

Whitepaper



# Controllo

## AI-Powered **EU AI** **Act** Compliance

Simplifying Compliance Automation for  
Multi Framework Management

# Table of Contents

No	Agenda for today	Page
01.	What is EU AI Act and Why it Matters	3 - 6
02.	Understanding EU AI Act	7 - 8
03.	Who Needs to Comply with EU AI Act?	9
04.	Key Terms in EU AI Act	10 - 11
05.	Controllo for EU AI Act & Risk Management	12 - 17
06.	Common Compliance Challenges	18 - 20
07.	EU AI Act Compliance Journey in Controllo	21 - 23
08.	Benefits of Using Controllo	24 - 27

# 01 What is EU AI Act and Why it Matters

The EU Artificial Intelligence Act (EU AI Act) is the world's first comprehensive regulation governing the development, deployment and use of artificial intelligence across the European Union.

Officially adopted in 2024 and entering into force in phases starting 2025, the regulation aims to ensure AI systems are safe, transparent, ethical and respect fundamental rights.

It introduces a risk-based classification for AI systems, ranging from minimal risk (e.g. spam filters) to unacceptable risk (e.g. social scoring) with stringent requirements imposed on high-risk AI (e.g. AI in healthcare, finance, public services, law enforcement).



# 01 What is EU AI Act and Why it Matters

## Core Components of EU AI Act



### Risk Based Classification Framework

Categorizes AI systems into unacceptable, high, limited, or minimal risk levels.



### High Risk AI Obligations

Imposes strict requirements on high-risk AI to ensure safety, accountability, and human oversight.



### Prohibited AI Practices (Unacceptable Risk)

Bans AI systems that pose unacceptable threats to rights, such as social scoring and manipulative surveillance.



### Transparency & Limited-Risk AI

Mandates user disclosure when interacting with AI or AI-generated content.

# 01 What is EU AI Act and Why it Matters

## Core Components of EU AI Act



### Governance and Enforcement

Establishes oversight via the European AI Office and national authorities.



### Obligations by Actor Role

Assigns compliance duties based on roles such as provider, user, or importer.



### Post-Market Monitoring & Incident Reporting

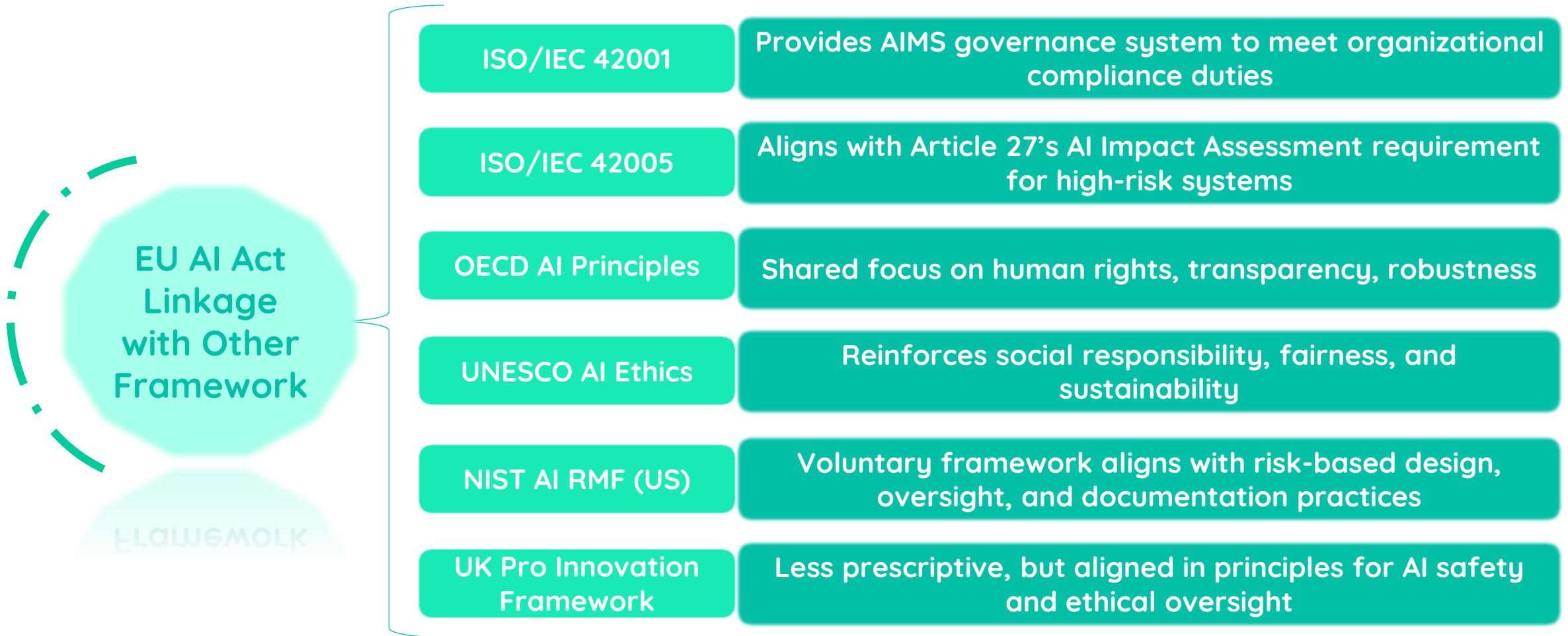
Requires ongoing risk monitoring and reporting of serious incidents after deployment.



### Extra-Territorial Scope

Applies to any AI system impacting EU citizens, regardless of the provider's location.

