COMPASS ROSE
BY 360ADVANCED

ISO STANDARDS

ISO 27001 | ISO 27701 | ISO 42001
CERTIFICATION GUIDE

INFO@360ADVANCED.COM | 360ADVANCED.COM | (866) 418-1708

TABLE OF CONTENTS

INTRODUCTION & PURPOSE

The purpose of this guide is to provide a clear, educational overview of three critical ISO standards:

- ISO/IEC 27001 (Information Security Management Systems)
- ISO/IEC 27701 (Privacy Information Management Systems)
- ISO/IEC 42001 (Artificial Intelligence Management Systems)

These frameworks establish internationally recognized requirements for managing information security, data privacy, and the responsible governance of artificial intelligence.

This guide is designed to help organizations understand the role of each standard, how they intersect, and what certification involves. By combining these standards into one resource, we aim to show how organizations can build stronger, more resilient governance programs across information security, privacy, and AI.

WHAT ARE ISO STANDARDS AND WHY DO THEY MATTER?

The International Organization for Standardization (ISO) develops globally recognized frameworks that help organizations operate securely, responsibly, and efficiently. ISO standards provide structured approaches to managing risks, implementing best practices, and demonstrating accountability to regulators, clients, and stakeholders.

- **ISO/IEC 27001** sets the baseline for building and maintaining an Information Security Management System (ISMS), ensuring organizations protect the confidentiality, integrity, and availability of organizational data.
- **ISO/IEC 27701** sets the baseline for building and maintaining data Privacy Information Management Systems (PIMS). Whether you are a processor, controller, or both, ISO 27701 aligns with federal requirements (CCPA/CCRA) and global privacy regulations like GDPR.
- **ISO/IEC 42001** is the first international standard for Artificial Intelligence Management Systems (AIMS), guiding organizations in ensuring responsible, transparent, and trustworthy AI practices for users, providers, developers, or producers.

Together, these standards provide a comprehensive framework for modern organizations navigating the risks associated with complex regulatory requirements, rising cybersecurity threats, and the ethical challenges of AI adoption. Certification with 360 Advanced Compass Rose demonstrates not only compliance but also a commitment to best practices, stakeholder trust, and long-term resilience rather than a checkbox approach.

OVERVIEW OF ISO 27001

Scope & Applicability

ISO/IEC 27001 is the internationally recognized standard for Information Security Management Systems. Its purpose is to help organizations establish, implement, maintain, and continually improve a risk-based structured framework for protecting organizational information. The standard applies to organizations of any size or sector, whether healthcare providers handling patient data, financial institutions managing transactions, technology firms safeguarding intellectual property, or public-sector entities protecting data subjects' records.

Control Domains & Structure

ISO 27001 is structured around a risk-based approach to ISMS. The standard defines requirements for:

- Establishing an ISMS that is aligned with organizational objectives.
- Conducting risk assessments and implementing risk treatment plans.
- Documenting policies, procedures, and controls to mitigate threats.
- Continual improvement driven by actionable intelligence through outputs defined in:
  - Internal and external audits
  - Risk assessment
  - Executive involvement
  - Strategic best practices

Annex A of ISO 27001 lists 93 controls organized into four major themes:

1. Organizational Controls
2. People Controls
3. Physical Controls
4. Technological Controls

These controls map to the Statement of Applicability (SOA) through your organizations impact of Confidentiality, Integrity, and Availability.

Certification Process

The ISO 27001 certification process typically follows three stages. If successful, certification is valid for three years with annual surveillance audits for the first two years and a recertification audit at the end of the cycle to maintain compliance.

