervals** or upon **significant change**.
  - **Document and retain** results for accountability.

AI Risk Assessment – Governance Approach

To align with AI governance best practices, organizations should:

- Identify and **rank AI risks**: unacceptable, high, limited, or minimal.
- **Evaluate likelihood of harm** and potential impact.
- Implement **mitigation measures** as needed.
- Leverage existing risk assessment frameworks (e.g., **NIST**, ISO 27005).
- Ensure compliance with **applicable laws and regulations** (e.g., **EU AI Act**).

Unacceptable (Prohibited) AI Risks

AI activities may be prohibited by law. Examples include:

- **Social scoring** (public/private).
- **Exploitation of vulnerable groups** or subliminal techniques.
- **Real-time remote biometric identification** in public spaces (w/ exceptions).
- **Predictive policing** targeting individuals.
- **Emotion recognition** in work/education (unless for safety/medical).
- **Discriminatory AI** (credit, hiring, housing, etc.).
- **Mass surveillance** or scraping biometric data (CCTV, internet).

High-Risk AI Activities

If not prohibited, assess if the activity is **high-risk**, e.g.:

- **Critical infrastructure**
- **Medical devices and healthcare AI**
- **Biometric surveillance or identification**
- **AI in hiring, lending, education**
- **Law enforcement & border control**
- **Deepfakes and synthetic content**
- **Financial, safety, environmental, or civil rights impact**

Limited & Minimal Risk AI

- **Limited Risk**: e.g., **chatbots** – must inform users they are interacting with AI.
- **Minimal Risk**: e.g., **AI in video games**, general-purpose tools.
- For such systems:
  - **No mandatory mitigation** under EU AI Act.
  - Voluntary **codes of conduct** may still be applied.
  - **Contextual risk elevation** should be considered (e.g., gaming AI used in competitions).

Assessing Likelihood of Harm

- After ranking AI risks, evaluate **probability of harm** (likelihood × severity).
- Use a **Risk Matrix** to categorize:
  - **Critical Risk**
  - **Moderate Risk**
  - **Low Risk**
- Risk may arise from:
  - **Security breaches**
  - **Reputation damage**
  - **Legal liability**
  - **Business disruption**
  - **Harm to individuals or society**

Documenting the AI Risk Assessment

- AI risk assessments should be documented to **demonstrate accountability**.
- Documentation should reflect:
  - Identified risks
  - Mitigation measures taken
  - Assessment of adequacy of measures
- Required by **GDPR (Art. 35)**, **CPRA**, **Colorado**, **Connecticut**, and **Virginia Privacy Acts**.
- Documentation provides legal defensibility and builds trust with stakeholders.

Regulatory Guidance for AI Risk Documentation

Sources for Documentation Best Practices:

- UK ICO: New PIA requirements for AI
- US (Colorado Privacy Act – 4 CCR 904-3-9.06): Profiling PIAs
- California (CPPA under CPRA): Upcoming regulations for AI risk assessments
- 📝 **Tip**: Align your AI risk assessment format with both **local privacy laws** and **industry guidelines**.

Ethical Dimensions of AI Risk Assessment

As per UNESCO Recommendations:

- Consider human rights and fundamental freedoms
- Focus on:
  - Vulnerable groups
  - Environmental and societal impact
  - Citizen participation

Ethical Data Impact Assessment (EDIA) - Hong Kong's Ethical Accountability Framework

- Conduct **EDIA + PIA** for comprehensive coverage
- EDIA scope includes:
  - All types of data (not just personal)
  - Aggregated or anonymized data
- Demonstrates good faith compliance with AI governance expectations

Fundamental Rights Impact Assessment (EU AI Act)

Includes:

- Description of **deployment processes**
- Time and frequency of use
- Categories of people affected
- Specific **risks of harm**
- Human oversight measures
- Mitigation actions for risk events

Continuous Risk Monitoring

Key Principle: Risk assessment is **not a one-time activity**.

Organizations must:

- Monitor emerging risks throughout the AI lifecycle
- Regularly update:
  - Risk registry
  - Controls and mitigation strategies
  - AI use cases and deployment context

Reference Framework for AI Risk Management

- **Based on National Institute of Standards and Technology (NIST)**, US Department of Commerce
- **AI Risk Management Framework (AI RMF) v1.0**

The AI RMF Core provides outcomes and actions for:

- Enabling dialogue on AI risks
- Managing risks across AI system life cycles
- Developing **trustworthy AI** through four core functions:
  - **GOVERN**
  - **MAP**
  - **MEASURE**
  - **MANAGE**

GOVERN Function: Risk Governance for AI

- Cultivates a culture of **AI risk management**.
- Aligns technical aspects with **organizational values**.
- Covers **full AI lifecycle** including third-party systems and data.
- Anticipates and manages AI risks to users and society.
  - **Practices (GOVERN 1–6):**
- Policies, accountability, workforce diversity, stakeholder engagement, supply chain risks.

Govern 1 - 6

- **GOVERN 1:** Policies, processes, procedures, and practices across the organization related to the mapping, measuring, and managing of AI risks are in place, transparent, and implemented effectively.
- **GOVERN 2:** Accountability structures are in place so that the appropriate teams and individuals are empowered, responsible, and trained for mapping, measuring, and managing AI risks
- **GOVERN 3:** Workforce diversity, equity, inclusion, and accessibility processes are prioritized in the mapping, measuring, and managing of AI risks throughout the lifecycle.
- **GOVERN 4:** Organizational teams are committed to a culture that considers and communicates AI risk.
- **GOVERN 5:**Processes are in place for robust engagement with relevant AI actors
- **GOVERN 6:** Policies and procedures are in place to address AI risks and benefits arising from third-party software and data and other supply chain issues.

MAP Function: Contextual Understanding of AI Systems

- Establishes **risk context** across the AI lifecycle.
- Recognizes **interdependencies** between actors, activities, and system parts.
- Frames risks to guide measurement and management actions.
  - **Practices (MAP 1–5):**
- Establish system context
- Categorize the AI system
- Benchmark benefits/costs
- Map third-party risks
- Characterize societal impacts

MAP 1 – 5

- **MAP 1:** Context is established and understood.
- **MAP 2:** Categorization of the AI system is performed.
- **MAP 3:** AI capabilities, targeted usage, goals, and expected benefits and costs compared with appropriate benchmarks are understood
- **MAP 4:** Risks and benefits are mapped for all components of the AI system including third-party software and data
- **MAP 5:** Impacts to individuals, groups, communities, organizations, and society are characterized

MEASURE Function: Risk Evaluation and Monitoring

- **Quantitative, qualitative, or mixed-methods** used to measure AI risks.
- Pre-deployment and post-deployment testing required.
- Focuses on system trustworthiness, social impacts, and human-AI interactions.
  - **Practices (MEASURE 1–4):**
- Select appropriate metrics
- Evaluate trustworthy characteristics
- Track AI risks over time
- Gather feedback for measurement improvement

MEASURE 1-4

- **MEASURE 1:** Appropriate methods and metrics are identified and applied
- **MEASURE 2:** AI systems are evaluated for trustworthy characteristics
- **MEASURE 3:** Mechanisms for tracking identified AI risks over time are in place
- **MEASURE 4:** Feedback about efficacy of measurement is gathered and assessed

MANAGE Function: Risk Response and Improvement

- Allocate risk resources based on mapped and measured results.
- Maintain processes for **incident response**, **recovery**, and **communication**.
- Emphasizes **continual improvement** of AI risk management.
  - **Practices (MANAGE 1–4):**
- Prioritize and manage AI risks
- Maximize benefits, minimize harms
- Manage third-party risks
- Monitor risk treatments regularly

MANAGE 1 – 4

- **MANAGE 1:** AI risks based on assessments and other analytical output from the MAP and MEASURE functions are prioritized, responded to, and managed.
- **MANAGE 2:** Strategies to maximize AI benefits and minimize negative impacts are planned, prepared, implemented, documented, and informed by input from relevant AI actors.
- **MANAGE 3:** AI risks and benefits from third-party entities are managed
- **MANAGE 4:** Risk treatments, including response and recovery, and communication plans for the identified and measured AI risks are documented and monitored regularly

How AI Risks Differ from Traditional Software Risks

Compared to traditional software, AI introduces unique risks:

Bias and poor data quality issues

Data drift, model drift, and concept drift

Use of outdated or detached datasets

Pre-trained models increase bias and reproducibility issues

Opacity in decision-making ("black-box" AI)