# 01 What is EU AI Act and Why it Matters



The EU AI Act is not only a legal mandate but a hub that connects the world's AI ethics, governance, and risk frameworks.

# 02 Understanding EU AI Act

## EU AI Act & ISO/IEC 42001 Compliance Mapping

EU AI Act Component	ISO/IEC 42001	Mapping/Compliance Strategy
Risk-Based Classification (Title II)	6.1.2 Risk Assessment Process	ISO/IEC 42001 requires AI-specific risk assessments aligned with business impact — aligns with EU’s risk-tiering model.
High-Risk AI Requirements (Title III, Chapter 2)	8.1–8.3 Operational Planning & Control	ISO requires control over data quality, human oversight, robustness, and transparency—matching EU AI Act criteria.
Data Quality & Governance	8.2.1 Data Management	ISO mandates data relevance, accuracy, and bias reduction—core to EU AI Act’s requirements for high-risk AI.
Transparency Obligations (Art. 52)	6.1.3 Impact Assessment, 7.4 Communication	ISO requires informing stakeholders and ensuring human-understandable explanations—matching EU AI transparency rules.
Human Oversight	8.3.2 Human Oversight Mechanisms	ISO defines processes to ensure human control over AI outcomes—directly fulfilling EU’s oversight mandate.
Technical Documentation (Art. 11)	7.5 Documented Information	ISO requires documenting all AIMS processes and system behavior—aligns with conformity documentation requirements.

# 02 Understanding EU AI Act

## EU AI Act & ISO/IEC 42001 Compliance Mapping

EU AI Act Component	ISO/IEC 42001	Mapping/Compliance Strategy
Post-Market Monitoring (Art. 61)	9.1 Monitoring, Measurement, Analysis, Evaluation	ISO requires ongoing performance monitoring and effectiveness checks—supporting EU AI Act’s post-deployment monitoring.
Incident Reporting (Art. 62)	10.1 Nonconformity & Corrective Action	ISO mandates reporting and corrective action for AI system failures—supports EU’s reporting timelines.
Prohibited AI Systems (Title II, Art. 5)	4.1–4.3 Purpose, Scope, Context	ISO supports identifying prohibited/undesirable use cases during context definition—enables proactive exclusion.
Governance & Accountability	5.3 Roles, Responsibilities, Authorities	ISO explicitly mandates assigning AI-specific accountability—supporting the EU AI Act’s provider-user obligations.
Compliance with EU Law (General)	6.1.4 Legal/Regulatory Requirements	ISO requires identification and compliance with applicable laws like the EU AI Act—acts as the compliance umbrella.
Audit & Conformity Assessment	9.2 Internal Audit; 9.3 Management Review	ISO includes internal audits and review mechanisms that support external audits under EU AI Act’s conformity process.



# 03 Who Needs to Comply with EU AI Act

Any organizations across all industries world-wide that develops, deploys, or relies on AI systems



## 04 Key Terms to Comply with EU AI Act



**Complying with the EU AI Act is not just about avoiding fines, it's about enabling ethical, safe, and globally acceptable AI practices that unlock trust, markets, and long-term sustainability.**

## 04 Key Terms to Comply with EU AI Act



Complying with the EU AI Act is not just about avoiding fines, it's about enabling ethical, safe, and globally acceptable AI practices that unlock trust, markets, and long-term sustainability.

## 05 Controllo for EU AI Act & Risk Management



Controllo is an AI-powered compliance automation platform designed to automate and simplify Compliance audits.

Controllo is built by auditors and tech professionals who understands that today's modern team needs rapid AI automation and transparency  
- not another **spreadsheet**.

