Whitepaper

Controllo

ISO 27001 Compliance with Controllo

Simplifying Compliance Automation

with AI-Powered Insights

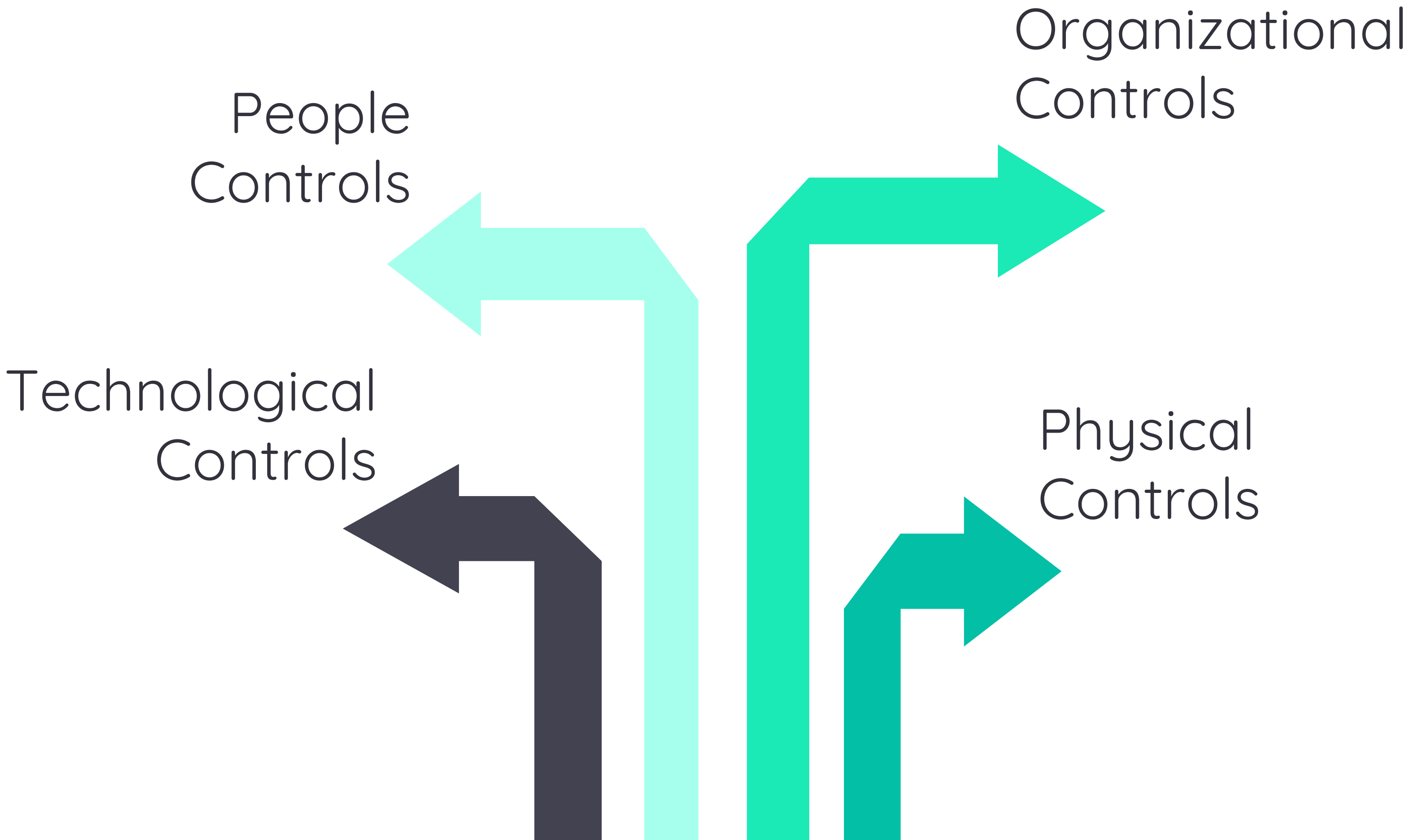
Table of Contents

01 What is ISO 27001 and Why it Matters

ISO/IEC 27001:2022 is the globally recognized standard for **information security management systems** (ISMS). Published by ISO and IEC, it provides a systematic approach to managing sensitive company and customer data, ensuring its confidentiality, integrity, and availability through a risk-based approach.

It helps organizations identify and mitigate information security risks across **people, processes, and technology**. The standard is designed to be flexible and scalable, making it suitable for businesses of all sizes and industries—from startups to global enterprises.

ISO/IEC 27001:2022 includes 10 management clauses and 93 Annex A controls across **4 themes**:



People Controls

Organizational Controls

Technological Controls

Physical Controls

01 What is ISO 27001 and Why it Matters

ISO/IEC 27001:2022 Structure	
ISO/IEC 27001:2022 Management System Clauses	**Annex A Control Themes**
These are part of the main body of the standard—focused on building and operating your ISMS.	There are 93 controls grouped under the following 4 control themes.
Clause 4 – Context of the Organization	A.5 Organizational Controls – 37 Controls
Clause 5 – Leadership	
Clause 6 – Planning	A.6 People Controls – 8 Controls
Clause 7 – Support	
Clause 8 – Operation	A.7 Physical Controls – 14 Controls
Clause 9 – Performance Evaluation	
Clause 10 – Improvement	A.8 Technological Controls – 34 Controls
Note: Clauses 0–3 are introductory (Scope, Normative References, Terms & Definitions). **Clauses 4–10 are certifiable**.	