Higher privacy risks due to enhanced data aggregation

Frequent need for corrective maintenance

Lack of mature testing and documentation standards

High environmental and computational costs

Difficult-to-predict failure modes and emergent properties

8.3 AI risk treatment

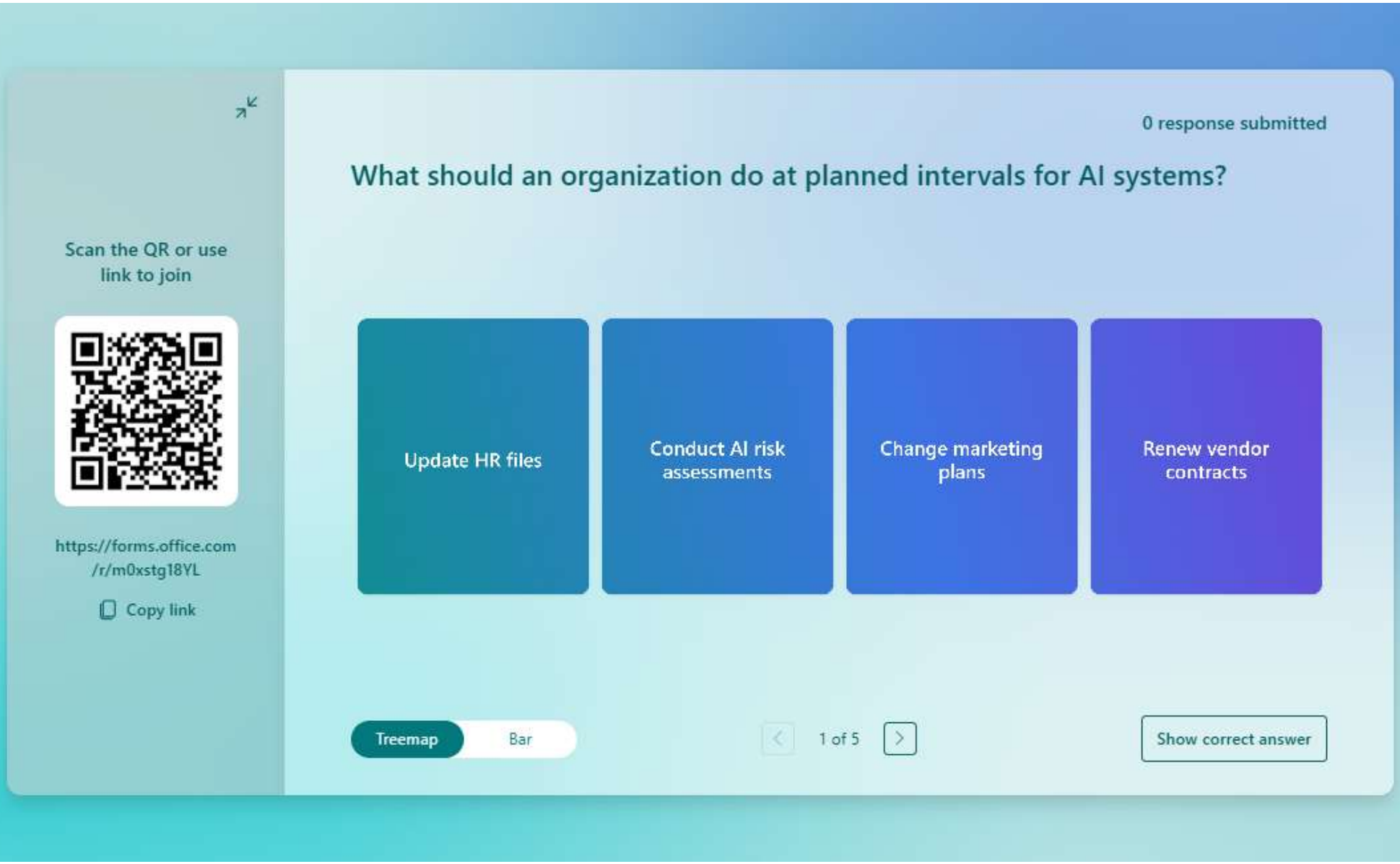
- **Implement the AI risk treatment plan** according to Clause 6.1.3.
- **Verify effectiveness** of the treatment measures implemented.
- When new risks are identified, **initiate AI risk treatment again** as per Clause 6.1.3.
- **Reassess and update** the risk treatment plan if controls are ineffective or outdated.
- **Retain documented information** on all AI risk treatment results.

8.4 AI system impact assessment

- **Perform AI system impact assessments** as per Clause 6.1.4, at **planned intervals and** when **significant changes** are proposed or occur.
- Assess the **potential consequences** of AI system deployment, use, and misuse on Individuals, groups or society as a whole.
- Consider **technical and societal context** in relevant jurisdictions.
- **Retain documented information** of all assessment results.

Recapitulation – Clause 8

- **Operational Planning and Control:**
  Plan, implement, and control AI system processes needed to meet AIMS requirements, including lifecycle activities like design, development, deployment, and monitoring.
- **AI Risk Assessment (Clause 8.2):**
  Perform AI-specific risk assessments at planned intervals and during significant changes; retain documented information on risk identification, ranking (prohibited, high, limited, minimal risks), mitigation actions, and results.
- **AI Risk Treatment (Clause 8.3):**
  Implement selected risk treatment options based on assessment results, referring to Annex A controls, and prepare a documented risk treatment plan and Statement of Applicability (SoA).
- **AI System Impact Assessment (Clause 8.4):**
  Conduct impact assessments to evaluate consequences for individuals, society, and organizations. Document and integrate findings into the risk assessment process.
- **Controls and Documentation:**
  Apply necessary controls identified through risk treatment, manage changes effectively, and retain documented information for operations, risk management, and system impacts.


0 response submitted
What should an organization do at planned intervals for AI systems?
Scan the QR or use link to join
https://forms.office.com/r/m0xstg18YL
Copy link
Update HR files
Conduct AI risk assessments
Change marketing plans
Renew vendor contracts
Treemap
Bar
1 of 5
Show correct answer

Clause 9 Performance Evaluation

9.1 Monitoring, measurement, analysis and evaluation

9.2 Internal audit

9.3 Management review

9.1 Monitoring, measurement, analysis and evaluation

The organization shall determine:

- What needs to be **monitored and measured** to evaluate AI performance and system effectiveness;
- The **methods** for monitoring, measurement, analysis, and evaluation to ensure valid and reliable results;
- **When** the monitoring and measuring shall be performed;
- **When** the results shall be analyzed and evaluated;
- Documented information shall be maintained as **evidence of the monitoring and measurement results**;
- The organization shall use this information to **evaluate the effectiveness and performance** of the AIMS.

9.2 Internal audit

Conduct internal audits of the AIMS:

- At **planned intervals**
- To determine whether the AIMS:
  - Conforms to the organization's own requirements and the ISO/IEC 42001 standard
  - Is **effectively implemented and maintained**

Internal Audit Programme

- **Plan, establish, implement, and maintain** an internal audit programme(s)
- Consider:
  - The **importance of processes**
  - **Results of previous audits**

Internal audit

- Select **objective** auditors.
- Elaborate an **audit plan** for each audit.
- **Report** the results to the relevant management

9.3 Management review

- Ensure that the AI Management System (AIMS) remains **suitable**, **adequate**, and **effective** by conducting management reviews at **planned intervals**.

Inputs to Management Review

Management shall consider the following:

- Status of actions from previous management reviews
- Changes in external and internal issues relevant to AIMS
- Changes in needs and expectations of interested parties
- Performance of the AIMS, including:
  - Nonconformities and corrective actions
  - Monitoring and measurement results
  - Audit results
- Opportunities for continual improvement

Results of Management Review:

The output shall include:

- Decisions on continual improvement opportunities
- Requirements for changes to the AIMS
- Documentation of review results for evidence and follow-up

- Evidence of review results and decisions must be retained to demonstrate management's engagement with AIMS and continual improvement efforts.

Recapitulation – Clause 9

- **Monitoring, Measurement, Analysis, and Evaluation :** Organizations must define what needs to be monitored and measured regarding the AI Management System (AIMS), how, when, and by whom, to evaluate AIMS performance and effectiveness.
- **Internal Audit :** Conduct internal audits at planned intervals to ensure that:
  - The AIMS conforms to ISO 42001 requirements and organizational requirements.
  - The AIMS is effectively implemented and maintained.
  - Audit planning must consider the importance of processes and results of previous audits.
- **Management Review :** Top management must review the organization's AIMS at planned intervals to ensure its continuing suitability, adequacy, effectiveness, and alignment with the organization's strategic direction.
  - Inputs include audit results, stakeholder feedback, risk assessment updates, nonconformities, and continual improvement opportunities.
- **Outcome :** Outputs from performance evaluation must include decisions and actions related to opportunities for improvement, changes to AIMS, and resource needs.

Scan the QR or use link to join

https://forms.office.com/r/7sqYGVbLnh

Copy link

0 response submitted

What is the purpose of monitoring and measuring the AIMS?

Treemap | Bar

1 of 5

Show correct answer

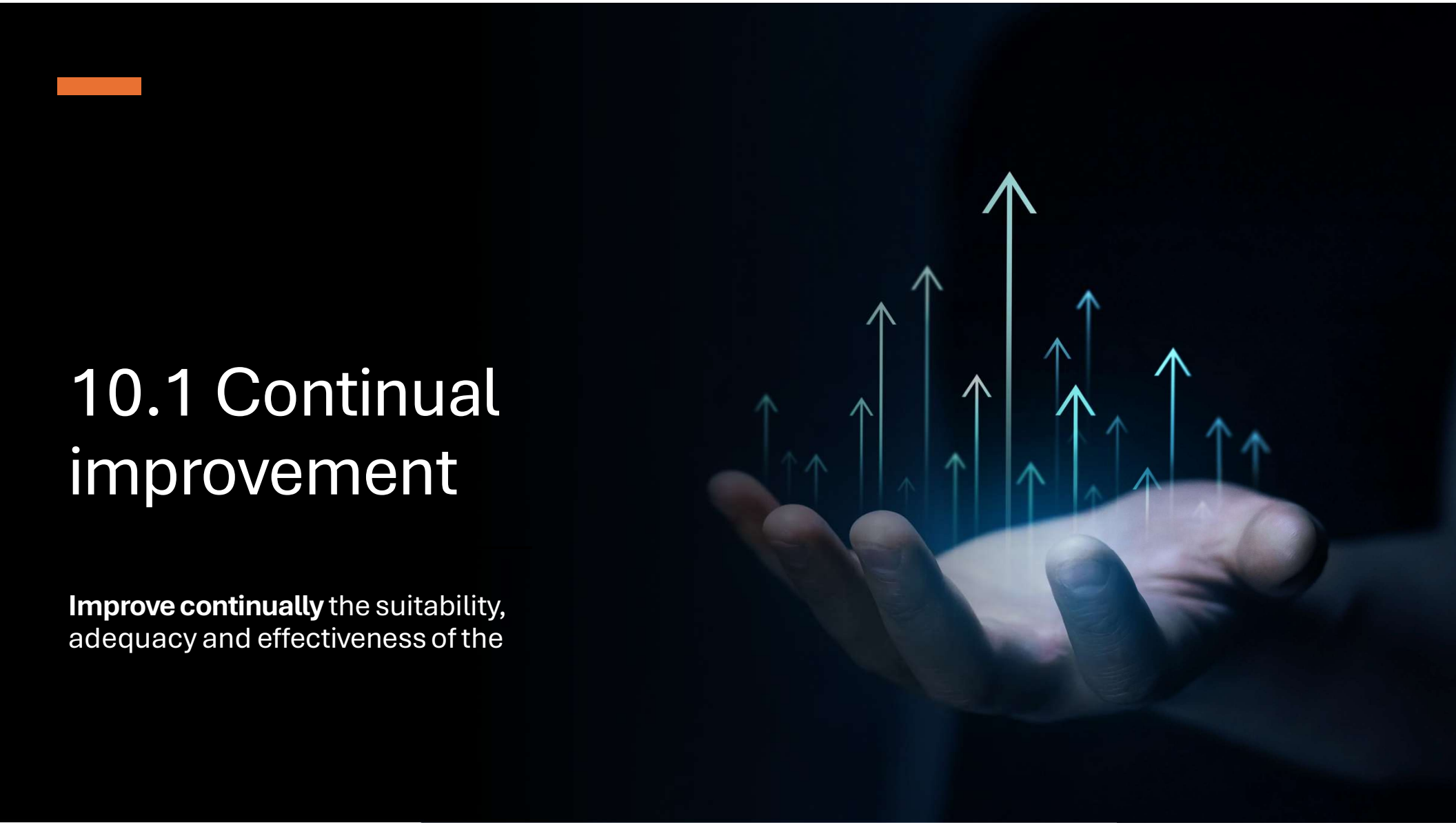
Clause 10 Continual Improvement

10.1 Continual improvement

10.2 Nonconformity and corrective action

10.1 Continual improvement

Improve continually the suitability, adequacy and effectiveness of the



Continual Improvement Can Be Achieved Through

- Results of **internal audits** and **management reviews**
- Evaluation of **AI system performance**
- **Feedback** from interested parties
- **Lessons learned** from incidents or near misses
- Innovation in **AI ethics, fairness, safety, and transparency**

10.2 Nonconformity and corrective action

Nonconformity is the **non-fulfilment of a requirement** related to the AI Management System.