# 05 Controllo for EU AI Act & Risk Management

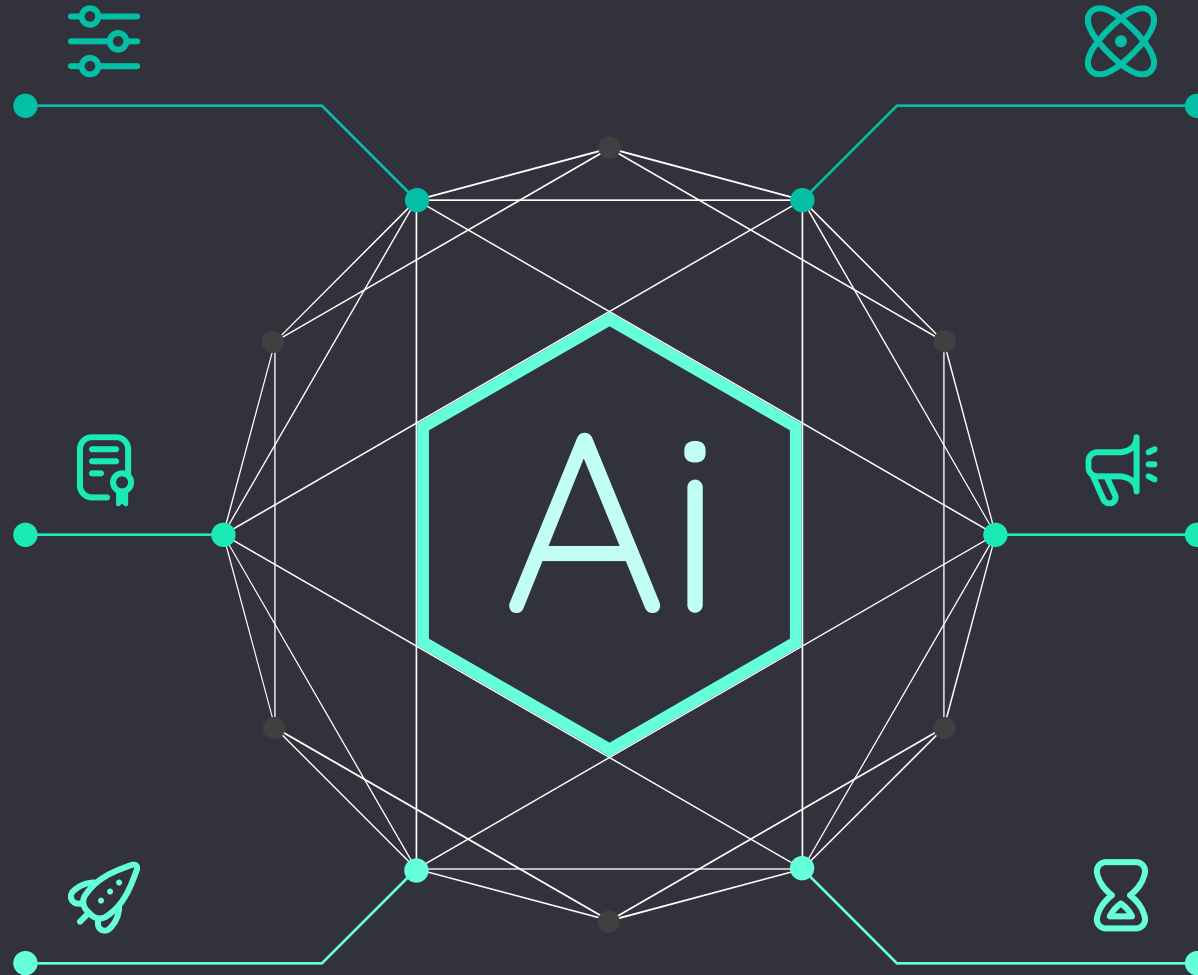
## The use of Artificial Intelligence (Ai) in Controllo

### Controls Mapping

AI elegantly harmonizes similar controls across diverse frameworks

Spanning a spectrum of 20+ leading compliance frameworks

Accelerates compliance while minimizing redundancy



### Smart Insights

Deep Intelligence AI powers actionable smart insights

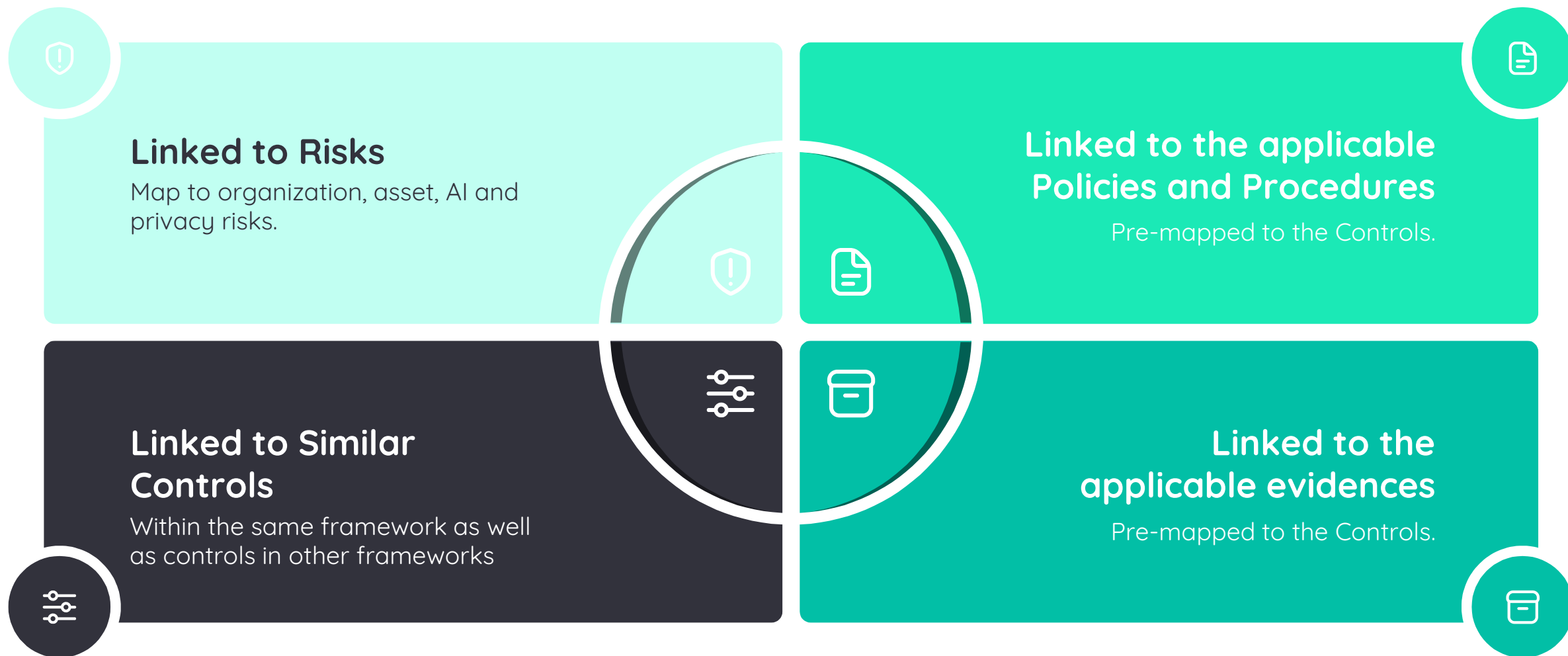
Get alerts: 1 more evidence can fulfill many controls across frameworks

Informed decisions and expedited compliance fulfilment

# 05 Controllo for EU AI Act & Risk Management

## Control Relationships in Controllo

Controllo has **20+** frameworks with over **33,000** control relationships.