01 What is ISO 27001 and Why it Matters

With the rise in cyber threats and stricter global compliance mandates, ISO/IEC 27001 has become a vital standard for demonstrating information security maturity. It showcases an organization’s commitment to safeguarding sensitive data and builds trust with customers, regulators, and partners:

30%

fewer data breaches experienced by Orgs with a certified ISMS

60%

of orgs work with 1,000+ vendors—ISMS improves third-party risk controls

48,000+

orgs globally are ISO 27001 certified

(ScienceLogic 2023)

78%

YoY increase in U.S. based ISO 27001 certifications shows rising demand

02 Structure of ISO 27001

Below is the detailed breakdown and structure of the ISO/IEC 27001:2022 standard:

Context of the Organization

Understand internal and external issues that affect information security.

Identify stakeholders and their requirements.

Define the ISMS scope based on business needs and risk.

Leadership

Top management must show commitment to ISMS.

Establish and communicate the information security policy.

Assign roles, responsibilities, and authorities clearly.

Planning

Identify information security risks and opportunities.

Define risk treatment plans aligned with the organization’s goals.

Set measurable information security objectives.

Support

Ensure availability of resources and competent personnel.

Promote training on ISMS policies and responsibilities.

Manage documented information (policies, procedures, records).

02 Structure of ISO 27001

Below is the detailed breakdown and structure of the ISO/IEC 27001:2022 standard:

Operation

Implement risk treatment plans and control processes.

Manage operational planning for achieving security objectives.

Address and manage changes and unforeseen events.

Performance Evaluation

Monitor and evaluate ISMS effectiveness regularly.

Conduct internal audits to identify non-conformities.

Management reviews for performance and improvement areas of ISMS.

Improvement

Take corrective action on non-conformities and incidents.

Continually improve the ISMS to enhance information security.

Promote a culture of risk management and learning.

03 Who Needs an ISO 27001 Certification?

Any organization that handles sensitive information and wants to demonstrate robust security practices should consider ISO/IEC 27001:2022 Certification. It is especially valuable for:

Examples of organizations that may need an ISMS Certification

- SaaS & Cloud Service Providers
- Fintech & Payment Platforms
- Healthcare & MedTech Companies
- AI & Data Analytics Firms
- Legal & Document Management Services
- Cybersecurity & MSSP Vendors
- eCommerce & Retail Platforms
- Government & Defense Contractors
- Telecom & Internet Service Providers
- HR Tech & Payroll Providers

04 Key Terms in ISO 27001

Understanding ISO/IEC 27001 starts with knowing the essential terms used throughout the standard:

ISMS

Information Security Management System – the full set of policies, processes, and systems to manage information risk

Statement of Applicability (SoA)

Document listing applicable Annex A controls and their implementation status

Risk Treatment Plan

A documented strategy for addressing information security risks

These roles are important because internal and external auditors rely on clearly defined responsibilities to evaluate whether the ISMS is effectively implemented and maintained.

04 Key Terms in ISO 27001

Understanding ISO/IEC 27001 starts with knowing the essential terms used throughout the standard:

Asset Owner

The individual responsible for ensuring the security of a specific information asset

Internal Audit

A required review to evaluate ISMS performance and compliance

Non-conformity

A deviation from the standard's requirements identified during an audit

These roles are important because internal and external auditors rely on clearly defined responsibilities to evaluate whether the ISMS is effectively implemented and maintained.

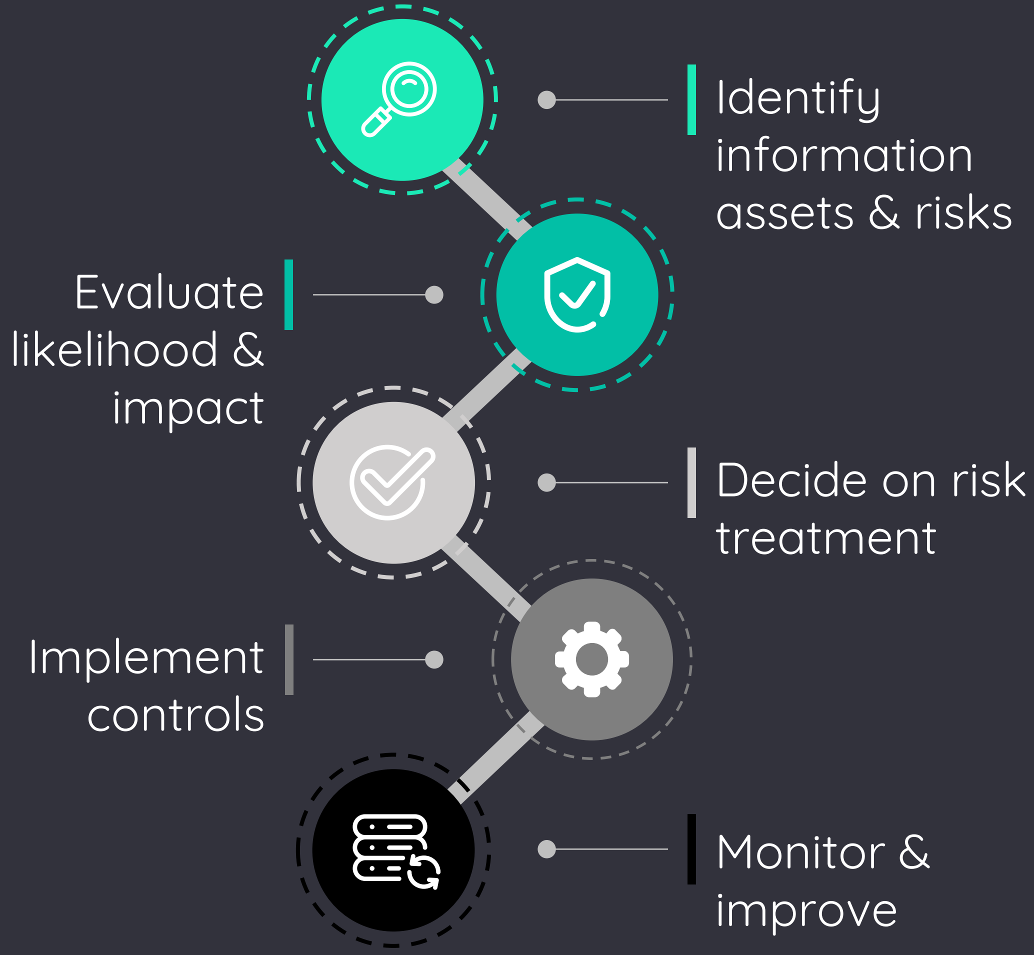
05 Controllo for ISO 27001 & Risk Management