Managing AI Nonconformities – Step-by-Step

QUALITY ASIA

React

- Take **immediate action** to:
  - **Control and correct** the nonconformity.
  - **Deal with the consequences**.

Investigate

- Evaluate the need to **eliminate the root cause**:
  - Review the nonconformity.
  - Determine its cause(s).
  - Assess if similar nonconformities exist or could occur.

Implement

- Take and **document corrective actions**.

Evaluate

- **Review the effectiveness** of the actions taken.

Update

- Make necessary **changes to the AIMS**, if required.

Documented Information Required

- Nature of the nonconformity.
- Actions taken and results of corrective action.

Recapitulation – Clause 10

- Nonconformity and Corrective Action:
  - When a nonconformity occurs, the organization must:
  - React promptly to control and correct it.
  - Deal with the consequences.
  - Investigate and determine the root cause.
  - Implement corrective actions to eliminate causes and prevent recurrence.
  - Review the effectiveness of corrective actions taken.
- Continual Improvement:
  - The organization must continually improve the suitability, adequacy, and effectiveness of the AI Management System (AIMS) to enhance AI governance, risk management, and responsible AI deployment.
- Focus Areas for Improvement:
  - Learn from AI incidents or near-misses.
  - Update AI system processes, risk treatments, and controls.
  - Strengthen ethical AI practices and stakeholder trust.

Scan the QR or use link to join

https://forms.office.com/r/5bDgphy8z1

Copy link

0 response submitted

What should an organization do when a nonconformity occurs?

Ignore it	Celebrate it	React, control, correct, and deal with the consequences	Hire more employees

Treemap | Bar

1 of 5

Show correct answer

Annex A – AIMS Controls

- **Annex A** of **ISO/IEC 42001:2023**
- Contains management system controls for AI grouped in themes/categories for responsible AI governance.

- Total 38 Controls categorized into 9 themes/categories
  - Policies related to AI
  - Internal organization
  - Resources for AI systems
  - Assessing impacts of AI systems
  - AI system life cycle
  - Data for AI systems
  - Information for interested parties of AI systems
  - Use of AI systems
  - Third-party and customer relationships

A.2 Policies related to AI

A.2.2 AI policy

A.2.3 Alignment with other organizational policies

A.2.4 Review of the AI policy

A.2.2 AI policy

Policies related to AI	A.2.2	AI Policy
The organization shall document a policy for the development or use of AI systems.		

- Develop a comprehensive AI policy that outlines the organization's approach to AI development, deployment, and usage, ensuring alignment with ethical standards and business objectives.

A.2.3 Alignment with Other Policies

Policies related to AI	A.2.3	Alignment with Other Policies
The organization shall determine where other policies can be affected by or apply to, the organization's objectives with respect to AI systems.		

- Review existing organizational policies to ensure consistency and integration with the AI policy, addressing any overlaps or conflicts.

A.2.4 Review of the AI Policy

Policies related to AI	A.2.4	Review of the AI Policy
The AI policy shall be reviewed at planned intervals or additionally, as needed to ensure its continuing suitability, adequacy and effectiveness.		

- Establish a regular review process for the AI policy to keep it up-to-date with technological advancements, regulatory changes, and organizational goals.

A.3. Internal Organization

A.3.2 AI Roles and Responsibilities

A.3.3 Reporting of Concerns

A.3.2 AI Roles and Responsibilities

Internal Organization	A.3.2	AI Roles and responsibilities
Roles and responsibilities for AI shall be defined and allocated according to the needs of the organization.		

- Clearly define and assign AI-related roles and responsibilities to ensure accountability and effective management of AI systems throughout their lifecycle.

A.3.3 Reporting of Concerns

Internal Organization	A.3.3	Reporting of concerns
The organization shall define and put in place a process to report concerns about the organization's role with respect to an AI system throughout its life cycle.		

- Implement a transparent reporting mechanism that allows stakeholders to raise concerns related to AI systems, ensuring issues are addressed promptly and appropriately.

A.4. Resources for AI Systems

A.4.2 Resource Documentation

A.4.3 Data Resources

A.4.4 Tooling Resources

A.4.5 System and Computing Resources

A.4.6 Human Resources

A.4.2 Resource Documentation

Resources for AI Systems	A.4.2	Resource documentation
The organization shall identify, and document relevant resources required for the activities at given AI system life cycle stages and other AI-related activities relevant for the organization.		

- Maintain detailed records of all resources, including data, tools, and personnel, involved in AI system development and operation to ensure traceability and accountability.

A.4.3 Data Resources

Resources for AI Systems	A.4.3	Data Resources
As part of resource identification, the organization shall document information about the data resources utilized for the AI system.		

- Ensure comprehensive documentation of data sources, quality, and management practices to support data integrity and compliance with data governance standards.

A.4.4 Tooling Resources

Resources for AI Systems	A.4.4	Tooling Resources
As part of resource identification, the organization shall document information about the tooling resources utilized for the AI system.		

- Keep an inventory of all tools and software used in AI system development and maintenance, including version control and licensing information.

A.4.5 System and Computing Resources

Resources for AI Systems	A.4.5	System and computing resources
As part of resource identification, the organization shall document information about the system and computing resources utilized for the AI system.		

- Record details of hardware and computing infrastructure supporting AI systems to manage capacity, performance, and scalability effectively.

A.4.6 Human Resources

Resources for AI Systems	A.4.6	Human Resources
As part of resource identification, the organization shall document information about the human resources and their competences utilized for the development, deployment, operation, change management, maintenance, transfer and decommissioning, as well as verification and integration of the AI system.		

- Maintain records of personnel involved in AI systems, including their roles, responsibilities, and competency levels, to ensure appropriate expertise is applied throughout the AI lifecycle.

A.5. Assessing Impacts of AI Systems

A.5.2 AI System Impact Assessment Process

A.5.3 Documentation of AI System Impact Assessments

A.5.4 Assessing AI System Impact on Individuals or Groups

A.5.5 Assessing Societal Impacts of AI Systems

A.5.2 AI System Impact Assessment Process

Assessing Impacts of AI Systems	**A.5.2**	AI System Impact Assessment Process
The organization shall establish a process to assess the potential consequences for individuals or groups of individuals, or both, and societies that can result from the AI system throughout its life cycle.		

- Develop a structured methodology for evaluating the potential impacts of AI systems, considering ethical, legal, and social implications.

A.5.3 Documentation of AI System Impact Assessments

Assessing Impacts of AI Systems	A.5.3	Documentation of AI System Impact Assessments
The organization shall document the results of AI system impact assessments and retain results for a defined period.		

- Keep detailed records of impact assessments, including methodologies, findings, and mitigation strategies, to demonstrate due diligence and inform decision-making.

A.5.4 Assessing AI System Impact on Individuals or Groups

Assessing Impacts of AI Systems	**A.5.4**	Assessing AI System Impact on Individuals or groups
The organization shall assess and document the potential impacts of AI systems to individuals of groups of individuals throughout the systems life cycle.		

- Analyze how AI systems may affect specific populations, ensuring considerations for fairness, bias, and discrimination are addressed.

A.5.5 Assessing Societal Impacts of AI Systems

Assessing Impacts of AI Systems	**A.5.5**	Assessing Societal Impact of AI Systems
The organization shall assess and document the potential societal impacts of AI systems throughout their life cycle.		

- Evaluate the potential societal consequences of AI deployment, including economic, cultural, and environmental effects, to promote responsible innovation.

A.6. AI System Lifecycle

- A.6.1 Management guidance for Al system development
  - A.6.1.2 Objectives for Responsible Development of AI Systems
  - A.6.1.3 Processes for Responsible AI System Design and Development
- A.6.2. AI System life cycle
  - A.6.2.2 AI System Requirements and Specification
  - A.6.2.3 Documentation of AI System Design and Development
  - A.6.2.4 AI System Verification and Validation
  - A.6.2.5 AI System Deployment
  - A.6.2.6 AI System Operation and Monitoring
  - A.6.2.7 AI System Technical Documentation
  - A.6.2.8 AI System Recording of Event Logs

A.6.1.2 Objectives for Responsible Development of AI Systems

AI System lifecycle	A.6.1.2	Objectives for responsible development of AI Systems
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.		

- Set clear, ethical objectives guiding the development of AI systems, ensuring alignment with organizational values and stakeholder expectations.

A.6.1.3 Processes for Responsible AI System Design and Development

AI System lifecycle	**A.6.1.3**	Processes for responsible AI System design and development
The organization shall define and document the specific processes for the responsible design and development of the AI system.		

- Establish standardized procedures for designing and developing AI systems that incorporate ethical considerations, risk management, and quality assurance.

A.6.2.2 AI System Requirements and Specification

AI System lifecycle	A.6.2.2	AI System requirement and specification
The organization shall specify and document requirements for new AI systems or material enhancements to existing systems.		

- Clearly define functional and non-functional requirements for AI systems, including performance metrics, compliance needs, and user expectations.

A.6.2.3 Documentation of AI System Design and Development

AI System lifecycle	A.6.2.3	Documentation of AI System Design and Development
The organization shall document the AI system design and development based on organizational objectives, documented requirements and specification criteria.		

- Maintain comprehensive records of design decisions, development processes, and testing outcomes to ensure transparency and facilitate future audits or reviews.

