PECB - North America

ISO 42001 & AI Risk Management

PECB REGIONAL WEBINARS

Your Tour Guide: Dallas N. Bishoff

IAPP (iapp.org)

FIP | CIPM | CIPP | CIPT & Instructor

IEEE (ieee.org)

Certified Biometric Professional & Instructor

ISACA (isaca.org)

CDPSE | CGEIT | CISA | CISM | CRISC & Instructor (Retired)

ISC2 (isc2.org)

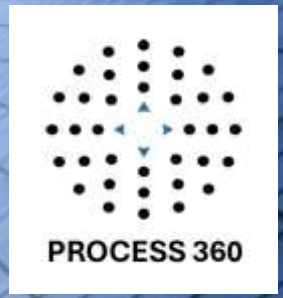
CCSP | CGRC | CISSP | HCISPP

ISO (iso.org)

9001 | 13485 | 20000 | 22301 | 27001 | 27701 | 37301 | 42001

Vanderbilt Law (law.vanderbilt.edu)

Executive Legal Certificate – Commercial and Business Law



Your Tour Guide: Dallas N. Bishoff

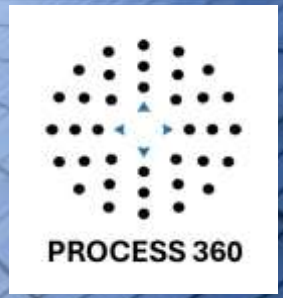
ISO Steering Committee 27 – Information Security, Cybersecurity, and Privacy Protection

ISO Steering Committee 42 – Artificial Intelligence

ISO Technical Committee 279 – Innovation Management

ISO Project Committee 302 – Audit of Management Systems

ISO Technical Committee 307 – Blockchain and Distributed Ledger Technologies (DLT)

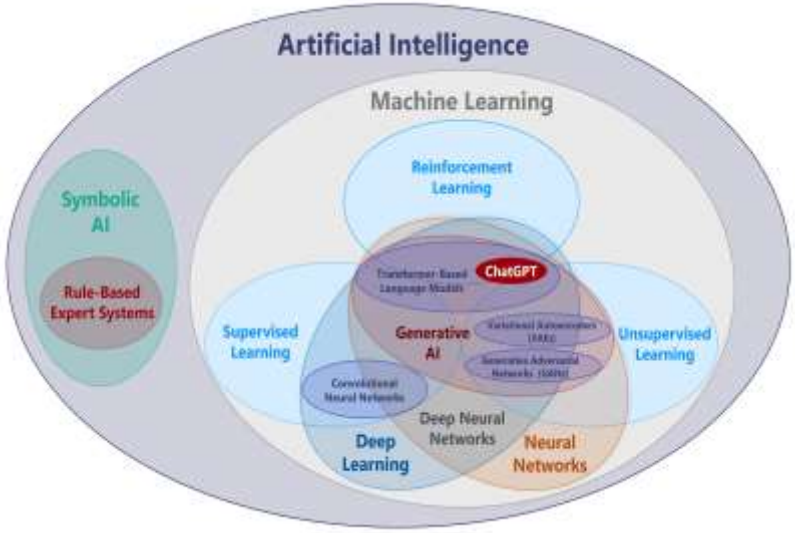


Agenda

1. Perspective is Everything
2. Major Challenges in the World of AI
3. Understanding ISO 42001
4. Understanding AI Risk Management
5. Getting Started

PERSPECTIVE IS EVERYTHING

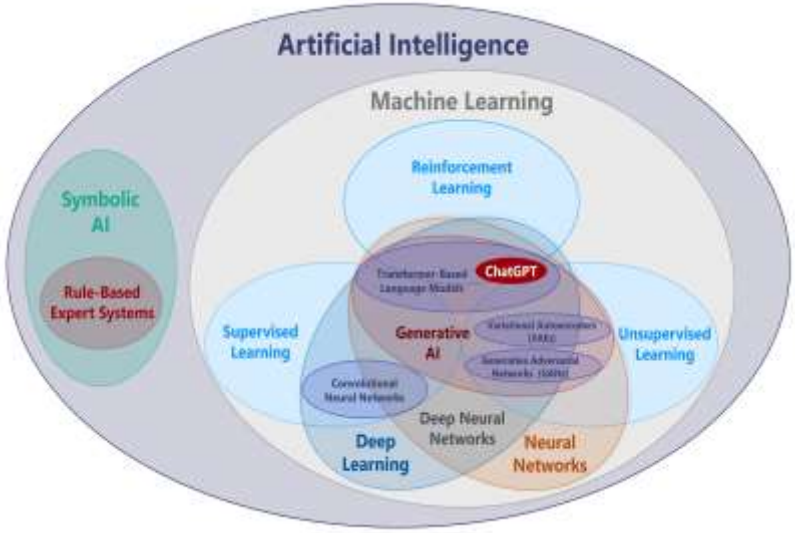
1. The Many Flavors of AI
2. AI is not Intelligent
3. The World of AI is Messy and Poetic
4. AI Will Rebalance Not Replace Human Labor
5. The Problem of AI Literacy