Controllo is an AI-powered compliance automation platform designed to automate and simplify ISO/IEC 27001 compliance.

Controllo is built by auditors and tech professionals who understand that today’s modern teams rapid AI automation and transparency — not another **spreadsheet**.

05 Controllo for ISO 27001 & Risk Management

Risk Management Lifecycle in ISO 27001



Identify information assets & risks

Evaluate likelihood & impact

Decide on risk treatment

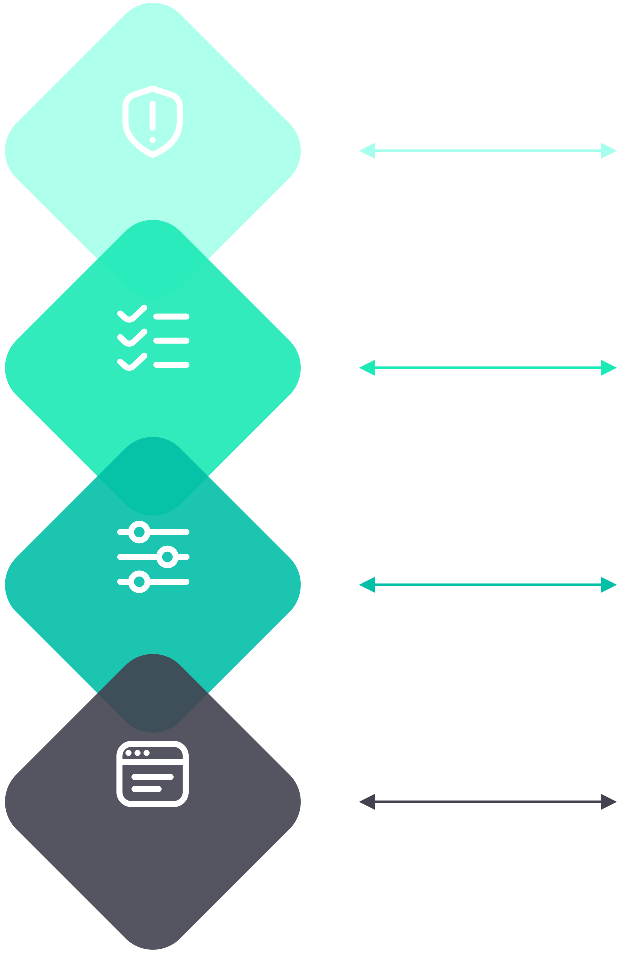
Implement controls

Monitor & improve

- ISO 27001 places risk management at the heart of information security.
- Organizations must identify, assess, and treat information-security related risks.
- The standard does not mandate a specific method, but encourages structured approaches like ISO 31000.
- Controls are based on risk levels, ensuring resources are used where most needed.
- Enables proactive, evidence-based ISMS and supports certification & continuous compliance.