# 05 Controllo for EU AI Act & Risk Management

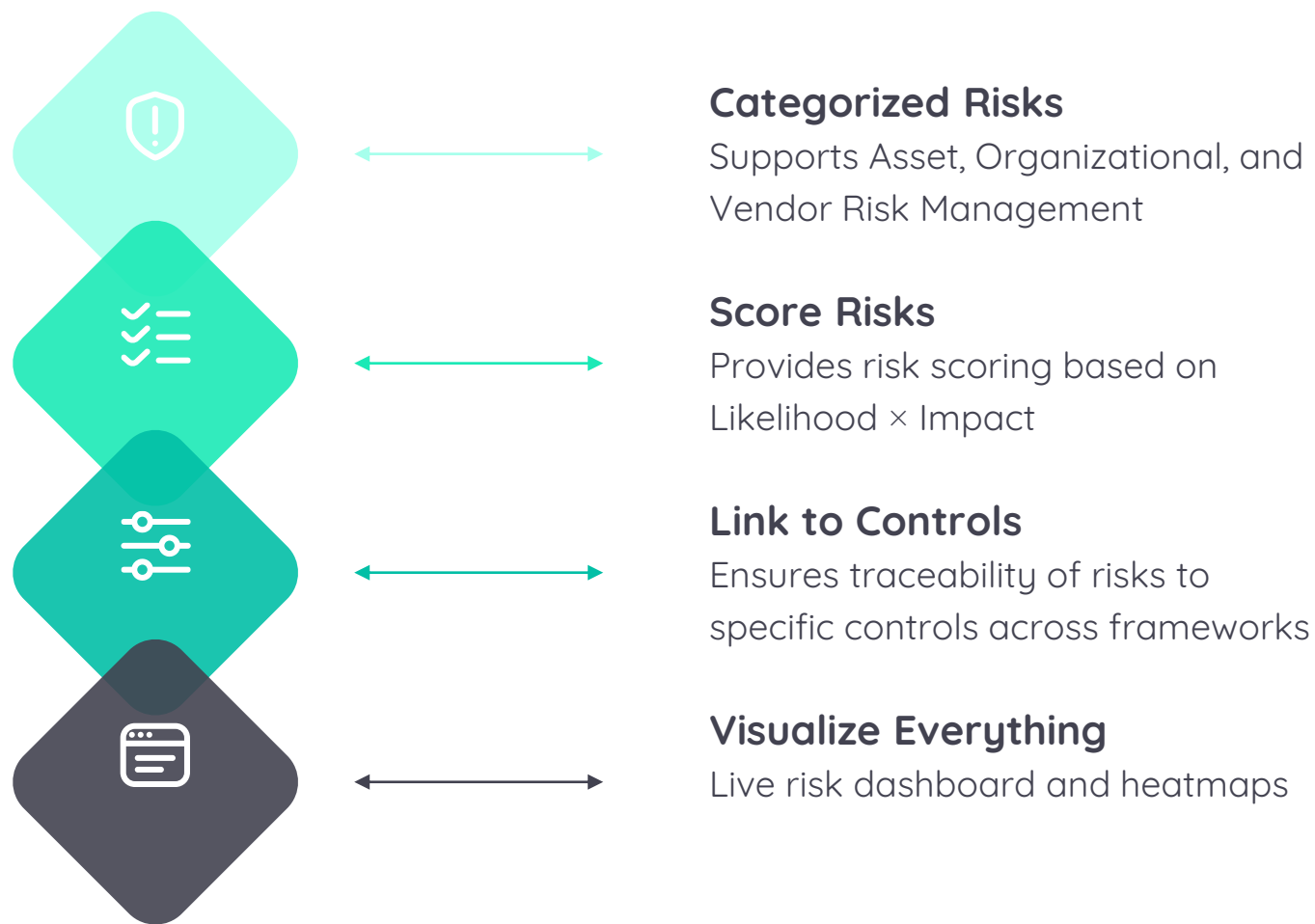
## Integrations in Controllo

Controllo can integrate with the below cloud platforms:



# 05 Controllo for EU AI Act & Risk Management


At Controllo, we've operationalized risk management by aligning our platform with the **NIST SP 800-30 & 37** framework—a globally accepted methodology for conducting risk assessments.



On the next slides,  
see how Controllo  
makes risk  
management  
effortless and audit-  
ready.



# Controllo for EU AI Act

Controllo

Dashboard

Dashboard

Risk Management

Privacy

Artificial Intelligence

Audit

Risks

Assets

Organization Risks

Vendors

Data Flow

Privacy Assessment

AI Systems

Audit Frameworks

Evidences

Policy & Procedures

SECURA

KC

EU AI Act

Search controls...

EU AI Act

GENERAL PROVISIONS

PROHIBITED AI PRACTICES

Article 5 Prohibited AI Practices

Article 5.1

The following AI practices shall be prohibited:

Article 5.2

The use of real-time remote biometric identification systems in publicly accessible spaces for the purposes of law enforcement for any of the objectives referred to in paragraph 1, f

Article 5.3

66%

For the purposes of paragraph 1, first subparagraph, point (h) and paragraph 2, each use for the purposes of law enforcement of a real-time remote biometr...