1956: Dartmouth Conference | 2000's Ethical and Illegal Outcomes | 2015: Governance

MAJOR CHALLENGES IN THE WORLD OF AI

1. Legal, Statutory, and Regulatory Roadmap
2. The Challenge of Governance
3. AI and Data Life Cyle Management
4. AI will rebalance but not reduce human labor
5. AI literacy is a major problem

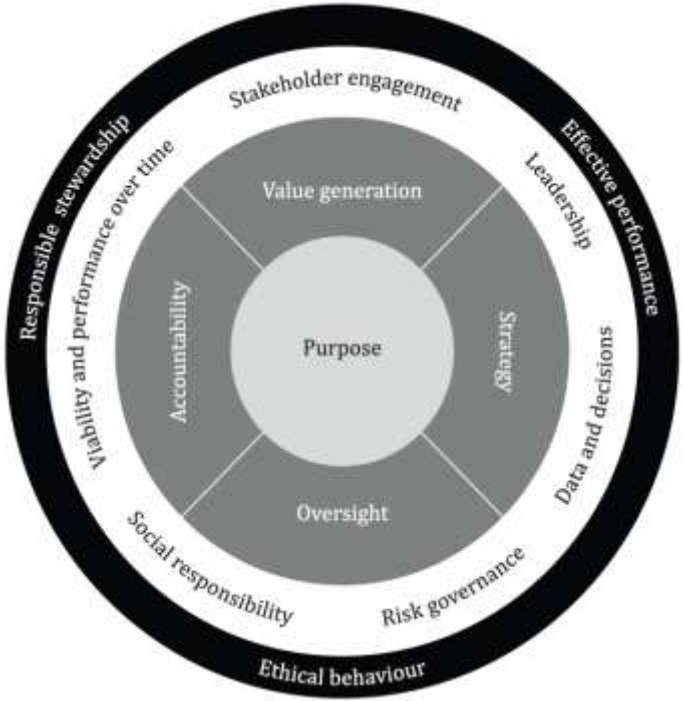


1956: Dartmouth Project | 2000's Ethical and Illegal Outcomes | 2015: Governance

THE CHALLENGES OF AI GOVERNANANCE

- AI governance should be integrated, not exist in a parallel universe.
- Allocation of roles and responsibilities is essential for governance.
- Proper resources are essential for success, but that is not always known.
- ISO 42001 needs to be integrated with your organizational policies