05 Controllo for ISO 27001 & 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.



Categorized Risks
Supports Asset, Organizational, and Vendor Risk Management

Score Risks
Provides risk scoring based on Likelihood × Impact

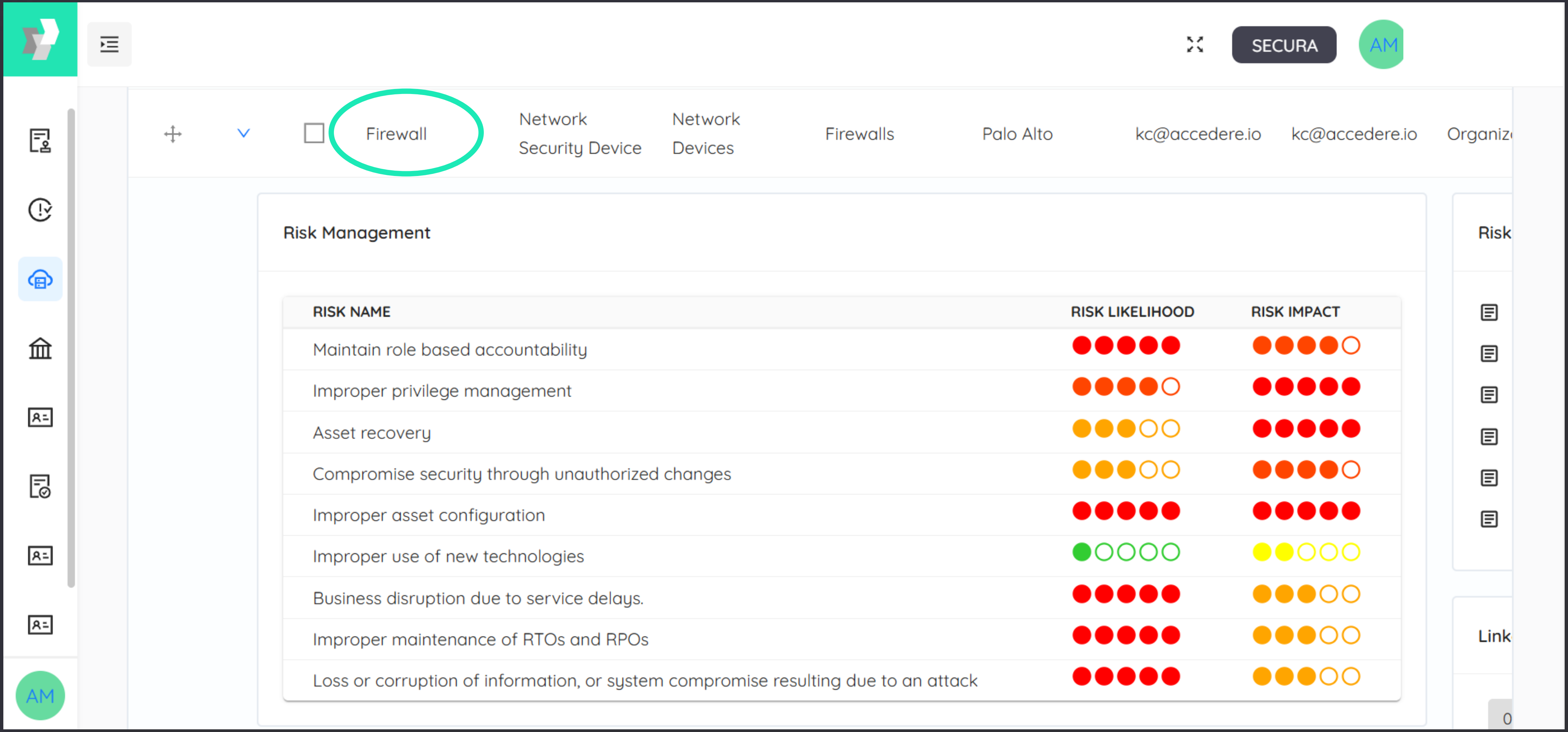
Link to Controls
Ensures traceability of risks to specific controls across frameworks

Visualize Everything
Live risk dashboard and heatmaps

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

Asset Risk Management

Instant Asset Risk Scoring – Easily set Risk Likelihood and Impact for each asset using a simple toggle-based interface.



□	Firewall	Network Security Device	Network Devices	Firewalls	Palo Alto	kc@accedere.io	kc@accedere.io	Organiz

Risk Management

RISK NAME	RISK LIKELIHOOD	RISK IMPACT
Maintain role based accountability	●●●●●	●●●●○
Improper privilege management	●●●●○	●●●●●
Asset recovery	●●●○○	●●●●●
Compromise security through unauthorized changes	●●●○○	●●●●○
Improper asset configuration	●●●●●	●●●●●
Improper use of new technologies	●○○○○	●●○○○
Business disruption due to service delays.	●●●●●	●●●○○
Improper maintenance of RTOs and RPOs	●●●●●	●●●○○
Loss or corruption of information, or system compromise resulting due to an attack	●●●●●	●●●○○