Article 5.4

66%

Without prejudice to paragraph 3, each use of a real-time remote biometric identification system in publicly accessible spaces for law enforcement purposes ...

Article 5.7

66%

The Commission shall publish annual reports on the use of real-time remote biometric identification systems in publicly accessible spaces for law enforce...

Article 5.5

A Member State may decide to provide for the possibility to fully or partially authorise the use of real-time remote biometric identification systems in publicly acc...

Article 5.6

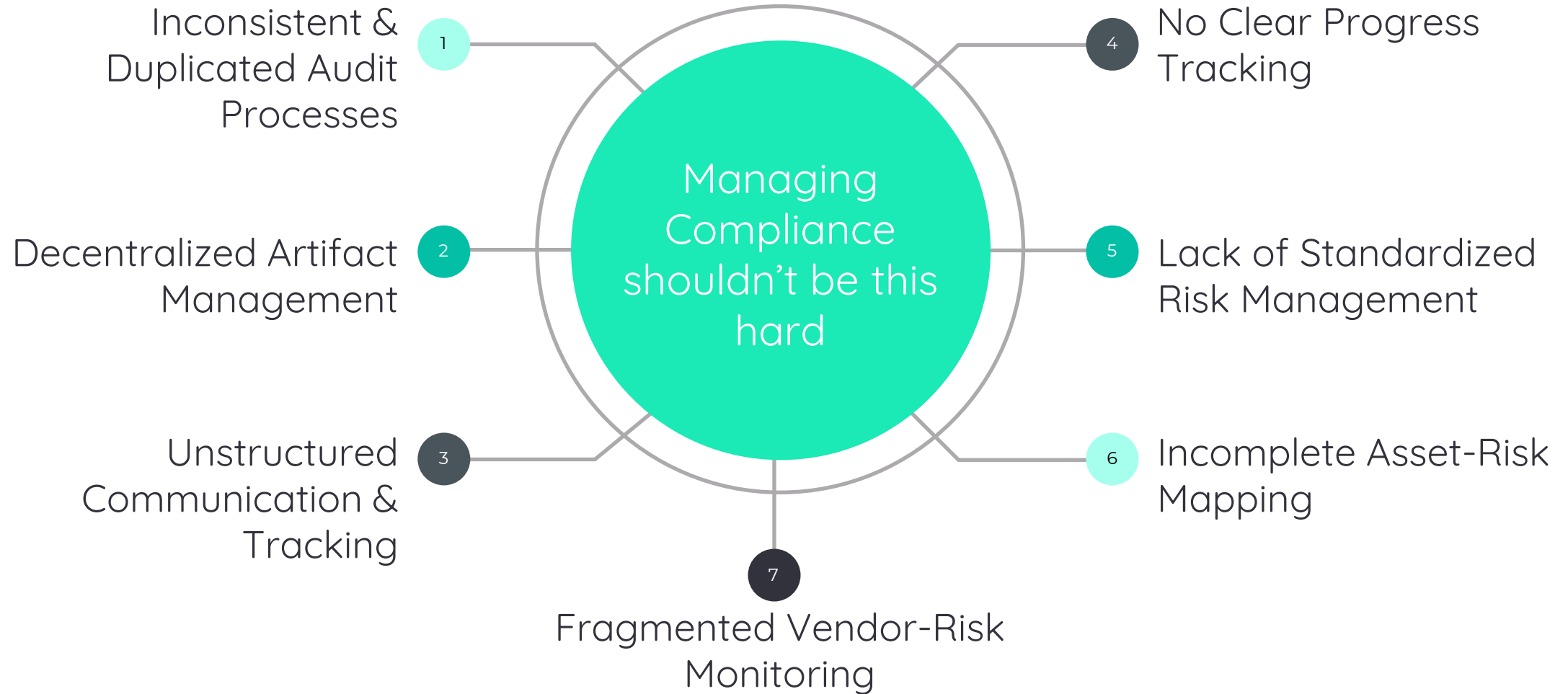
National market surveillance authorities and the national data protection authorities of Member States that have been notified of the use of real-time remote bio...

Article 5.8

This Article shall not affect the prohibitions that apply where an AI practice infringes other Union law.