Diagram: ISO 37000:2021 Governance of Organizations - Guidance



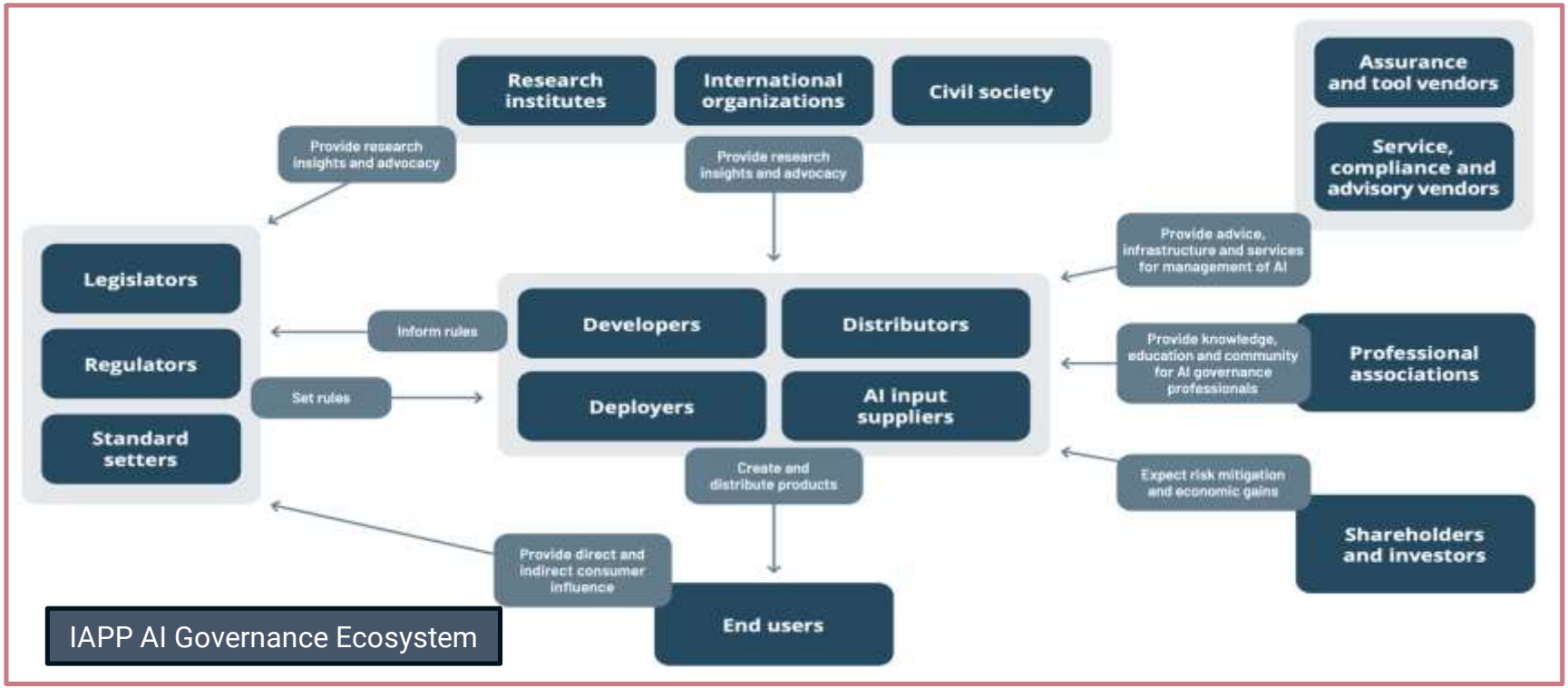
THE CHALLENGES OF AI GOVERNANANCE

The NIST AI Risk Management Framework (RMF) representation can be used to ensure control coverage.

- The governance functional area has five categories, with 17 total controls defined.
- The Map, Manage, and Measure areas can be useful when trying to identify control gaps.
- The companion AI RMF Playbook fills in certain gaps, like logging.

Diagram: NIST AI Risk Management Framework

THE CHALLENGES OF AI GOVERNANANCE



THE CHALLENGES OF AI GOVERNANANCE

The Cloud Security Alliance recently published the AI Control Matrix (AICM), which aligns with their Cloud Control Matrix (CCM). The are 18 domains with 243 controls. ISO 42001 only has 38 controls.

A&A	Audit & Assurance	IAM	Identity & Access Management
AIS	Application & Interface Security	IPY	Interoperability & Portability
BCR	Business Continuity Mgmt & Op Resilience	I&S	Infrastructure Security
CCC	Change Control & Configuration Management	LOG	Logging & Monitoring
CEK	Cryptography, Encryption & Key Management	MDS	Model Security
DCS	Datacenter Security	SEF	Sec. Incident Mgmt, E-Disc & Cloud Forensics
DSP	Data Security & Privacy	STA	Supply Chain Mgmt, Transparency & Accountability
GRC	Governance, Risk Management & Compliance	TVM	Threat & Vulnerability Management
HRS	Human Resources Security	UEM	Universal EndPoint Management

UNDERSTANDING ISO 42001– BACKGROUND

- **ISO oversees a worldwide federation of 175 countries that has been setting standards for AI since the early 2000s, which includes ISO 42001Information Technology – Artificial Intelligence – Management System (AIMS), published in December of 2023.**
- **There are over 26,000 ISO standards, but only about 80 management systems. The construct of an AI management system standard enables what are called integrated management systems (IMS), which allows organizations to glue the various ISO managements systems together.**
- **Without question, ISO 42001 is the most complex of all ISO management systems. While ISO 42001 maintains commonality with other management systems, there are novel differences in an AIMS which are presented in the webinar.**
- **ISO 42001 also anticipates that an organization will declare Responsible AI principles, which might align with the OECD list, the EU AI Act, or as otherwise determined by an organization.**

  - See the OECD Responsible AI Principles (https://www.oecd.org/en/topics/sub-issues/ai-principles.html)
  - See the EU AI Act, Recital 27 (https://artificialintelligenceact.eu/recital/27/)

UNDERSTANDING ISO 42001– BACKGROUND

Several of the ISO 42001 Annex A controls are evaluated against the Responsible AI principles elected by the organization:

- A.3 Internal Organization
- A.6.1 Management Guidance for AI System Development
- A.9 Use of AI Systems
- A.10 Third-Party and Customer Relationships

There are several ISO publications that can be leveraged to properly understand the intent and implementation of Responsible AI:

- ISO 6254:2025 Artificial Intelligence – Objectives and Approaches for Explainability and Interpretability of ML Models and AI Systems
- ISO 12791:2024 Artificial Intelligence – Treatment of Unwanted Bias in Classification and Regression Machine Learning Tasks
- ISO 12792:2025 Artificial Intelligence – Transparency Taxonomy of AI Systems
- ISO 24027:2021 Artificial Intelligence – Bias in AI Systems & AI Aided Decision Making
- ISO 24028:2020 Artificial Intelligence – Overview of Trustworthiness in AI
- ISO 24368:2022 Artificial Intelligence – Overview of Ethical and Societal Concerns

UNDERSTANDING ISO 42001– BACKGROUND

While most ISO management systems can be implemented without relying on other ISO standards, this is not the case with ISO 42001. Through out the management clauses, the standard cites a collection of related standards, which are covered below and in this webinar. Understanding these standards is necessary for proper implementation, and defense during the AIMS audit:

- ISO 5229, a multi-part series on machine learning (ML) data quality
- ISO 5338:2023 Artificial Intelligence – AI System Life Cycle Processes
- ISO 8183:2023 Artificial Intelligence – Data Life Cycle Framework
- ISO 22989:2022 Artificial Intelligence Concepts and Terminology
- ISO 23894:2023 Artificial Intelligence – Guidance on Risk Management
- ISO 24030:2024 Artificial Intelligence – Use Cases
- ISO 24368:2022 Artificial Intelligence – Overview of Ethical and Societal Concerns
- ISO 38507:2022 Governance of IT – Governance Implications of the Use of AI
- ISO 42005:2025 Artificial Intelligence – AI System Impact Assessment

UNDERSTANDING ISO 42001– CLAUSES

4	Context of the Organization
5	Leadership
6	Planning
7	Support
8	Operation
9	Performance Evaluation
10	Improvement

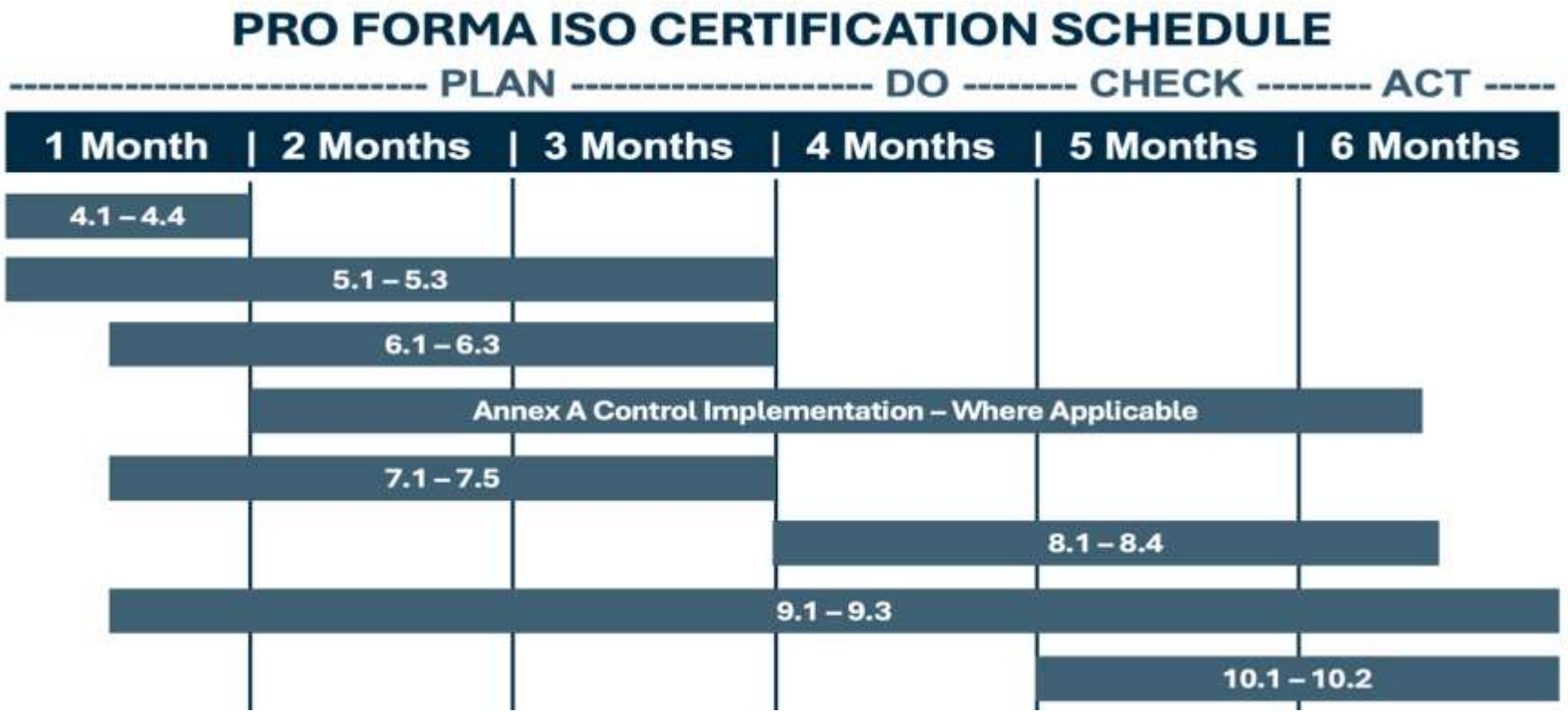
ISO 42001 is an Annex SL structured management system

By design you can glue it together with other management systems like ISO 9001, 27001, and 27701.