A.6.2.4 AI System Verification and Validation

AI System lifecycle	**A.6.2.4**	AI System verification and validation
The organization shall define and document verification and validation measures for the AI system and specify criteria for their use.		

- Implement testing and evaluation procedures to confirm that AI systems function as intended and comply with established standards and regulations.

A.6.2.5 AI System Deployment

AI System lifecycle	A.6.2.5	AI system Deployment
The organization shall document a deployment plan and ensure that appropriate requirements are met prior to deployment.		

- Develop deployment strategies that include risk assessments, rollback plans, and stakeholder communication to ensure smooth integration into operational environments.

A.6.2.6 AI System Operation and Monitoring

AI System lifecycle	A.6.2.6	AI System operating and monitoring
The organization shall define and document the necessary elements for the ongoing operation of the AI system. At the minimum, this should include system and performance monitoring, repairs, updates and support.		

- Establish monitoring mechanisms to track AI system performance, detect anomalies, and implement corrective actions as necessary.

A.6.2.7 AI System Technical Documentation

AI System lifecycle	A.6.2.7	AI System technical documentation
The organization shall determine what AI system technical documentation is needed for each relevant category of interested parties, such as users, partners, supervisory authorities, and provide the technical documentation to them in the appropriate form.		

- Create and update technical manuals, user guides, and system specifications to support maintenance, user training, and regulatory compliance.

A.6.2.8 AI System Recording of Event Logs

AI System lifecycle	A.6.2.8	AI System recording and event logs
The organization shall determine at which phases of the AI system lifecycle, record keeping of event logs should be enabled, but at the minimum when the AI system is in use,		

- Implement logging practices that capture relevant events and system activities, facilitating troubleshooting, security analysis, and accountability.

A.7. Data for AI Systems

- A.7.2 Data for Development and Enhancement of AI Systems
- A.7.3 Acquisition of data
- A.7.4 Quality of data for AI systems
- A.7.5 Data provenance
- A.7.6 Data preparation

A.7.2 Data for Development and Enhancement of AI Systems

Data for AI System	A.7.2	Data for Development and Enhancement of AI Systems
The organization shall define, document and implement data management processes related to the development of AI systems.		

- Establish data governance processes, define responsible roles, document procedures for sourcing, curating, storing, and validating data used in AI development.

A.7.3 Acquisition of data

Data for AI System	A.7.3	Acquisition of data
The organization shall determine and document details about the acquisition and selection of the data used in AI systems		

- Identify data sources, establish acquisition criteria, document agreements or licensing, and ensure traceability of data collection processes.

A.7.4 Quality of data for AI systems

Data for AI System	A.7.4	Quality of data for AI Systems
The organization shall define and document requirements for data quality and ensure that data used to develop and operate the AI system meet those requirements.		

- Define quality parameters (accuracy, completeness, consistency), set quality thresholds, and regularly review and validate data against these standards.

A.7.5 Data provenance

Data for AI System	A.7.6	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.		

- Maintain logs of data source, transformation history, and usage. Implement version control and traceability mechanisms across the AI lifecycle.

A.7.6 Data preparation

Data for AI System	A.7.6	Data preparation
The organization shall define and document its criteria for selecting data preparations and the data preparation methods to be used.		

- Document preprocessing steps (cleaning, labeling, normalization), select appropriate tools and techniques, and validate the prepared data before use in AI models.

A.8. Information for Interested Parties

- A.8.2 System documentation and information for users
- A.8.3 External reporting
- A.8.4 Communication of incidents
- A.8.5 Information for interested parties

A.8.2 System documentation and information for users

Information for interested parties	A.8.2	System documentation and information for users
The organization shall determine and provide the necessary information to users of the AI system.		

- Create user-facing documentation that includes system functionality, usage guidelines, limitations, and any potential risks. Ensure it is understandable.

A.8.3 External reporting

Information for interested parties	A.8.3	External reporting
The organization shall provide capabilities for interested parties to report adverse impacts of the AI system.		

- Set up feedback channels, helpdesks, or online forms that enable stakeholders to report issues or concerns. Document and track responses.

A.8.4 Communication of incidents

Information for interested parties	A.8.4	Communication of incidents
The organization shall provide capabilities for interested parties to report adverse impacts of the AI system.		

- Develop a communication protocol for incident disclosure—include severity-based messaging, timelines, and responsible personnel for external reporting.

A.8.5 Information for interested parties

Information for interested parties	A.8.5	Information for interested parties
The organization shall provide capabilities for interested parties to report adverse impacts of the AI system.		

- Identify legal, contractual, and ethical obligations. Define the type of information (risks, capabilities, changes, etc.) and the reporting mechanism.

A.9. Use of AI systems

- A.9.2 Processes for responsible use of AI systems
- A.9.3 Objectives for responsible use of AI system
- A.9.4 Intended use of the AI system

A.9.2 Processes for responsible use of AI systems

Use of AI systems	A.9.2	Processes for responsible use of AI systems
The organization shall define and document the processes for the responsible use of AI systems.		

- Develop and formalize responsible use policies. Define user responsibilities, ethical boundaries, and approval steps.

A.9.3 Objectives for responsible use of AI system

Use of AI systems	A.9.3	Objectives for responsible use of AI System
The organization shall identify and document objectives to guide the responsible use of AI systems.		

- Set goals aligned with organizational values (e.g., fairness, safety, transparency) and integrate into project planning.

A.9.4 Intended use of the AI system

Use of AI systems	A.9.4	Intended Use of the AI System
The organization shall ensure that the AI system is used according to the intended uses of the AI system and its documentation.		

- Validate usage against documented scope. Train users accordingly and prevent unintended or unauthorized uses.

A.10.1 Third-party & customer relationships

A.10.2 Allocating responsibilities

A.10.3 Suppliers

A.10.4 Customers

A.10.2 Allocating responsibilities

Third-party & customer relationships	**A.10.2**	Allocating responsibilities
The organization shall ensure responsibilities within the AI life cycle are allocated between the organization, partners, and third parties.		

- Define and document roles clearly in contracts or agreements. Use RACI charts if needed for AI system lifecycle stages.

A.10.3 Suppliers

Third-party & customer relationships	A.10.3	Suppliers
The organization shall establish a process to ensure supplier usage aligns with responsible development and use of AI systems.		

- Conduct supplier evaluations. Align procurement with AI policy and ethics. Include responsible use clauses in contracts.

A.10.4 Customers

Third-party & customer relationships	A.10.3	Customers
The organization shall ensure its responsible approach to AI considers customer expectations and needs.		

- Capture customer feedback. Reflect AI usage risks and safeguards in documentation or user agreements.

QUALITY ASIA

Audits: Definition, Principles, and Types

Audit

- “Systemic, independent and documented process for obtaining audit evidence and evaluating it objectively to determine the extent to which audit criteria are fulfilled.”

- Alternative Definitions:
  - Impartial documented activity
  - Follows written checklists and documentation
  - Uses examination of audit evidence to determine the existence of objective evidence
  - Verifies that applicable processes of a AIMS have been identified and are effectively controlled.

Reasons for Conducting Audits

- To examine the Artificial Intelligence Management System for Improvements
- To ensure ISO 42001, and all other standards, are being complied with.
- To determine compliance or non-compliance
- To meet regulatory requirements
- To enable certification

Effective Audits - Requirements

- Timely access to facilities, documents and personnel, including top management
- Defined auditing procedures
- Support/involvement of management
- Competent audit team
- Impartial and objective audit team