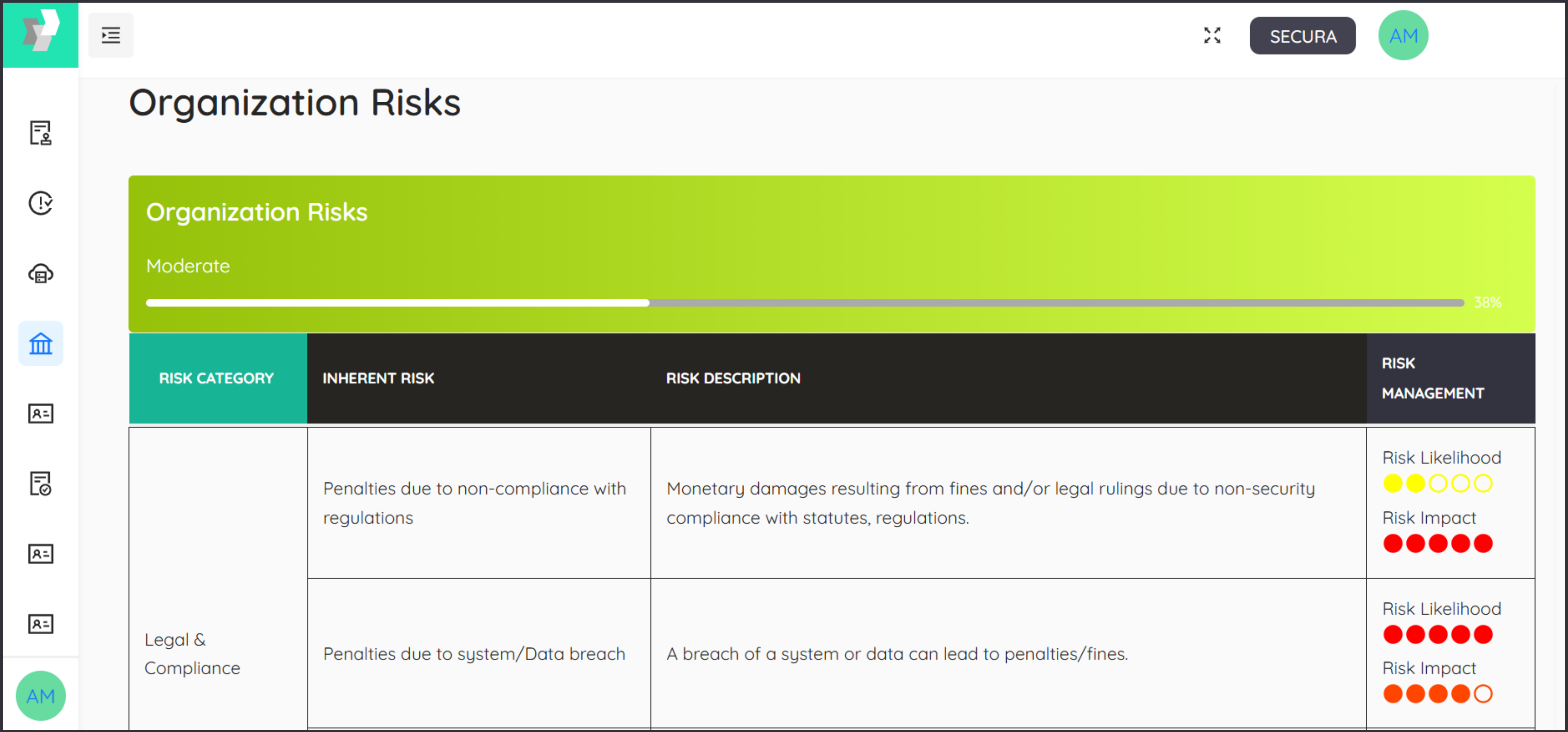
Risk

Link

0

Organisational Risk Management

Effortless Risk Management – Manage organizational risks easily with a preloaded, structured risk library.