UNDERSTANDING ISO 42001– THE ANNEXES

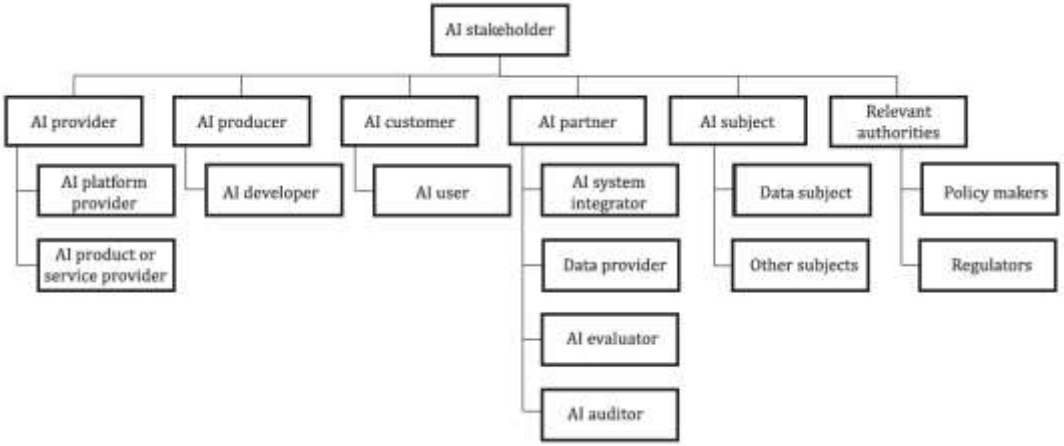
A	Reference Control Objectives and Controls (10 Control Areas with 38 Controls)
B	Implementation Guidance for AI Controls
C	Potential AI-Related Organizational Objectives and Risk Sources
D	Use of the AI Management System Across Domains or Sectors

UNDERSTANDING ISO 42001



4 – CONTEXT OF THE ORGANIZATION

- **Clause 4.1 Understanding the Organization and Its Context**
  - ISO 42001 introduces AI stakeholder roles depicted below, and further explained in ISO 22989, Clause 5.19. The roles will appear in your AIMS scope statement (Clause 4.3)



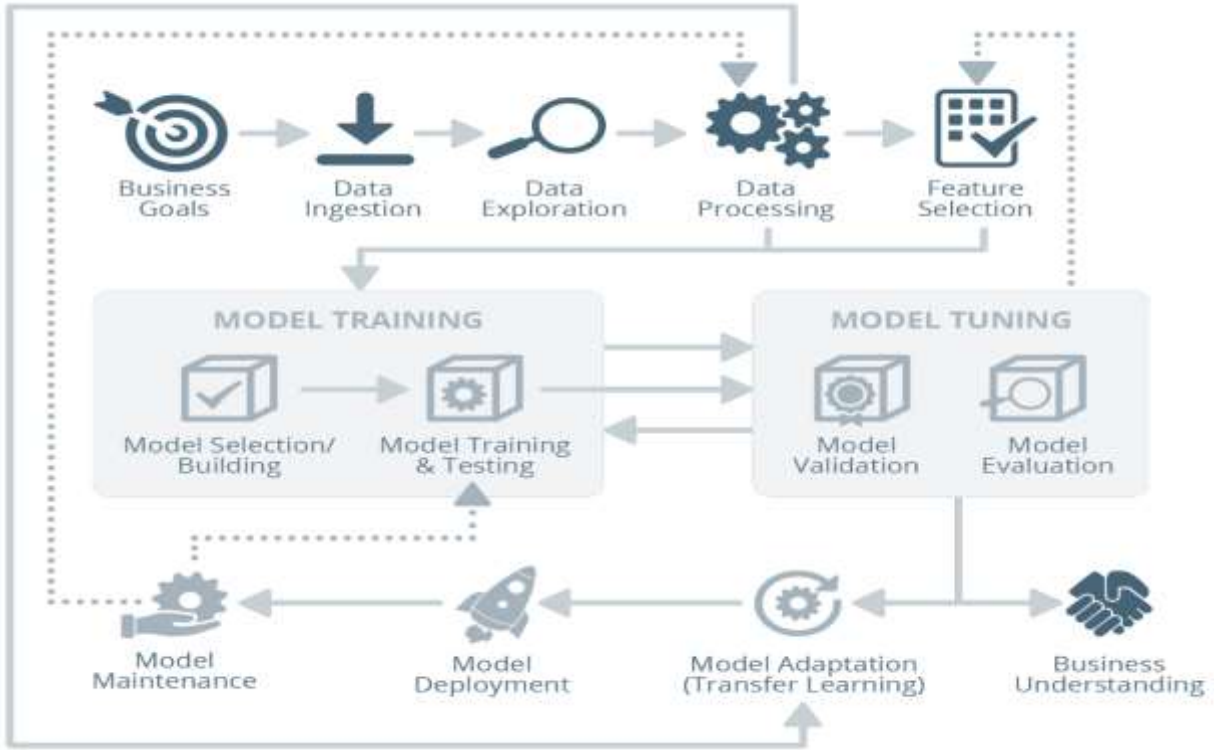
The roles that your organization elects will change your implementation. The roles are declared in the ISO 42001 scope statement.