Type of Audit

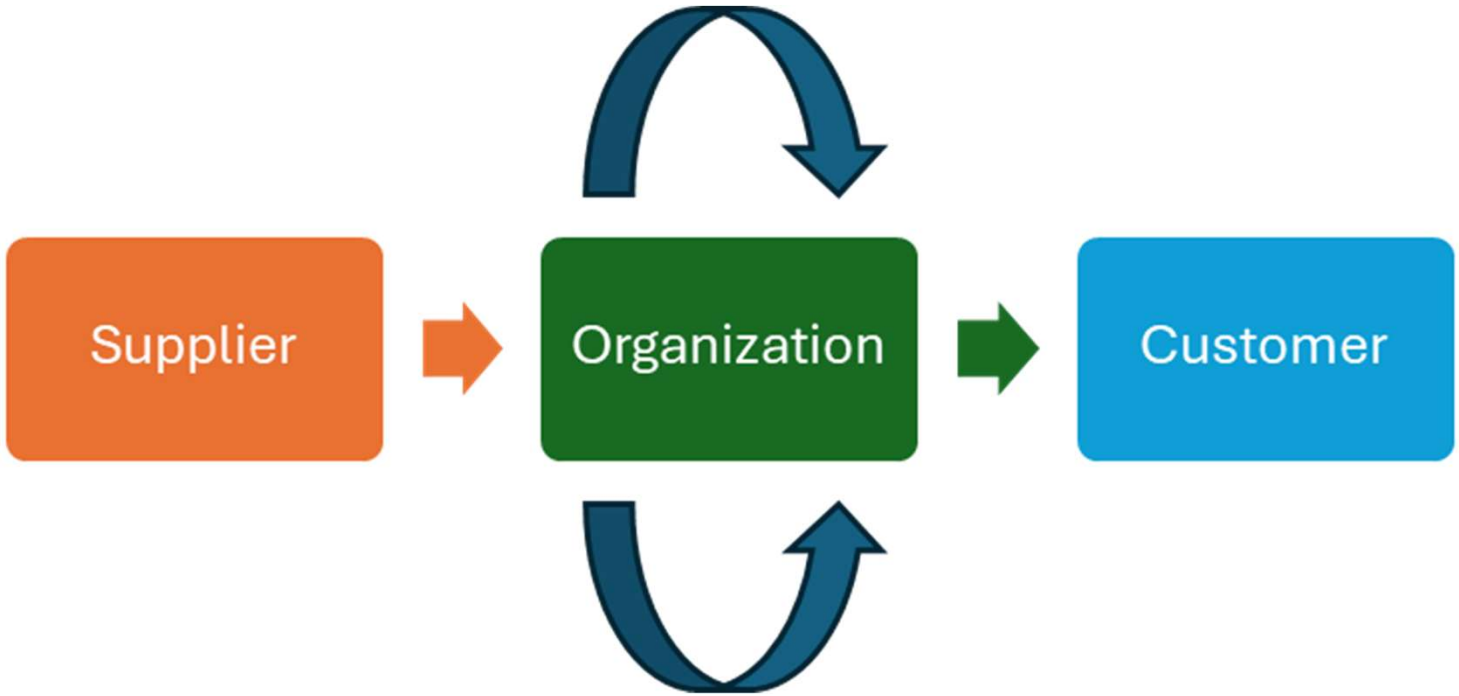
First Party Audits

Second Party Audits

Third Party Audits

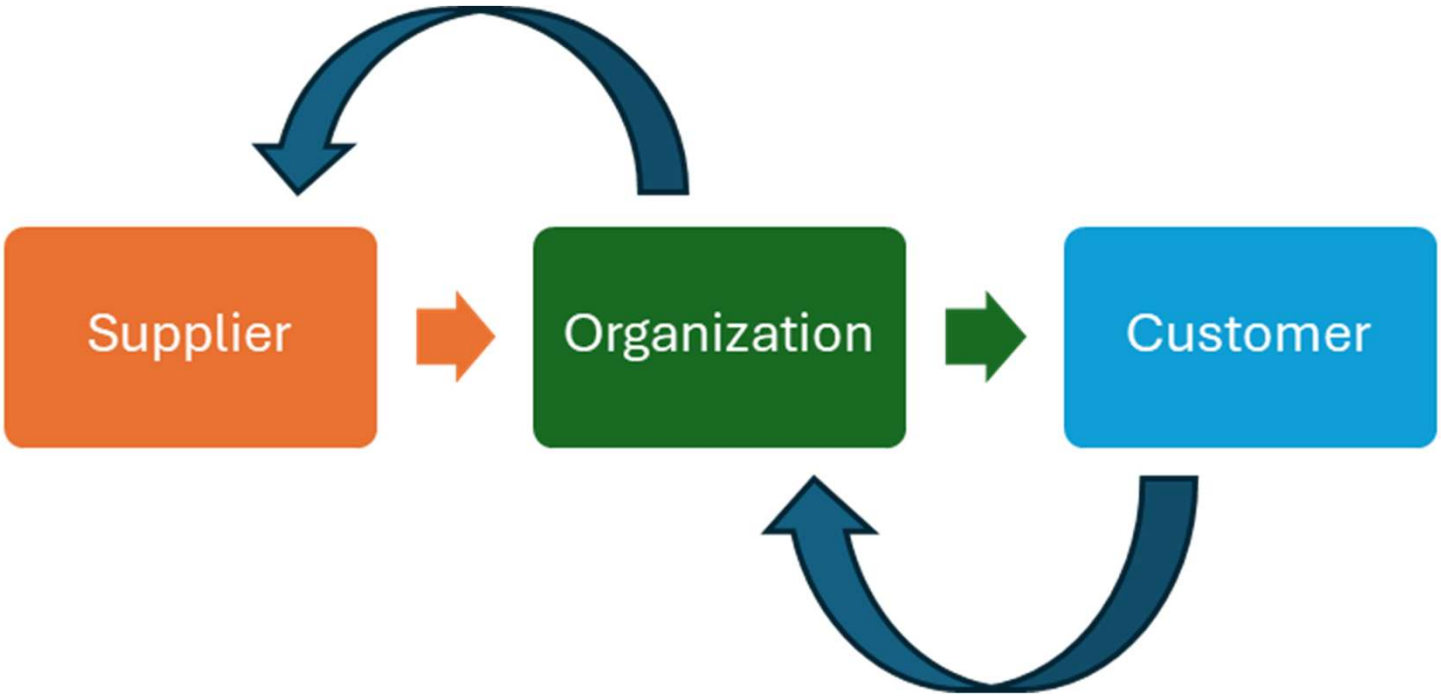
First Party Audit

- Internal audits
- Performed within an organization
- Auditors have no vested interest in the area being audited



Second Party Audit

- Performed by Customers on suppliers
- Before or after awarding a contract



Third Party Audit

- Performed by an audit organization independent of the customer-supplier relationship
- Free from any conflict of interest

Audit participants

Client – Organization or person requesting the audit

Auditor – A Person who conducts the audit

Auditee – Organization or individual being audited

Client, responsible for..

- Initiates audit
- Determines audit purpose and scope
- Provide resources
- Receives the audit report
- Determine the report distribution

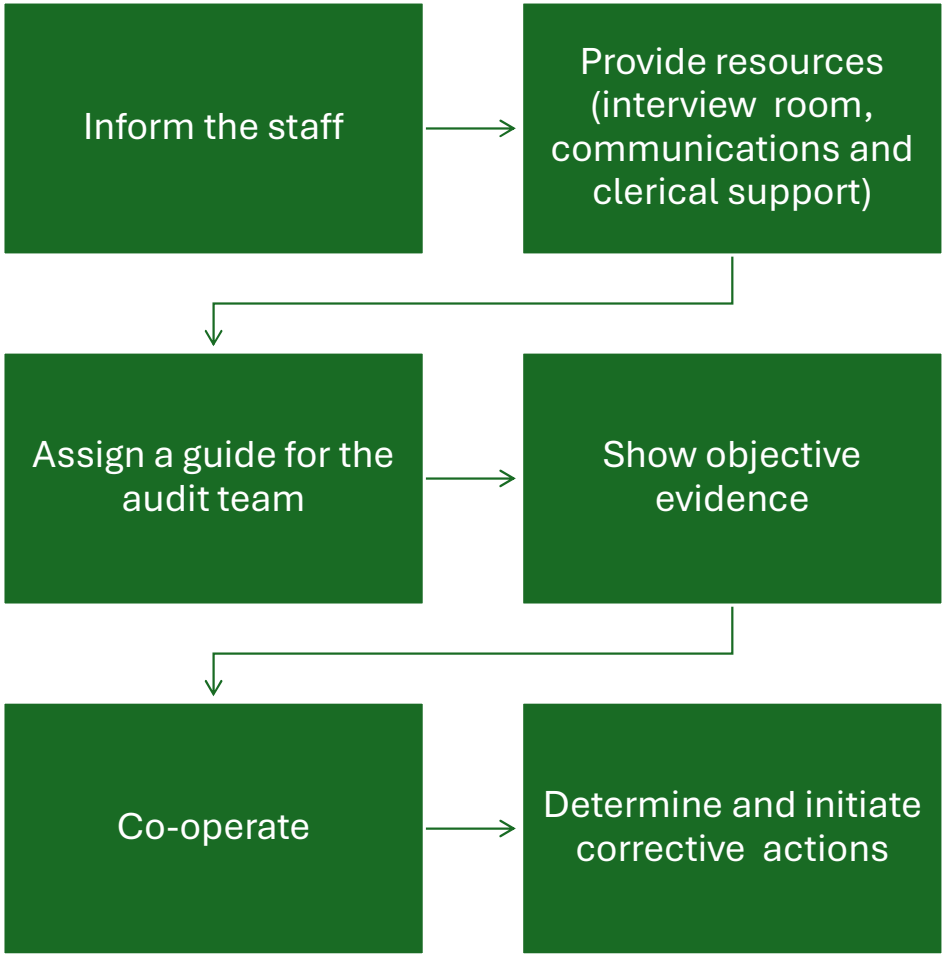
Auditor, responsible for…

- Understand the purpose, scope and audit criteria.
- Plans the audit
- Perform the audit
- Collect audit evidences
- Analyze audit evidences
- Reports the audit
- Follows up the action on audit findings

Lead auditor, responsible for...

- Balance the strength and weaknesses of team members
- Manage the audit process
- Represent the audit team
- Lead the audit team
- Prepare and complete the audit report

Auditee, responsible for...



Audit participants - 2

Technical Expert – a person who provides specific knowledge or expertise to the audit team.

Observer – a person who accompanies the audit team but does not audit.

Guide – a person appointed by the auditee to assist the audit team.

Phases of an Audit

Phases of an Audit

- Planning
- Preparation
- Performance
- Reporting and Follow Up

Planning the Audit Stage

- Frequency and timing
- Responsibility
- Criteria
- Scope
- Methods
- Duration

QUALITY ASIA

Planning Internal Audits

Frequency and timing:	Based on status and importance
Responsibility:	Competent auditor with technical knowledge
Criteria:	Organization's own procedures, specifications, documents, etc. Internal Standards e.g., ISO 42001:2023
Scope:	A process An area of the company, e.g. distribution, Quality control, servicing
Duration	Depends on the size of the scope

Planning Second Party Audits

Frequency and timing:	As determined by the organization
Responsibility:	Competent auditor with technical knowledge
Criteria:	Contractual obligations Organization's management system ISO 42001 or other agreed standards
Scope:	The entire facility An area of the company, e.g. a product line
Duration	Depends on the size of the scope

Planning third Party Audits

Frequency and timing:	Responsibility:	Criteria:	Scope:	Duration
• As determined by the accreditation	• Qualified auditor with technical knowledge & experience	• ISO 42001 or other standards	• Entire organization • Management system operations as defined by applicable standard	• Depends on accreditation requirements

Audit Procedure

- External audits are usually agreed in advance with the auditee and carefully planned, however ‘unannounced audits’ may be carried out by the Certification Bodies or Customers and their representatives as a policy or when there is some justification for such an audit