Organization Risks

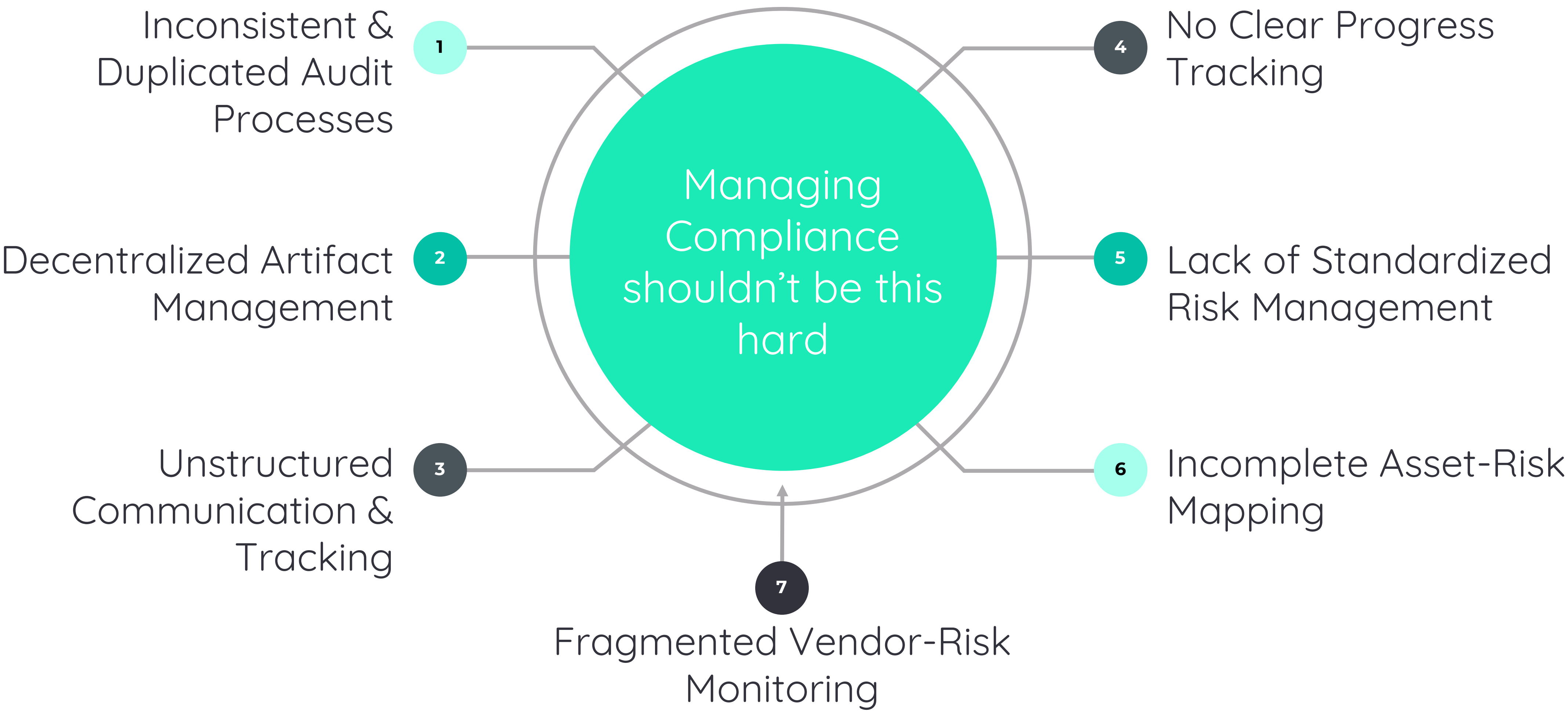
Organization Risks

Moderate

38%

RISK CATEGORY	INHERENT RISK	RISK DESCRIPTION	RISK MANAGEMENT
Legal & Compliance	Penalties due to non-compliance with regulations	Monetary damages resulting from fines and/or legal rulings due to non-security compliance with statutes, regulations.	Risk Likelihood ●●○○○ Risk Impact ●●●●●
	Penalties due to system/Data breach	A breach of a system or data can lead to penalties/fines.	Risk Likelihood ●●●●● Risk Impact ●●●●○