NOTE: The EU AI Act roles are different: deployer; importer; distributor, and authorized representative.

4 – CONTEXT OF THE ORGANIZATION

- AI Producer
- AI Provider
- AI User
- AI Partner

NOTE: The roles change the implementation



4 – CONTEXT OF THE ORGANIZATION

Clause 4.1 Understanding the Organization and Its Context

- As required by ISO 27001 Clause 4.1, organizations will have to identified and keep up-to-date a listing of the international statutory, regulatory, and contractual requirements.

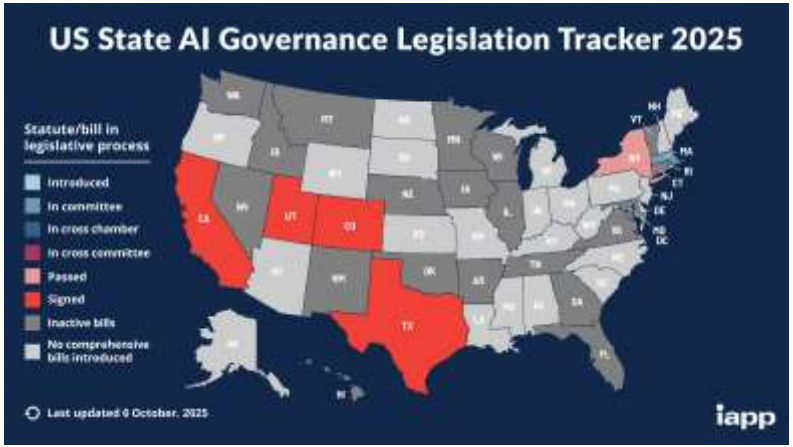
Your implementation may span geographic boundaries. This will be an important consideration. The EU AI Act has a different set of roles defined.

See https://iapp.org/resources/article/global-ai-legislation-tracker/#global-ai-map_

4 – CONTEXT OF THE ORGANIZATION

Clause 4.1 Understanding the Organization and Its Context

- As required by ISO 27001 Clause 4.1, organizations will have to identified and keep up-to-date with the evolving U.S. State laws for AI. Some States provide ‘safe harbor’ related to ISO 42001.



As provided for in the 10th Amendment, until a U.S. federal law exists, the States have the lead on regulating AI.

See https://iapp.org/resources/article/us-state-ai-governance-legislation-tracker/#state-ai-governance-law-map

5 – Leadership

5.1 Leadership and Commitment

- Expectations for ‘top management’

5.2 AI Policy

- Framework to set objectives (6.2)
- Commitment to meet requirements
- Refer to other organizational policies
- ISO 38507 – AI Governance