Activities Prior to the Audit

Create audit program and audit plan and notify the auditee

Arrange audit logistics

Prepare audit checklist

Audit preparation

Notify person to be audited and agree to a date and time

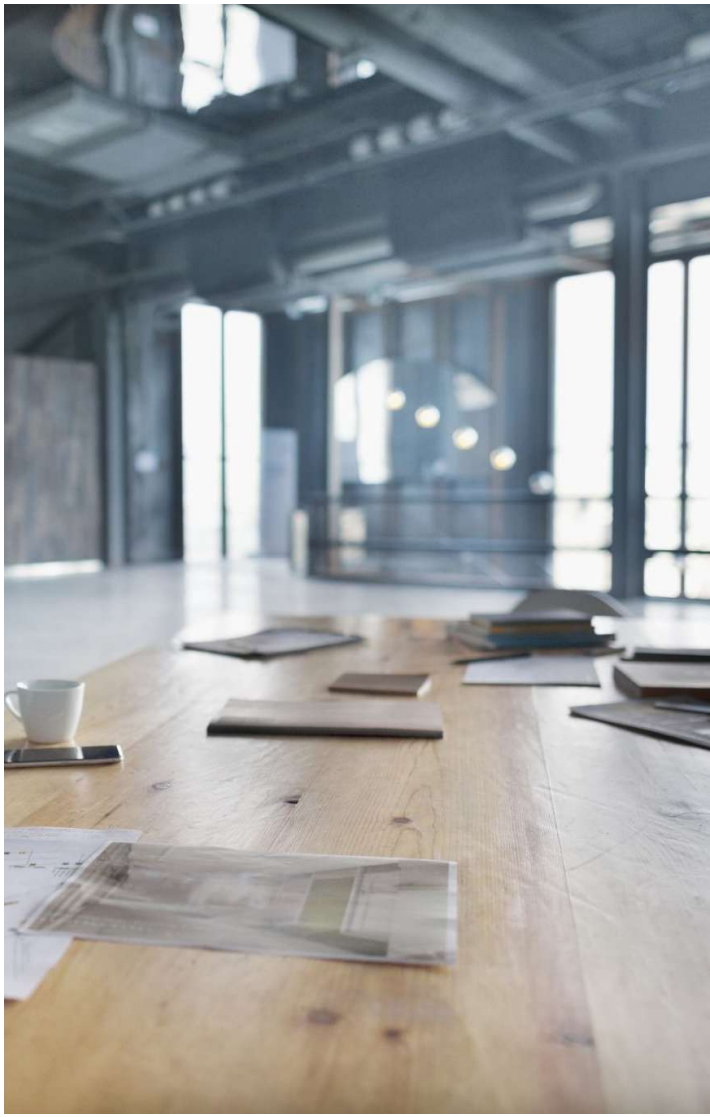
Review documents: procedures, forms, previous reports, corrective action requests, work instructions, etc.

Prepare/review/update checklists

Brief auditor/team

Arrange for Audit Logistics

- Travel and accommodation
- Safety and security considerations
  - Personal Protective Equipment (PPE)
  - Location and/or Camera Permit
- Need for a Guide
- Translators
- Facilities
  - Working area, conference room, internet, printer, tea/coffee and working lunch



Audit Checklist

The Checklist

- To be used as a working document and as a record
- Tool to audit company processes, not standard
- Should follow the natural process of the organization

The Purpose of the Checklist

- To provide guidance to the auditor
- To ensure that the audit scope is covered (processes, activities)
- To reinforce the objectives and scope of the audit
- To act as a record

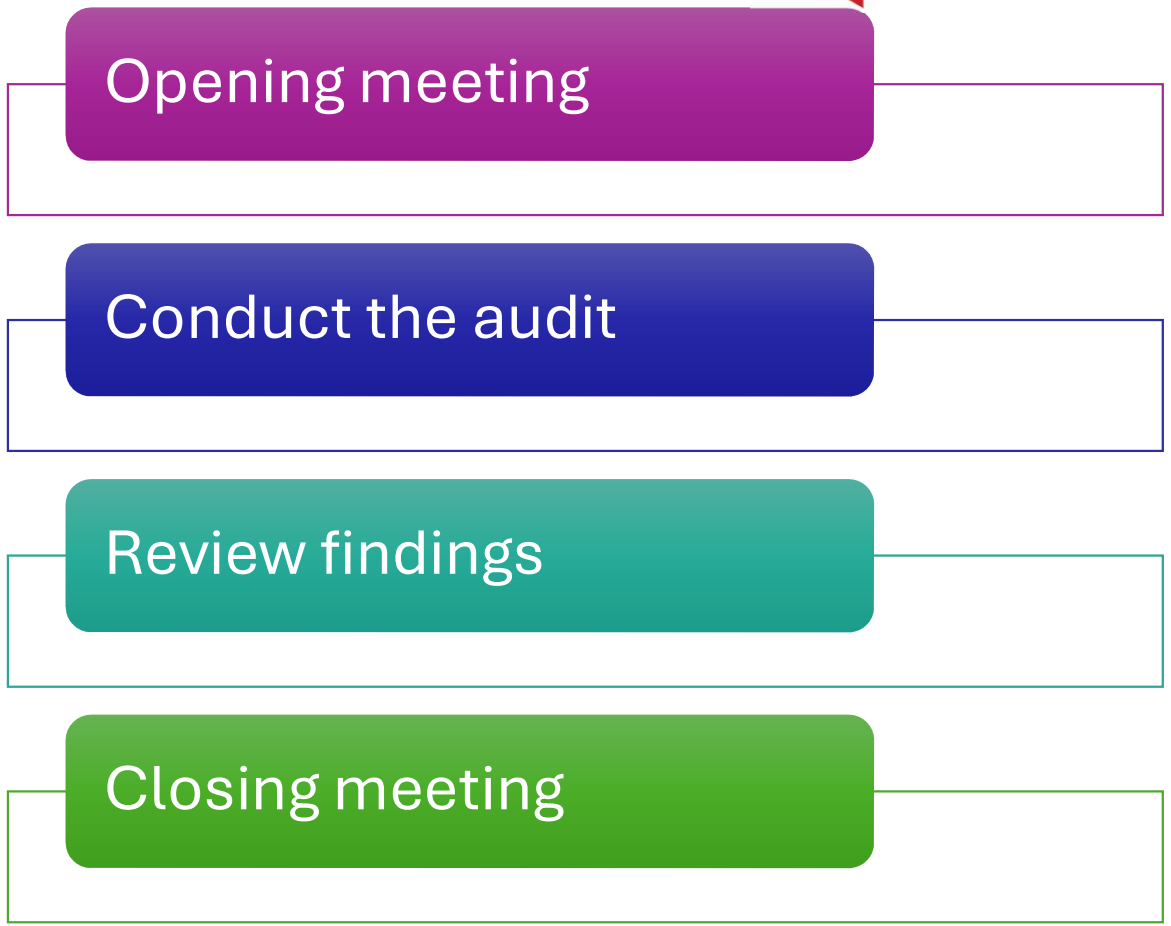
Risks of the Checklist

- Too focused on a single area
- Insufficient information included to evaluate conformance in interviews
- Not customized to reflect company's practices

Sample Checklist

Audit Checklist		Assessment No.
Specification	Location	Date
REQUIREMENT	SPEC	OBSERVATIONS
		Sheet of form QA1

Audit Performance



Opening Meeting

- Introduce auditors or audit team
- Discuss audit scope and process
- Explain reporting and follow-up procedures
- Necessary for:

  a) Good communication

  b) Co-operation

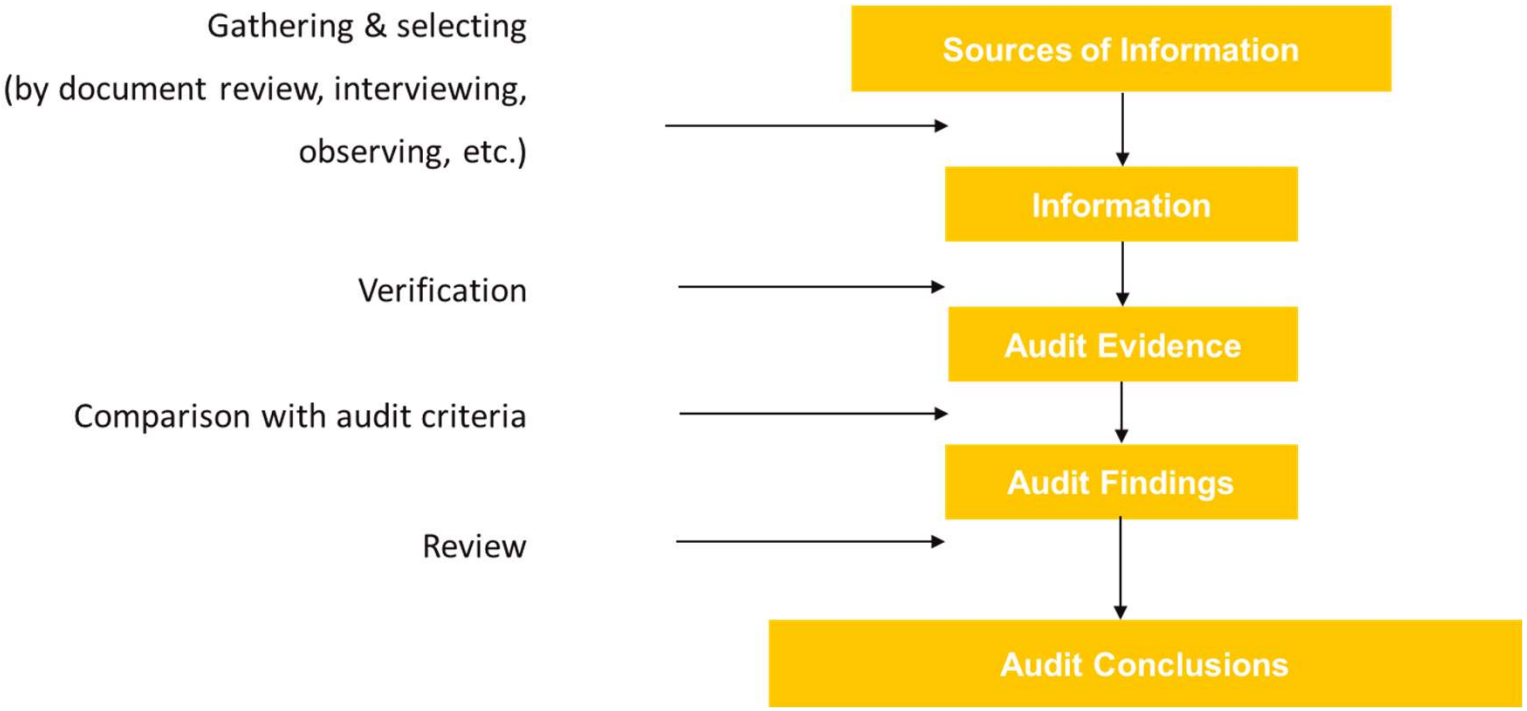
  c) Openness

QUALITY ASIA

The Auditor must:

- Deal with top management
- Understand the key issues in the organization
- Focus on the critical processes
- Audit for business improvement
- Meet the area representative first
- Always talk to those performing the task
- Explain the purpose of the visit
- Be calm, polite, reassuring
- Never talk down
- Never act superior
- Speak clearly and carefully

The Auditor Process



Obtaining objective (audit) Evidence

May be gathered from:

- Interviews with people
- Observation of activities
- Interactions between functions, activities, processes
- Measurement of processes and programs
- Documents/records
- Data summaries, reports from other sources (e.g., customer feedback)

- People:
  - Does anyone understand the systems and documentation?
  - Are the employees competent?
  - Is there co-operation?
  - Are there any system problems?