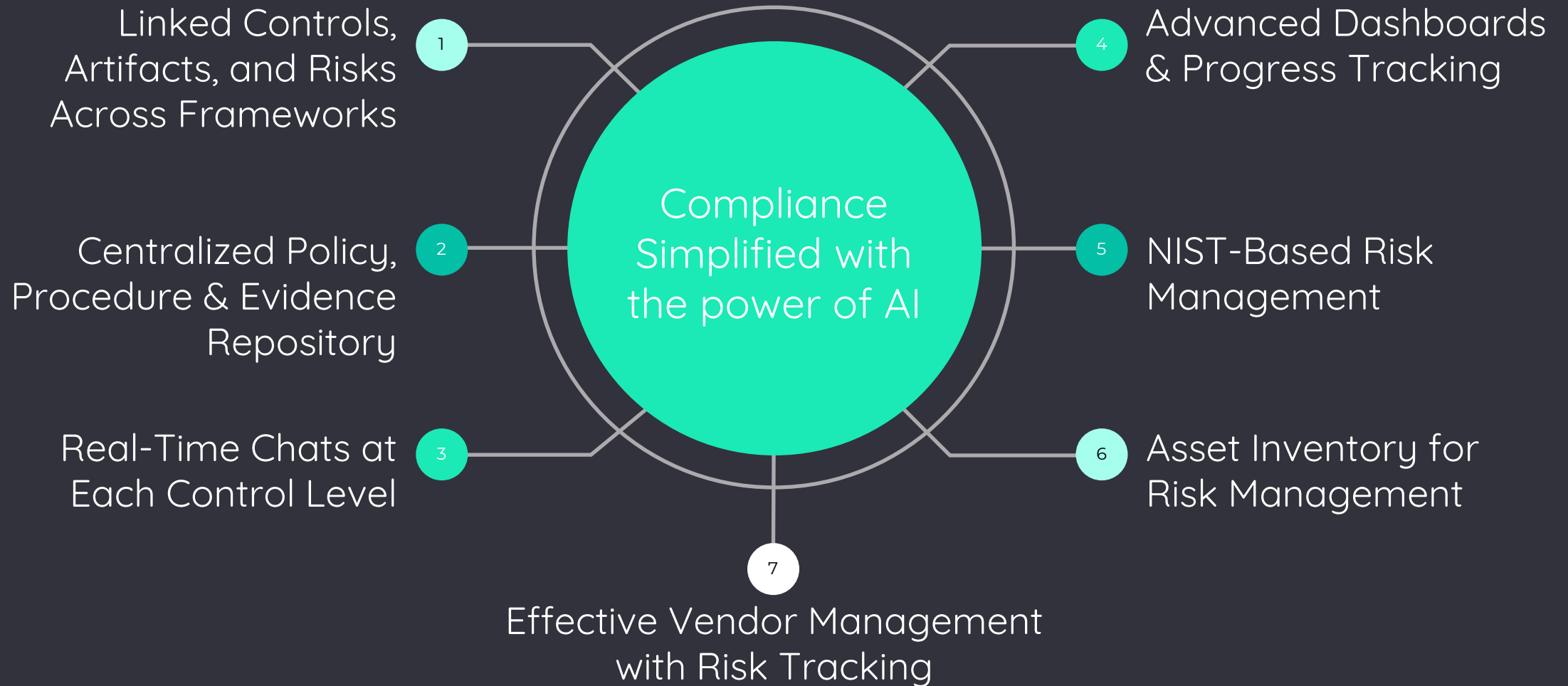
HIGH RISK AI SYSTEMS

## 06 Common Compliance Challenges



# 06 Common Compliance Challenges

## How Controllo Solves Compliance Challenges



# 06 Common Compliance Challenges

## AI Challenges Solved by Controllo

AI Model Risk  
Classification

AI Bias & Fairness  
Audits

Algorithmic  
Transparency &  
Explainability

Model Lifecycle  
Governance

Training Data  
Compliance &  
Provenance

Automated  
Decisions  
Auditability

Model Validation  
and Testing  
Documentation

AI Incident  
Logging and  
Escalation

Third-Party AI  
Risk Management

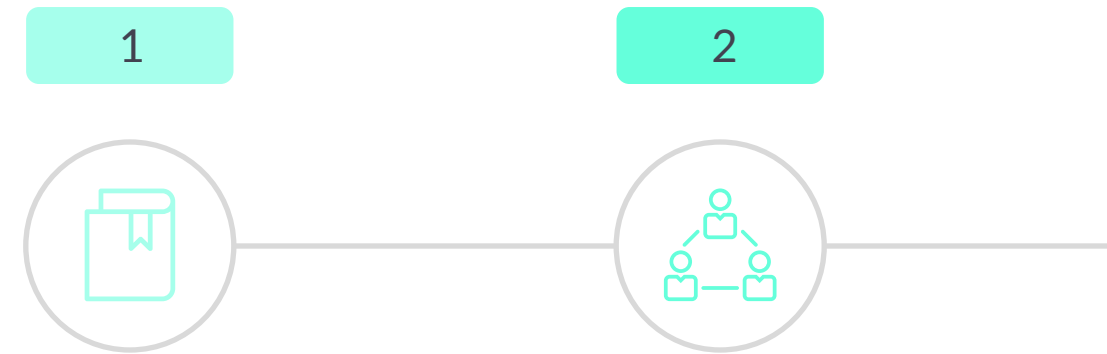
AI-Specific  
Regulatory  
Mapping

AI-Powered  
GRC  
Compliance  
Tool

# 07 EU AI Act Compliance Journey in Controllo

## Accelerate Your EU AI Act Journey with Controllo

A smarter way to manage controls, evidence, and risk across teams-aligned with EU AI Act and beyond.



### EU AI Act Preloaded Framework

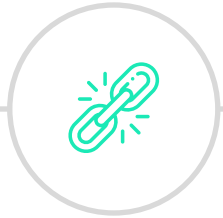
Choose the EU AI Act Framework and Controllo comes with all control requirements built in. The platform guides you through every mandatory requirements, expectation, and evidence requirement.

### Role Assignment

Assign ownership across IT, HR, DevOps, and Legal or any other department-everyone has visibility.

# 07 EU AI Act Compliance Journey in Controllo

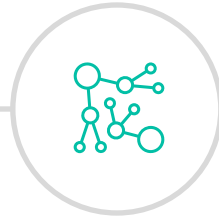
3



## Policy & Evidence Upload

Use prebuilt templates or upload existing documents. Your controls, risks, and evidence are linked across frameworks like SOC 2, ISO, CCM, DORA, and NIST. Implement once, reuse everywhere.