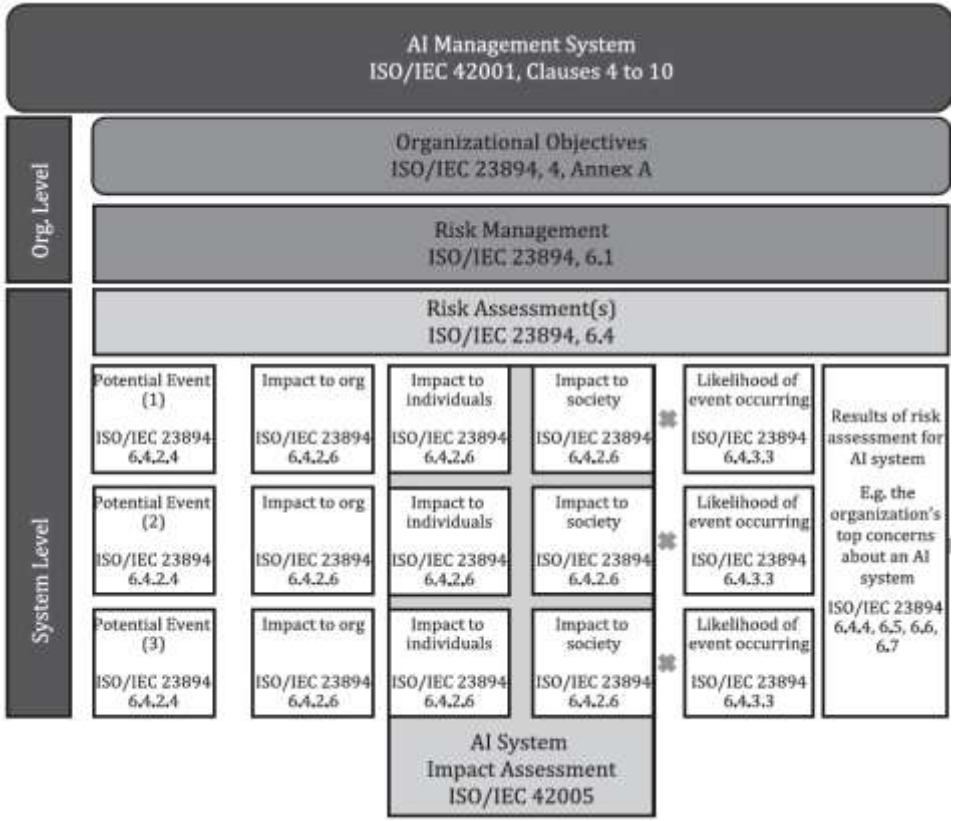
5.3 Roles, Responsibilities and Authorities

- Management system is conforming
- Performance reporting (9.1)

NOTE: Guidance in Annex B, along with other sources like the NIST AI RMF.

6 – PLANNING

- ISO 42001
- ISO 23894
- ISO 42005

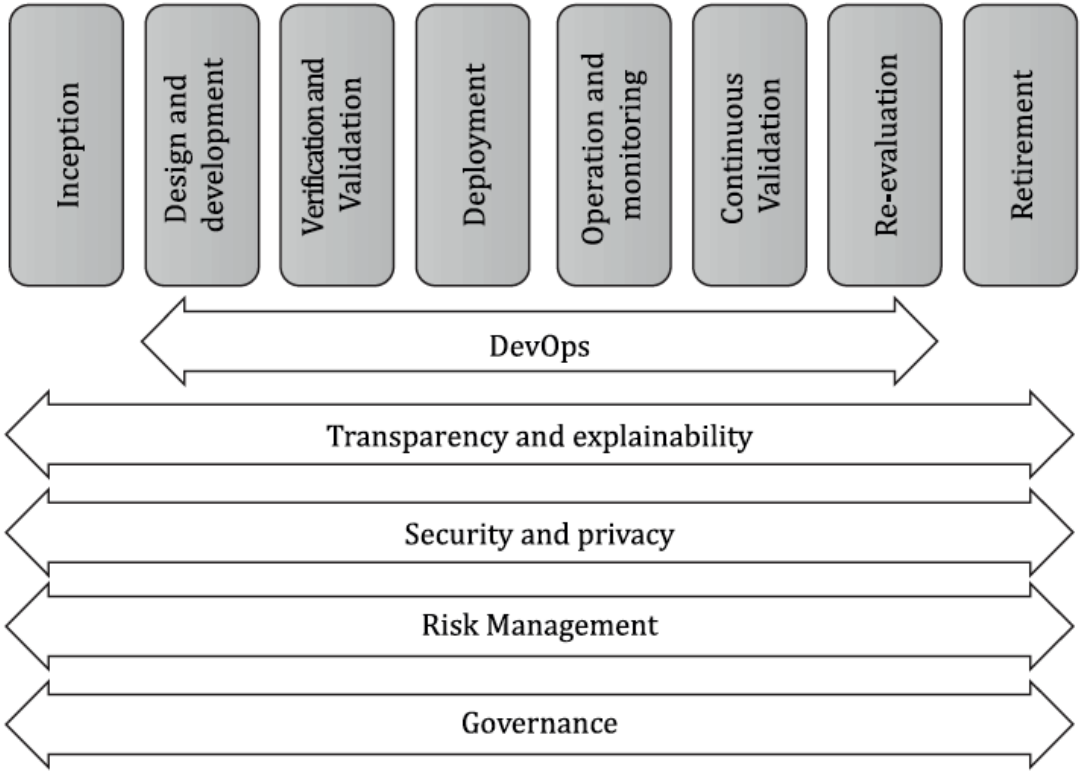


6 – PLANNING

ISO 5338 AI Life Cycle

- Inception
- Design and Development
- **Verification and Validation**
- Deployment
- Operation and Monitoring
- **Continual Validation**
- **Re-Evaluation**
- Retirement

NOTE: In a traditional SDLC, when you establish the system knows that 1+1= 2 you generally do not perform ongoing validation in production. AI systems are different, and behavior evolves.