Obtaining objective (audit) Evidence (Continued)

- Observation of activities
  - Are the processes efficient? Effective?
  - Are things in logical sequence?
  - Are the interactions between processes defined?
  - What is the significance of links between processes?
  - Can inputs and outputs be identified?
- Measurement of processes and programs
  - Capacity of processes
  - Product measurement
  - Accuracy
  - Dependability
  - Cycle times
  - Resource utilization
  - Productivity

Obtaining objective (audit) Evidence (Continued)

Documents/records

- Issue status?
- Complete and concise?
- Condition?
- Legibility?
- Identity?
- Approval?
- Availability?

Data summaries

- Customer feedback
- Vendor analysis
- Internal Audits
- Financial measurements
  - Preventive, appraisal and failure cost analysis (Cost of quality)
  - Cost of nonconformity

Examine objective Evidence

Examine:

- Documents/data
  - Fully complete
  - Accurate data
  - Check for authorization
  - Review analysis of data
- Physical Evidence
- Environmental Conditions

Establish:

- Extent of conformity/nonconformity
- Nature for nonconformity
- Sample: According to the amount and variety of evidence

Use the Checklist

- To record conformity/nonconformity
- To track where you are and manage time
- To control the pace of the audit and manage auditee personalities
- To ensure all areas are covered
- To make notes for follow-up in other areas
- For future reference

Questioning Techniques


Who?


What?


When?


Where?


Why?


How?

QUALITY ASIA

Controlling the Audit

- Insist that people being questioned answer for themselves
- Do as little talking as possible
- Do not let others dictate the pace
- Rephrase misunderstood questions
- Give compliments
- Say, “Thank you”
- Be aware of hidden agendas and emotional blackmail

Some Basic Issues

- Establish that the company is demonstrating control over the operation
- Involve management in the audit process
- Observe work progression when possible
- Evaluate physical objective evidence
- Examine inputs and outputs
- Make comprehensive notes

Some Basic Rules

Seek verification

- Do not assume people will lie, but seek to verify statements if necessary

Do not accept pre-prepared samples

- Choose your own

General Principles of Auditing

- **Integrity –** the foundation of professionalism
- **Fair presentation –** the obligation to report truthfully and accurately
- **Due professional care –** the application of diligence and judgment in auditing
- **Confidentiality –** security of information
- **Independence –** the basis for the impartiality of the audit and objectivity of the audit conclusions
- **Evidence-based approach –** the rational method for reaching reliable and reproducible audit conclusions in a systematic audit process

Auditor's Personal Attributes

Ethical – Fair, truthful, sincere, honest and discreet

Open-minded – willing to consider alternative ideas or points of view

Diplomatic – tactful in dealing with people

Observant – actively observing physical surroundings and activities

Perceptive – aware of and able to understand situations

Versatile – able to readily adapt to different situations

Tenacious – persistent and focused on achieving objectives

Decisive – able to reach timely conclusions based on logical reasoning and analysis

Self-reliant – able to act and function independently whilst interacting effectively with others

General knowledge and skills of Management System Auditors

- Audit principles, procedures and methods
- Management system and reference documents
- Organizational context
- Applicable legal and contractual requirements and other requirements that apply to the auditee
- Discipline and sector-specific knowledge and skills of management system auditors

Generic Knowledge and Skills of Audit Team Leaders

QUALITY ASIA

Audit team leaders should be able to:

- Balance the strengths and weaknesses of the individual audit team members
- Develop a harmonious working relationship among the audit team members.
- Plan audits and effectively use audit resources
- Manage the uncertainty of achieving audit objectives
- Protect the health and safety of the audit team members including compliance with the requirements
- Organize and direct the audit team members
- Provide direction and guidance to auditors-in-training
- Prevent and resolve conflicts as necessary
- Represent the audit team
- Lead the audit team to reach the audit conclusions
- Prepare and complete the audit report

Good Practices for Auditors

- Introduce self and/or audit team
- Ensure agenda is understood
- Keep to agenda
- Keep control of the audit and time
- Avoid arguments
- Listen
- Keep records
- Remain polite, calm, professional

Audit Review

- Conduct a private review when the audit is finished
- Interim or “end of the day” reviews (or both) may be appropriate
- Review and complete checklists
- Study and compare notes (team)
- List nonconformities

Analyzing Results

Review if:

- The deficiency is an isolated error or a breakdown of a system
- Auditee is aware of the problem
- The deficiency has been reported before

Closing Meeting


Explain/discuss the findings


Obtain agreement


State overall degree of conformity


Mention the positive points

Internal audits	Second party audits	Third party audits
• Informal • Constructive • System improvement	• Contracts at stake • Reports used as future reference • More emotional situation than first party audit meeting • Be prepared to be challenged	• Contracts at stake • Reports used as future reference • More emotional situation than first party audit meeting • Be prepared to be challenged

Non-conformance management in first party audits

Identification: Auditors identify non-conformities against the organization's internal procedures or ISO requirements.

Recording: Non-conformances are documented in the audit report.

Corrective Action: The organization takes corrective actions to address root causes and prevent recurrence.

Verification: Follow-up audits or reviews ensure actions are implemented effectively.

Purpose: Improve internal systems, ensure compliance, and prepare for external audits.

Non-conformance management in second party audits

- **Identification**: Non-conformities against agreed terms, product specifications, or food safety requirements are identified.
- **Reporting**: Issues are communicated to the supplier formally.
- **Corrective Action**:
  - The supplier is required to provide a Corrective Action Plan (CAP) within a specified timeline.
  - Actions include root cause analysis, corrective measures, and preventive actions.
- **Verification**: Follow-up audits or supplier reviews are performed to verify corrections.
- **Purpose**: Ensure suppliers meet contractual obligations and quality standards.

Non-conformance management in third party audits

- **Identification**: Non-conformities are classified as:
  - Major: Systematic failures or high-risk non-compliance.
  - Minor: Isolated issues that don't pose significant risk.
- **Reporting**: Non-conformities are included in the audit report and communicated to the auditee.
- **Corrective Action**:
  - Auditees must submit an action plan with root cause analysis, corrective actions, and preventive measures.
  - A timeline is set to resolve major non-conformities (often 30-90 days).
- **Verification**:
  - Major non-conformities require evidence submission and/or re-audit.
  - Minor non-conformities are checked during the next surveillance audit.
- **Purpose**: Achieve certification, regulatory compliance, or demonstrate conformity to standards.

Nonconformance Statement

A short statement describing the nonconformity including:

- What - The issue in question
  (a statement of nonconformity)

- Why - What the statement is raised against?
  (the requirement, or specific reference to the requirement)

- Objective Evidence - The objective evidence found
  (the objective evidence observed that supports statement of nonconformity)

Nonconformance report

- Used to report non-conformity audit findings
- Must be factual
- Must be understandable and traceable
- Raise non-compliances on completion of an audit
- Allow the auditee to implement corrective action prior to the closing meeting
- The auditee is requested to sign signifying an understanding and acceptance of the non-compliance

Wording of NC report

- It is important when preparing and wording NC-Report's to take care and ensure it is justified
- Failure to achieve clear information will invite challenge of the findings at the closing meeting
- This will be particularly important in areas where the emphasis has changed with respect to the requirements in order that they will be clearly understood, i.e.
  - Management Commitment
  - Competence
  - Communication
  - Continual Improvement

Example of Nonconformance Statement

- **A statement of nonconformity:**
  - The organization's employees lacked adequate awareness of AI management system policies and procedures, resulting in a failure to address AI-related risks and responsibilities effectively.
- **The requirement, or specific reference to the requirement:**
  - ISO/IEC 42001:2023 Clause 7.3 Awareness:
  - "Persons doing work under the organization's control shall be aware of:
    - the AI policy;
    - their contribution to the effectiveness of the AI management system, including the benefits of improved AI performance;
    - the implications of not conforming with the AI management system requirements."
- **The objective evidence observed that supports statement of nonconformity:**
  - During employee interviews, it was found that several staff members involved in AI system development were unaware of the organization's AI policy, including procedures to ensure responsible use and compliance. No records of awareness training or briefings could be presented.

Audit Reporting

The audit report should include:

- Auditors, contracts, scope
- Overall conclusions
- Deficiencies, observations, supporting objective evidence
- Follow-up details

Exclude from Report:

- Confidential information given in interviews
- Matters not raised or discussed at the closing meeting
- Subjective opinions – use only verifiable facts / objective evidence
- Ambiguous statements
- Antagonistic words or phrases

Audit Reporting

- Description of audit aim, purpose and scope
- Number of non-compliances and summary of audit findings
- Description of good points and any main concerns
- Description of the identified opportunities for improvement
- Recommendations made because of audit findings

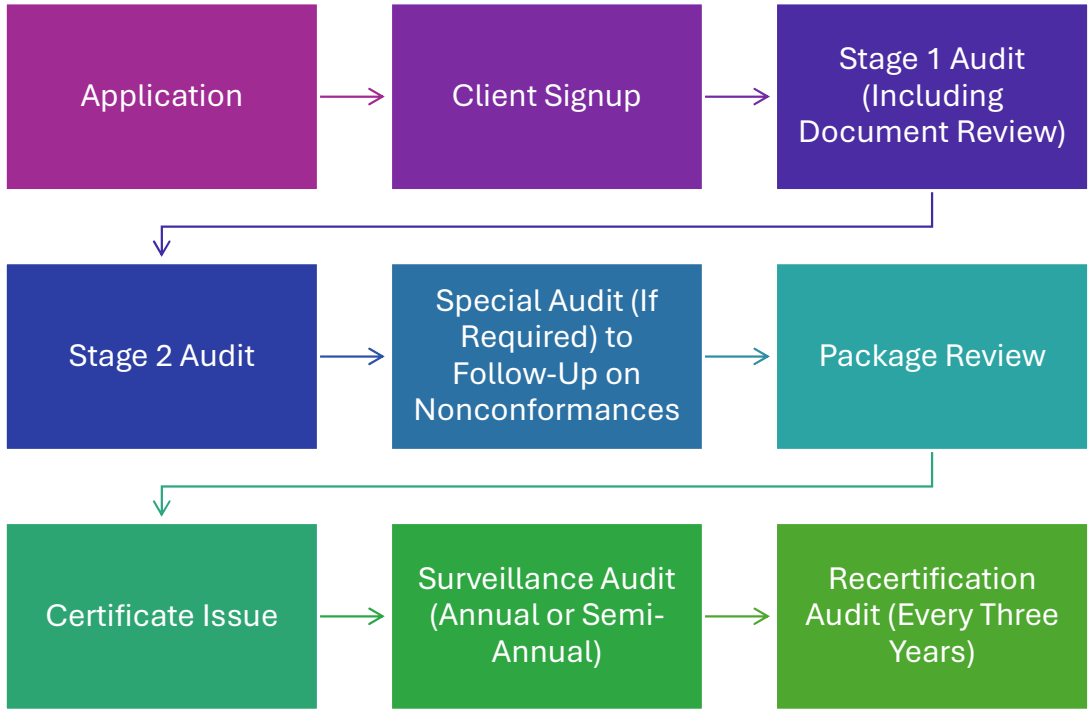
Audit Follow-Up

- Verify that action(s) are implemented
- Ensure short- and long-term effectiveness
- Record follow-up details & objective evidence reviewed
- Sign off forms