06 Common Compliance Challenges



Managing Compliance shouldn’t be this hard

1 Inconsistent & Duplicated Audit Processes

2 Decentralized Artifact Management

3 Unstructured Communication & Tracking

4 No Clear Progress Tracking

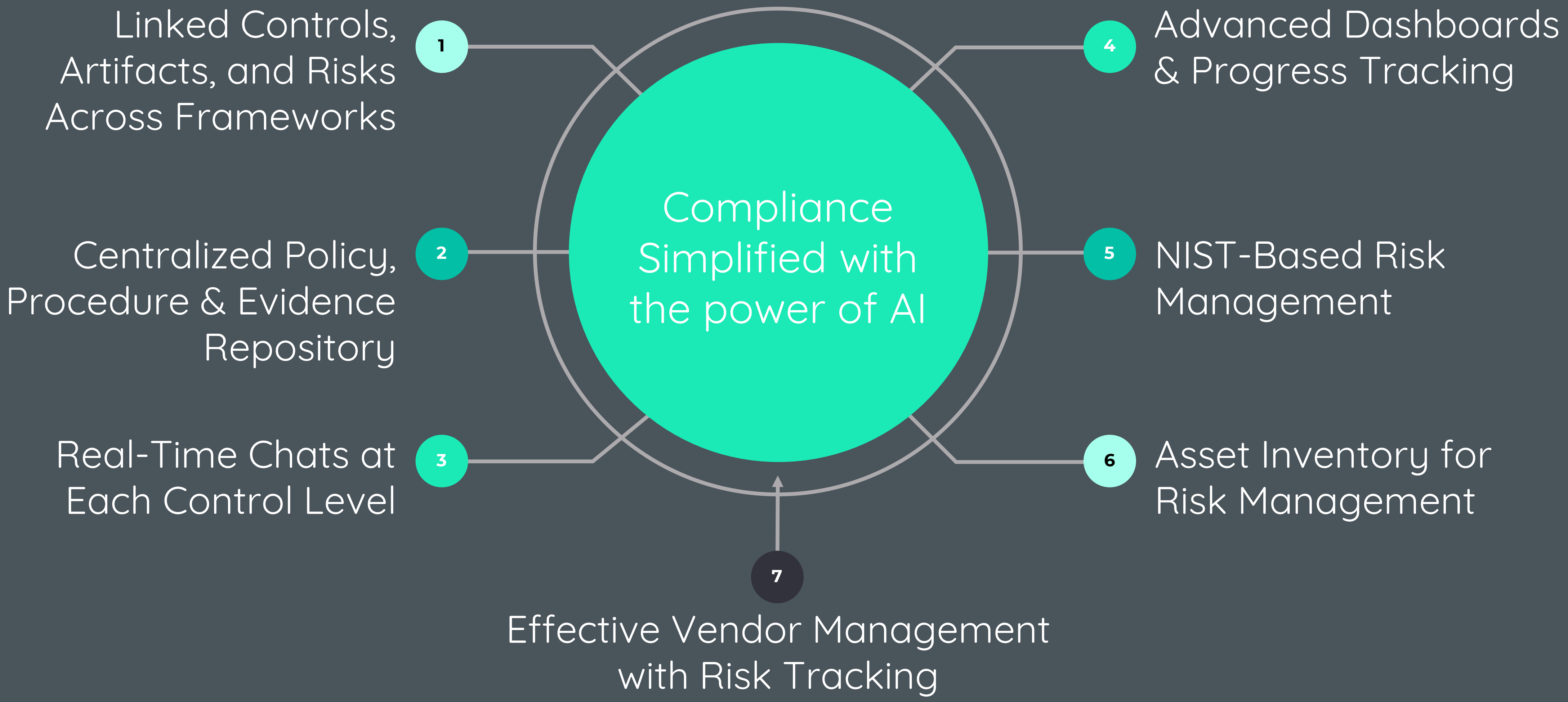
5 Lack of Standardized Risk Management

6 Incomplete Asset-Risk Mapping

7 Fragmented Vendor-Risk Monitoring

06 Common Compliance Challenges

How Controllo Solves Compliance Challenges



Compliance Simplified with the power of AI

1 Linked Controls, Artifacts, and Risks Across Frameworks

2 Centralized Policy, Procedure & Evidence Repository

3 Real-Time Chats at Each Control Level

4 Advanced Dashboards & Progress Tracking

5 NIST-Based Risk Management

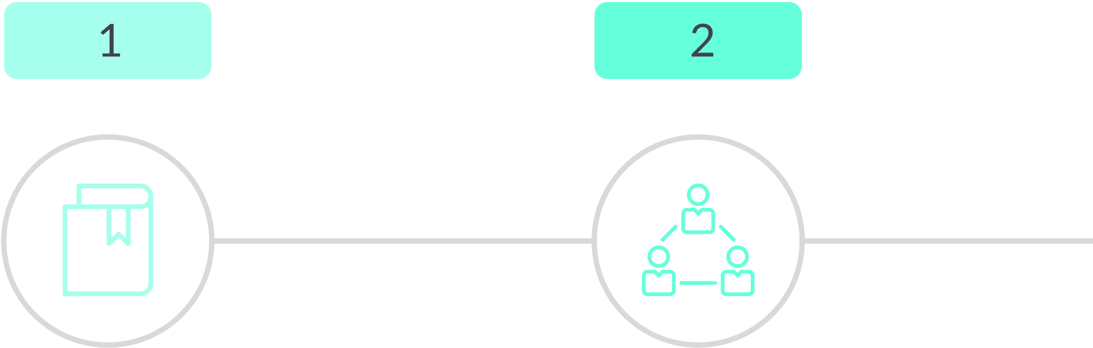
6 Asset Inventory for Risk Management

7 Effective Vendor Management with Risk Tracking

07 ISO 27001 Compliance Journey in Controllo

Accelerate Your ISO 27001 Journey with Controllo

A smarter way to manage controls, evidence, and risk across teams—aligned with ISO 27001 and beyond.



1

ISO 27001 Framework Preloaded

Choose the ISO 27001 framework and access preloaded clauses and Annex A controls built in. The platform guides you through every control, expectation, and evidence requirement.

2

Role Assignment

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

07 ISO 27001 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, NIST, and CCM. Implement once, reuse everywhere.

4

AI-Powered Control Mapping

Controls from ISO 27001 automatically map to SOC 2, CCM, DORA, NIST, ISO 42001 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 ISO 27001 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 the clauses and annex with control-level drilldowns. Have visibility into your risk posture through a separate risk dashboard.

Stay Aligned,

Stay Ready

08 Benefits of Using Controllo

AI-Powered Insights for better Compliance Management

Time Savings

Reduce compliance effort by 70-80% with automation.

Faster Compliance Readiness

Be audit-ready always with automated tracking & real-time visibility.

Organizational Transparency

No more scattered audit documents—everything is structured in one platform.

Cost Efficiency

Cut down on multiple audits and consultant costs, making compliance more affordable.

Scalability

Adapts to growing compliance demands, whether you're handling ISO 27001, NIST, or multiple frameworks at once.

Better Decision-Making

Gain real-time risk visibility & manage compliance gaps.

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.