6 – PLANNING

6.1.1 General
- ISO 5338, ISO 38507, and ISO 23894
- NOTE 2: AI Systems may need separate artifacts

6.1.2 AI Risk Assessment
- Documented process
- Identify risks that aid or prevent objectives (6.2)
- Considers the AI System Impact Assessment
- One or more risk assessment artifacts

6.1.3 AI Risk Treatment
- Documented process
- Select risk treatment options
- One or more Statement of Applicability (SoA)

6.1.4 AI System Impact Assessment
- ISO 42005 – Persons, groups of persons, societies

Visualization of risk management process by ISO 31000

6 – PLANNING

6.2 AI Objectives and Planning to Achieve Them

- Do not restate the requirements
- Measurable and achievable
- Relationship to Clause 9.1

6.3 Planning of Changes

- Deming Model (P-D-C-A)
- Change creates risk
- Identify the changes
- Identify the plan(s) to change

7 – Support

7.1 Resources
- A.4 Resources for AI Systems

7.2 Competence
- Clause 5.3 Roles, Responsibilities & Authorities
- A.3 Internal Organization
- A.4.6 Human Resources

7.3 Awareness

7.4 Communication
- Internal and External
- A.3.3 Reporting of Concerns
- A.8 Information for Interested Parties of AI Systems

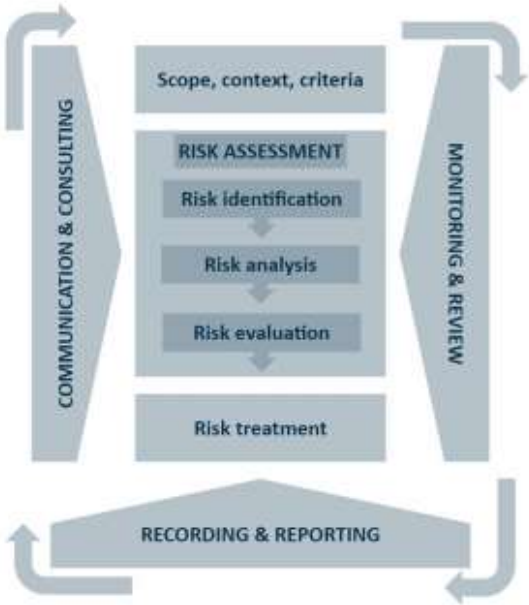
7.5 Documented Information
- Most Annex A controls require documentation
- A.4.2 Resource Documentation

8 – OPERATION

8.1 Operational Planning and Control
8.2 AI Risk Assessment
8.3 AI Risk Treatment
8.4 AI System Impact Assessment

NOTE: Make sure that you document the planned interval, along with the types of triggers that would force reconsideration.

NOTE: Do not overwrite the risk artifacts. They need to be versioned to support traceability.



Visualization of risk management process by ISO 31000

9 – PERFORMANCE EVALUATION

9.1 Monitoring, Measurement, Analysis and Evaluatio

- Make sure you include the AI Objectives (6.2)

9.2 Internal Audit

- 9.2.1 General
- 9.2.2 Internal Audit Programme

9.3 Management Review

- 9.3.1 General
- 9.3.2 Management Review Inputs
- 9.3.3 Management Review Results

NOTE: ISO 17021-1 is the primary audit & certification reference, augmented by ISO 42006. ISO 19011 explains all aspects of audit management.

10 – IMPROVEMENT

10.1 Continual Improvement
10.2 Nonconformity and Corrective Action

ANNEX A – PROBLEMATIC CONTROLS

AI Incidents
- A.3.3 Reporting of Concerns
- A.8.3 External Reporting
- A.8.4 Communication of Incidents
- A.10.4 Customers

A.5 Assessing Impacts of AI Systems (4)

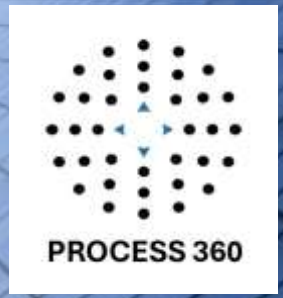
A.6 AI System Life Cycle (9)

A.7 Data for AI Systems (5)

Q&A Session

Contact

- Website: www.process360.com
- Phone: 214-216-3950
- Cell: 505-999-7511
- Email: dallas@process360.com
- LinkedIn: https://www.linkedin.com/in/dallasbishoff/



For any questions or comments, you can contact us below:

support@pecb.com