ISO/IEC 27001 Certifications for organizations

- Obtained after passing an **audit**.
- Valid for **3 years** with annual **surveillance audits**.
- Can be **suspended** or **withdrawn**.
- Visit Us: https://www.qualityasia.in/contact.php

Registration Process Flow



Certifications and Internal Auditor Trainings offered

- We offer certifications and internal auditor training for -
  - ISO 9001 (QUALITY MANAGEMENT SYSTEMS)
  - ISO 14001 (ENVIRONMENT MANAGEMENT SYSTEMS)
  - ISO 45001 (OCCUPATIONAL HEALTH & SAFETY MANAGEMENT SYSTEMS)
  - ISO 50001 (ENERGY MANAGEMENT SYSTEMS)
  - ISO 27001 (INFORMATION SECURITY MANAGEMENT SYSTEMS)
  - ISO 22000 (FOOD SAFETY MANAGEMENT SYSTEMS)
  - ISO 13485 (MEDICAL DEVICES QUALITY MANAGEMENT SYSTEMS)
  - ISO 26000 (SOCIAL ACCOUNTABILITY MANAGEMENT SYSTEMS)
  - ISO 42001 (ARTIFICIAL INTELLIGENCE MANAGEMENT SYSTEM)

QUALITY ASIA

QUALITY ASIA

Our Accreditation

- At Quality Asia Certifications, our commitment to excellence is validated through our prestigious accreditations.
- We are proud to be recognized by leading national and international accreditation body, including **NABCB (National Accreditation Board for Certification Bodies), IAF Accredited** ensuring the highest standards of quality and compliance.
- Our accreditations reflect our rigorous adherence to industry standards and our dedication to providing reliable and trustworthy certification services. These credentials are a testament to our expertise and our unwavering commitment to delivering value to our clients.
- Proud BNI (Business Network International) Member

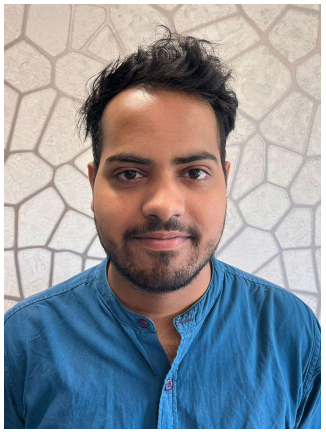
MEMBER OF MULTILATERAL RECOGNITION ARRANGEMENT
IAF

NABCB
QM-085

LEADERSHIP TEAM

			
Mr Atul Suri	**Mrs. Seema Suri**	**Mr Samarth Suri**	**Ms Palak Ahuja**
Lead Auditor & Reviewer	**Director - Accreditations**	**Managing Director**	**GM - Certifications**
Responsible for Leading Teams of Auditors and Establishing Excellence in Auditing Operations	Responsible for Maintaining Accreditation Status and Heading Audit Review and Certification Decision Process	Responsible for Marketing & Promotions, and ensuring Right Visibility of the Certification Body	Responsible for Heading and Managing Certification and Operations and Ensuring Client Success through Certifications

CORE TEAM

			
Mr Parveen Singh Negi	**Mr Sagar Mahour**	**Team of Auditors**	**Team of Executives**
Business Development Head	**Quality Assurance Officer**		
Responsible for Heading Sales Teams and Ensuring Customer Acquisition in the Most Ethically Right Manner	Responsible for compliance with accreditation standards, manages documentation and audits, assists in training programs, and supports marketing and operational excellence initiatives.	Responsible for Conducting Ethical and Quality Rich Audits, enabling Organizations to Understand and Upgrade their Systems and Processes	Responsible for Managing the Shows behind the scenes

QUALITY ASIA

Training Information and Evaluation

Training Material will be provided to you through mail.

Training Evaluation, a google form link is provided to you through mail.

Training Feedback is the part of the Training evaluation form, please provide your valuable feedback.

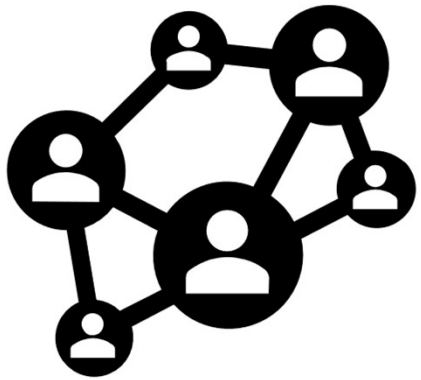
QUALITY ASIA

Quality Asia School and Free Training program updates...

- **Quality Asia School: Explore comprehensive training programs on various ISO standards: https://www.qualityasia.in/qasia-school.php**
- **Join our WhatsApp channel for convenient access to live training sessions: https://whatsapp.com/channel/0029VamtSmnJ93wcEDIsrT1Z**
- **Free Internal Auditor Training Calendar: Explore upcoming training sessions on various ISO standards, including ISO 14001, on our website: https://www.qualityasia.in/training-calendar.php**

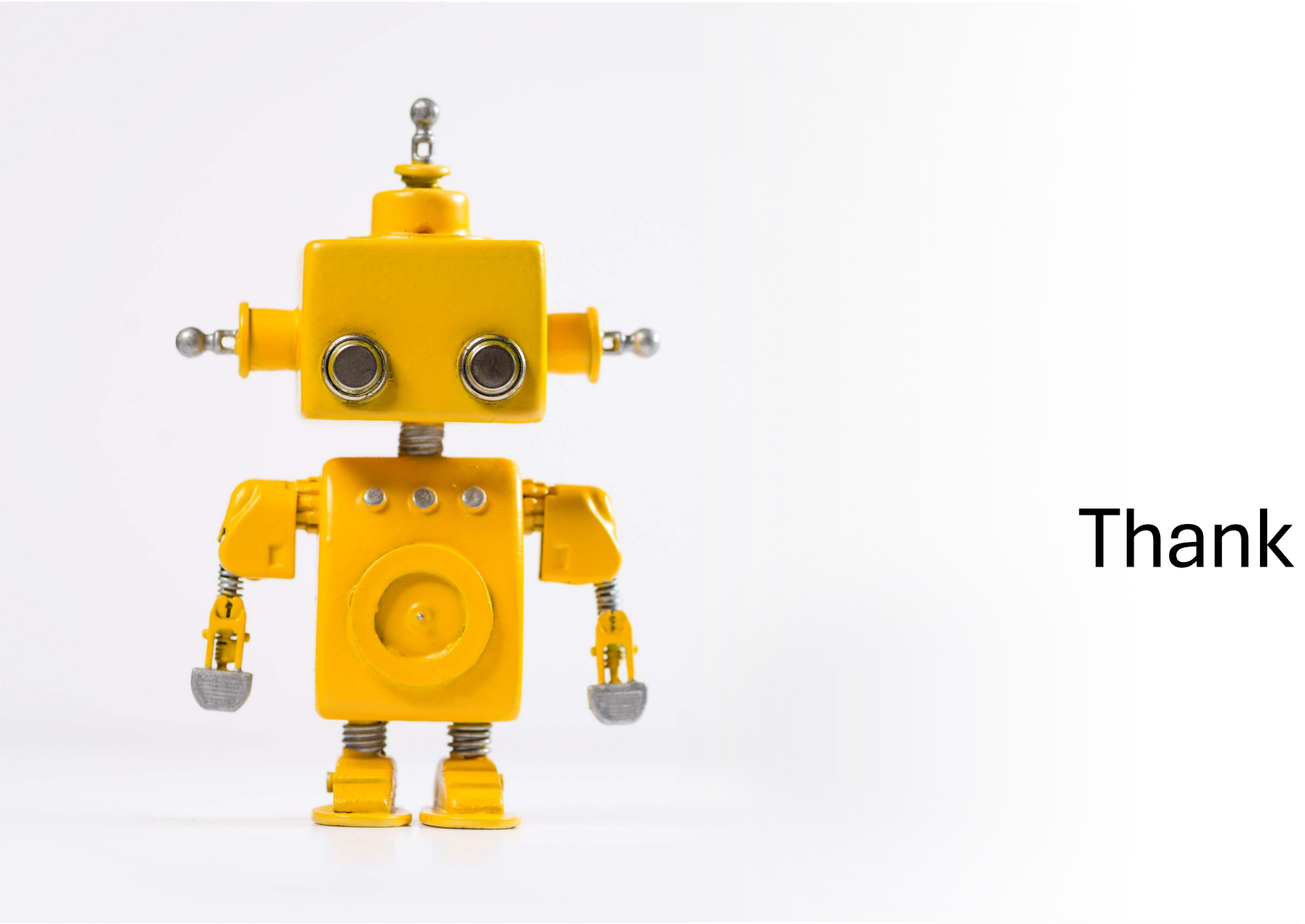
Join us on...

- Follow and Connect with Quality Asia Certifications: Stay updated on our latest news and training programs by following us on Social media:
  - Instagram: https://www.instagram.com/qualityasia/
  - LinkedIn: https://www.linkedin.com/company/quality-asia/mycompany/
- Quality Asia YouTube Channel: Subscribe for insights and educational videos on ISO standards and auditing practices: https://www.youtube.com/@QualityAsia



Training Evaluation Form

Create QR codes at
littleappy.co/qrcodes



Thank You.