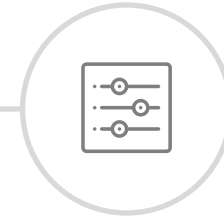
4



## AI-Powered Control Mapping

Controls from ISO 42001:2023 automatically map to SOC 2, ISO 27001, ISO 27701, ISO 22301, CCM, DORA, NIST, and many more.

5



## Risk Inventory

Track and assess risks at the asset, vendor, and organization levels. Toggle and do risk management from the platform itself based on NIST 800-30 classification.

# 07 EU AI Act Compliance Journey in Controllo

6



## Collaboration & Audit Trail

Use control-specific chat, discuss tasks, and track all activity in one place. Get email notifications, so you don't miss out anything.

7

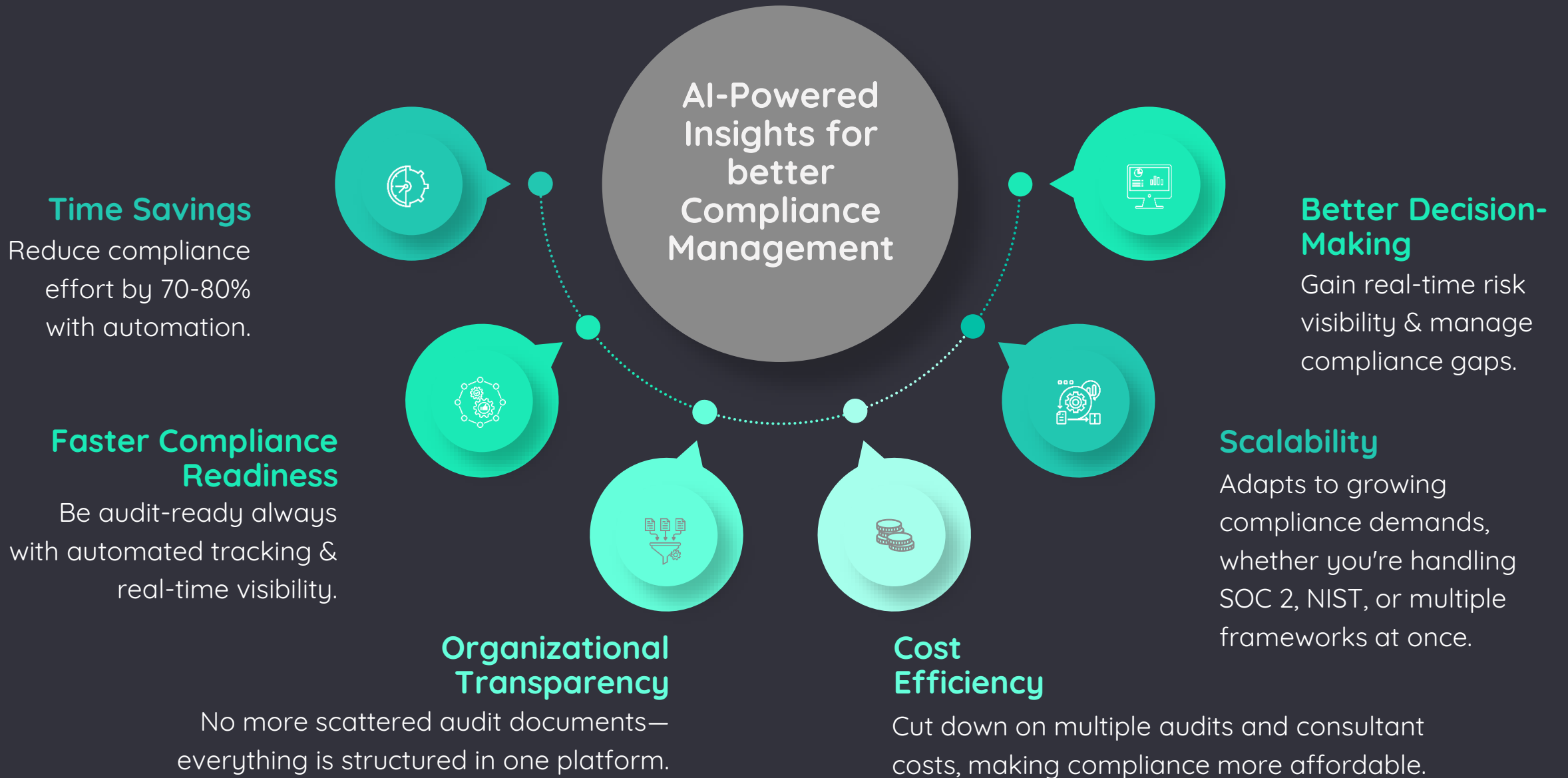


## Audit Readiness Dashboard

Visualize progress across various Frameworks with control-level drilldowns. Have visibility into your risk posture through a separate risk dashboard.

Stay Aligned,  
Stay Ready

# 08 Benefits of Using Controllo





## 08 Benefits of Using Controllo



### Time Savings

**Reduce compliance effort by 70-80% with automation.** Controllo automates the most tedious aspects of compliance—like evidence collection, control mapping, and audit prep—so your teams can focus on execution instead of administration. Linked controls across multiple frameworks eliminate duplication. Built-in templates streamline every stage, reducing manual workload and enabling you to reach compliance milestones faster.

### Faster Compliance Readiness

**Be audit-ready always with automated tracking and real-time visibility.** No more scrambling before audits. With real-time dashboards, evidence progress tracking, and auditor-ready document templates, Controllo ensures you always know your current status. Audit readiness becomes a continuous process—not a once-a-year panic. Alerts and automated workflows keep everyone on track.