OVERVIEW OF ISO/IEC 27701

Scope & Applicability

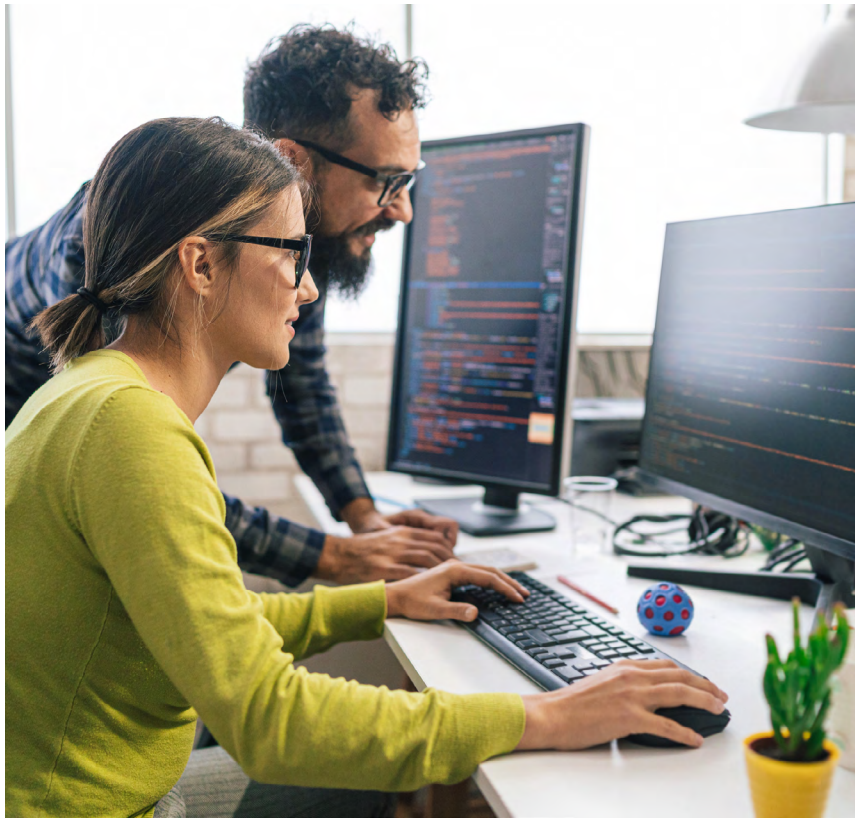
ISO/IEC 27701 focuses on privacy information management. It establishes a Privacy Information Management System (PIMS) that enables organizations to manage personally identifiable information (PII) in compliance with privacy laws and regulations. It applies to both data controllers and processors, making it especially valuable for industries that rely heavily on personal data, such as healthcare, finance, and technology.

Control Domains & Structure

Formerly an extension of ISO 27001, ISO 27701 has now evolved into a standalone privacy management standard, outlining specific requirements for building and maintaining a PIMS:

1. Roles and responsibilities for privacy management.
2. Processes for consent and data subject rights.
3. Requirements for third-party processor management.
4. Controls for cross-border data transfers.

The standard closely aligns with GDPR and other global privacy frameworks.



Certification Process

With the 2025 update, organizations may now pursue ISO 27701 certification independently, allowing greater flexibility for entities focused primarily on privacy compliance programs rather than full information security certification. Certification is valid for three years with annual surveillance audits.

OVERVIEW OF ISO/IEC 42001

Scope & Applicability

ISO/IEC 42001 is the first international standard for Artificial Intelligence Management Systems (AIMS). It provides a governance framework for ensuring responsible, transparent, and trustworthy AI. It applies to any organization developing, deploying, or using AI, particularly where systems impact individuals, sensitive data, or critical infrastructure.