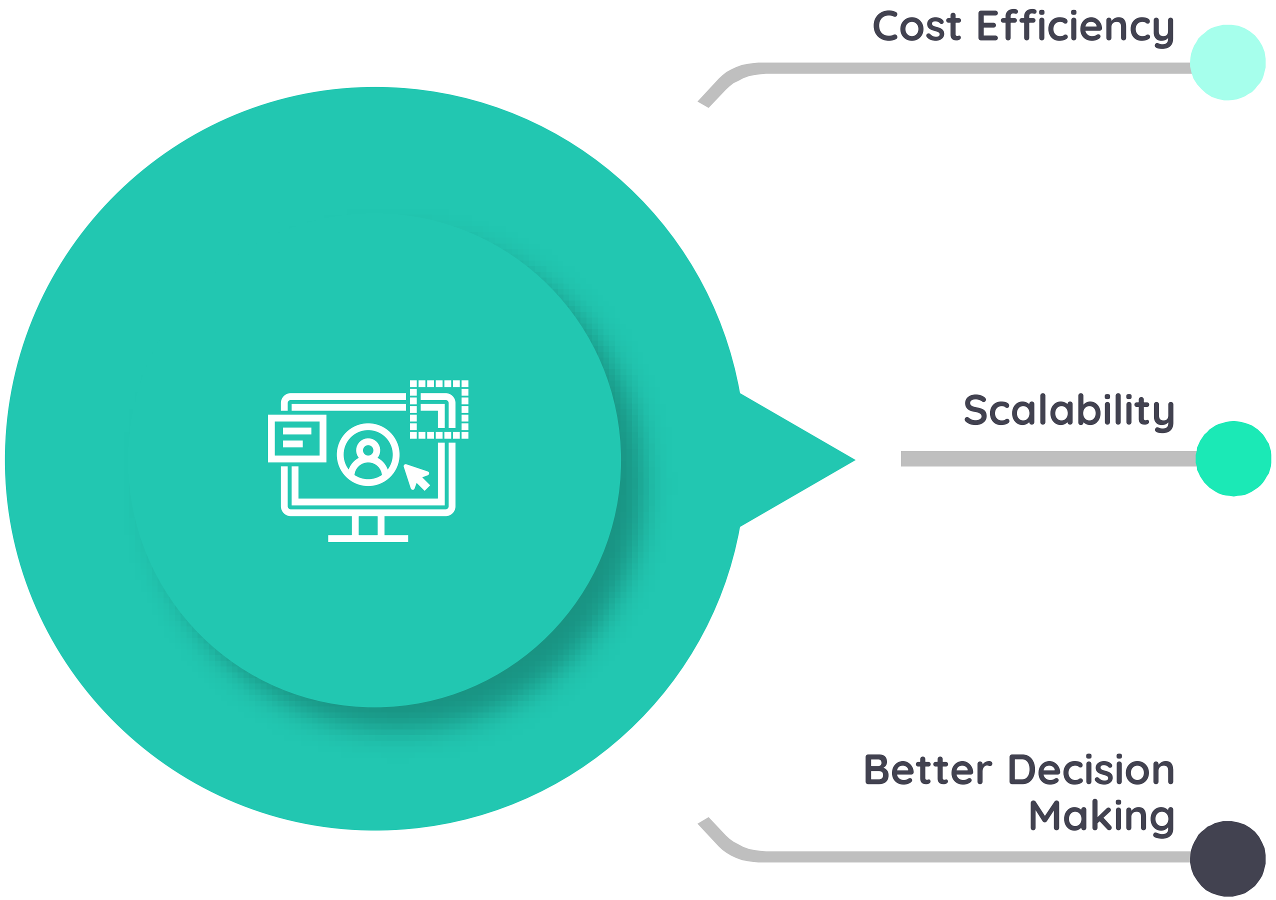
Faster Compliance Readiness

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 ISO 27001 and easily expand to SOC 2, 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.

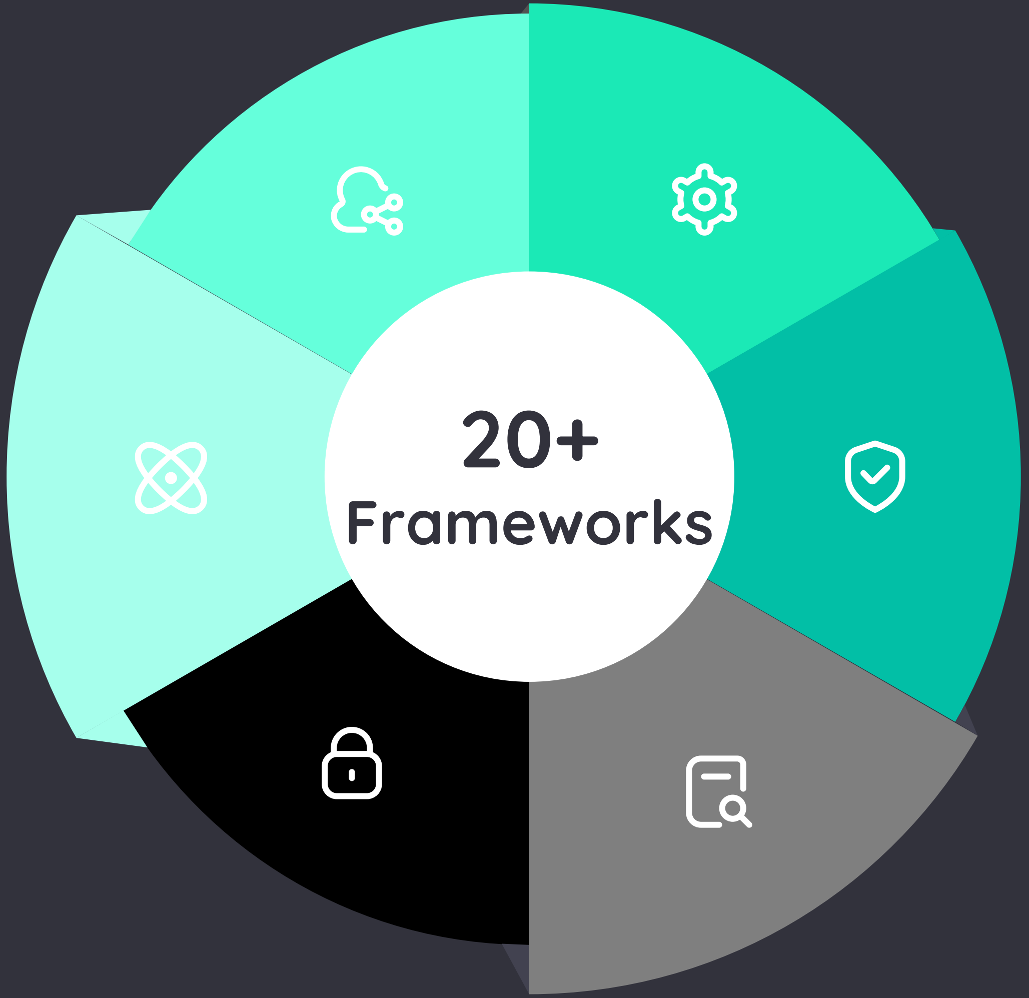
Better Decision Making

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 ISO 27001. Scale with Confidence.

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



- SOC 2
- NIST CSF & 800-53
- NIST 171 r2
- CSA CCM v4
- PCI DSS
- DORA
- NIS 2
- EU AI Act
- ISO/IEC 42001
- CPRA
- CIS Framework
- ISO/IEC 27701

To know more about Controllo, contact us on:

info@accedere.io or Book Demo