### Organizational Transparency

**No more scattered audit documents—everything is structured in one platform.** Controllo acts as your single source of truth for all things compliance. Store policies, procedures, and evidences in one secure, searchable repository. Each control has a centralized workspace with ownership, chat history, uploaded artifacts, and implementation notes—eliminating silos and enhancing collaboration between security, IT, legal, HR, and leadership.

## 08 Benefits of Using Controllo



### Cost Efficiency

**Cut down on multiple audits and consultant costs, making compliance more affordable.** With smart automation and AI-powered cross-framework mapping, Controllo helps you reuse your work across standards—reducing audit duplication and the need for external consulting. You gain efficiency, minimize audit prep timelines, and reduce dependence on manual interventions, making compliance more cost-effective and scalable.

### Scalability

**Adapts to growing compliance demands.** Controllo grows with you. Start with EU AI Act and easily expand to ISO 27001, NIST, GDPR, HIPAA, or DORA. The platform intelligently links overlapping controls and artifacts, so you can manage multiple standards from a single pane of glass. Whether you're entering new markets or scaling your security program, Controllo keeps you aligned and audit-ready.

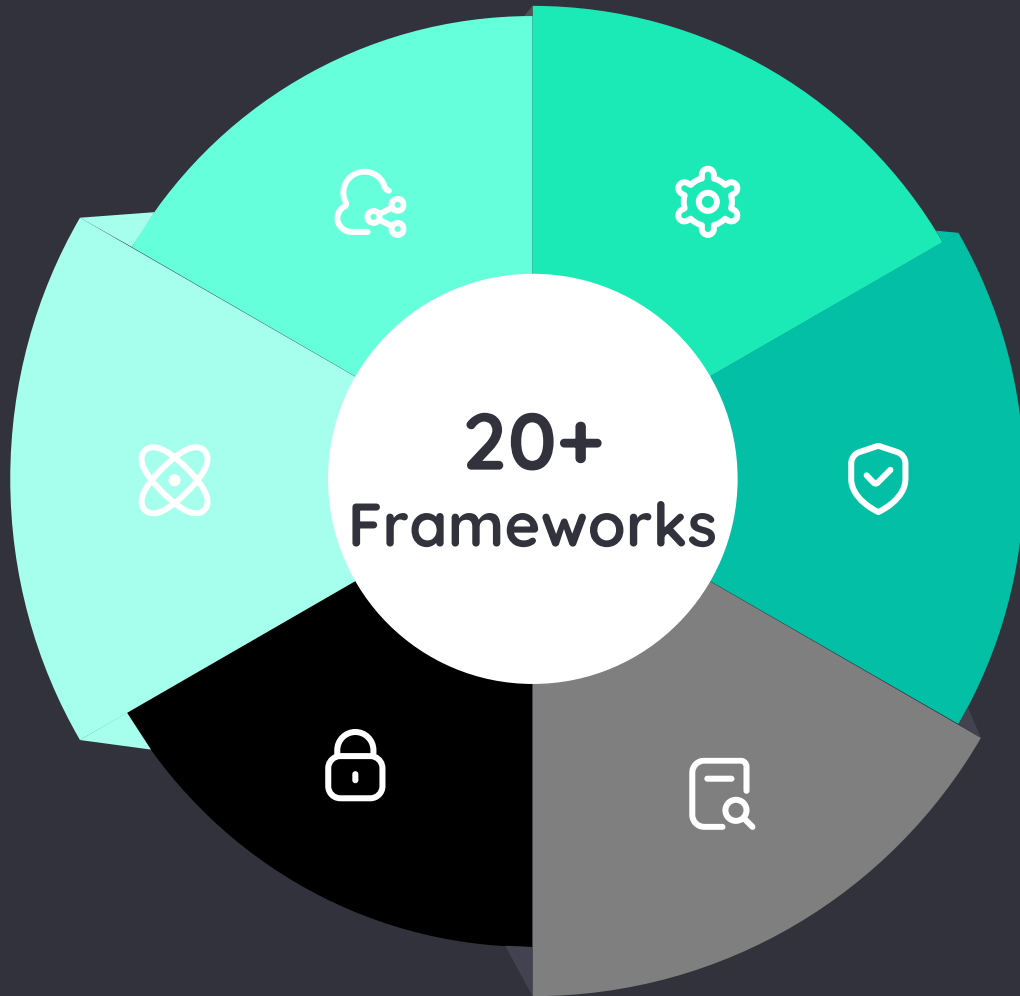
### Better Decision Making

**Gain real-time risk visibility & manage compliance gaps.** Controllo offers dashboards that visualize risk across organizational, vendor, and asset layers. It helps CISOs, IT leaders, and compliance heads see where they stand in real time, prioritize what needs attention, and make data-driven decisions. Gaps are flagged early. Risks are scored. Controls are tracked—all enabling smarter, faster compliance decisions.

## 08 Benefits of Using Controllo

**Start with EU AI Act. Scale with Confidence.**

Controllo supports a growing library of frameworks. Some of those are:



- ISO/IEC 27001
- ISO/IEC 22301
- ISO/IEC 27701
- GDPR
- HIPAA
- SOC 2
- DORA
- ISO 42001
- PCI DSS
- CPRA
- CPA
- CSA CCM v4

To know more about other frameworks contact us on

[info@accedere.io](mailto:info@accedere.io)

or

[Book Demo](#)