Control Domains & Structure

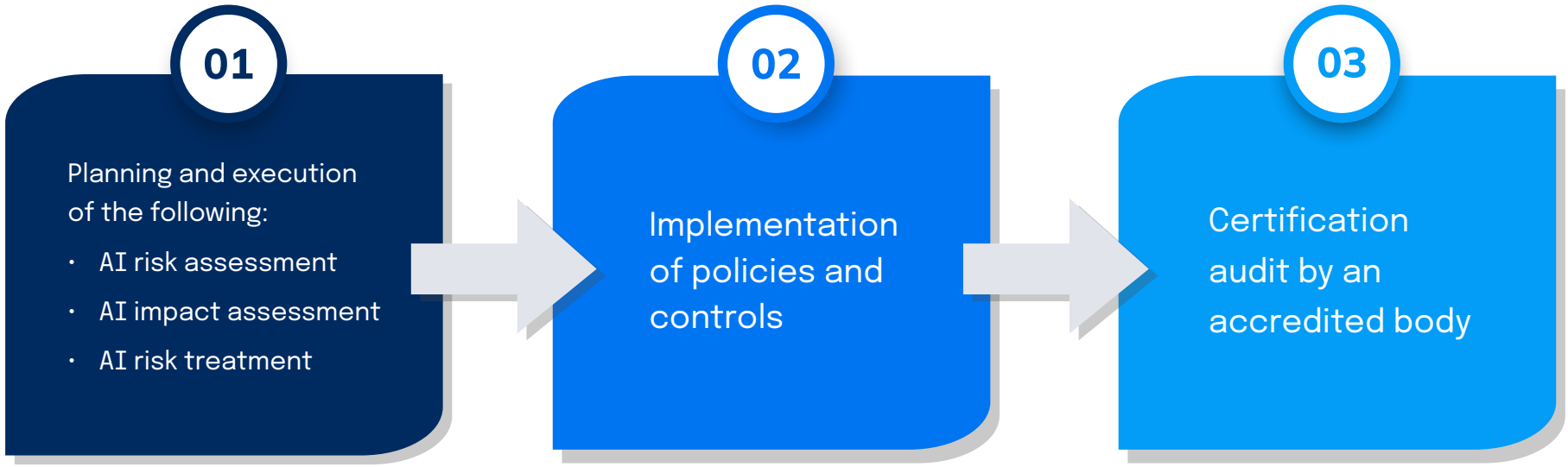
ISO 42001 follows a management systems model with the following domains:

- Governance and Accountability
- Risk Management
- Data and Model Management
- Transparency and Documentation
- Human Oversight

This ensures organizations demonstrate both technical maturity and ethical responsibility.

Certification Process

As the use of AI agents and autonomous systems accelerates across industries, organizations are under increasing pressure to demonstrate responsible governance and control. ISO 42001 certification provides a structured path for validating that AI technologies are deployed ethically, transparently, and with appropriate safeguards. The certification process includes:



KEY ROLES & STAKEHOLDERS

Certification requires collaboration across roles:

- **Executive Leadership**: Strategic oversight and resources
- **CISO/ISO**: Management of ISMS
- **Privacy Officer/DPO**: Oversight of PIMS and privacy regulations
- **AI Governance Leads**: Oversight of corporate AI governance
- **IT & Security Teams**: Implementation of technical controls
- **Risk Management Teams**: Risk assessments and treatment plans
- **Legal & Compliance Teams**: Ensure regulatory alignment
- **Employees**: Follow policies and training
- **External Certification Bodies**: Conduct audits and certification

BENEFITS & LIMITATIONS

ISO certifications provide measurable benefits but also pose challenges.

Benefits

- Enhanced security and privacy posture
- Global recognition
- Operational efficiency
- Customer and stakeholder trust
- Competitive advantage

Limitations

- Resource intensive
- Cultural change requirements
- Complex documentation
- Ongoing maintenance
- Scalability challenges for smaller organizations

Understanding these factors will help your organization effectively navigate any of the ISO certification processes.

MAINTAINING CERTIFICATION & RECERTIFICATION

ISO certifications are valid for three years, with annual surveillance audits required. Organizations must:

- Monitor and review ISMS, PIMS, and AIMS regularly
- Update policies and controls to reflect changes
- Train staff on evolving requirements
- Address nonconformities promptly
- Plan for recertification at the end of the cycle

These steps reflect a culture of continuous improvement and proactive risk management.

FURTHER RESOURCES / REFERENCES

ISO/IEC 27001:2022

ISO/IEC 27701:2019

ISO/IEC 42001:2023

360 Advanced