Whitepaper

Controllo

SOC 2 Compliance with Controllo

Simplifying Compliance Automation with AI-Powered Insights

Table of Contents

No	Agenda for today	Page
01.	What is SOC 2 and Why it Matters	3 - 5
02.	Understanding SOC 2 Type I vs. Type II	6
03.	Who Needs a SOC 2 Report?	7
04.	Key Terms in a SOC 2 Report?	8
05.	Controllo for SOC 2 & Risk Management	9-13
06.	Common Compliance Challenges	14 - 15
07.	SOC 2 Compliance Journey in Controllo	16 - 18
08.	Benefits of Using Controllo	19 - 22

01 What is SOC 2 and Why it Matters

SOC 2 (System and Organization Controls) is a voluntary compliance standard developed by the American Institute of CPAs (AICPA) designed for service providers that store or process customer data in the cloud. It requires companies to establish and follow strict information security policies and procedures. These controls are designed to ensure the security, availability, privacy, confidentiality, and integrity of customer data.

The framework defines criteria for managing customer data based on five trust service principles also known as TSC (trust service criteria).

Trust Service Criteria's

01 What is SOC 2 and Why it Matters

Security

Protects systems and data from unauthorized access and breaches.

Includes firewalls, encryption, access controls, and patching.

Core requirement for all SOC 2 reports.

Availability

Ensures systems are reliably accessible when needed.

Covers uptime, backups, disaster recovery, and scalability.

Minimizes downtime and service disruption.

Confidentiality

Protects sensitive information from unauthorized disclosure.

Involves access control, secure storage, and data retention.

Mitigates legal and reputational risks.

Processing Integrity

Ensures data is processed accurately and without errors.

Includes validation, automation, and error handling.

Builds trust in system outputs.

Privacy

Manages personal data in line with privacy laws.

Covers consent, transparency, and breach response.

Aligns with GDPR, CCPA, HIPAA, etc.

01 What is SOC 2 and Why it Matters

Rise in data breaches and tightening data protection regulations have made SOC 2 a critical benchmark. It exhibits an organization's commitment to maintaining a robust security posture and gives assurance to customers, partners, and stakeholders.

82%

of B2B buyers ask for SOC 2 before signing a contract

70%

SaaS buyers cite security certifications as a key factor in vendor selection

$4.88M

The average cost of a data breach

(IBM 2024)

SOC 2

de facto standard for showing internal security and process maturity

02 Understanding SOC 2 Type I vs. Type II

When pursuing SOC 2 compliance, it's essential to understand the difference between Type I and Type II reports—because each serves a different purpose, requires a different level of effort, and delivers different outcomes. Here's the breakdown:

Feature	SOC 2 Type I	SOC 2 Type II
Time Frame	Point-in-time report	Covers a specific period (typically 6–12 months)
Control Focus	Evaluates the **design** of controls	Evaluates both **design and operating effectiveness** of controls
Audit Depth	Limited testing; controls reviewed as of a specific date	Detailed testing of control performance over time
Use Case	Informational; often used in the **first year** of compliance	Preferred by customers for ongoing assurance
Value to User Auditor	Generally, not sufficient to reduce control risk assessment	Can be used to reduce control risk during customer audits
Assessment Rigor	Lower; does not test if controls are functioning as expected	Higher; includes actual **evidence of control execution**
Internal Effort Required	Lower	Significantly higher; requires consistent documentation and monitoring
Non-Compliance Identification	May not fully identify instances of operational failures	Identifies **actual instances of non-compliance** if controls requirements are not met
Audit Usage	Common when launching SOC 2 for the first time	Required for clients demanding full control assurance
Evidential Emphasis	Minimal; more about existence of controls	High; auditors demand **proof of operating effectiveness** over time

03 Who Needs a SOC 2 Report?

While SOC 2 was originally designed for technology and cloud service providers, today it is widely required across multiple industries. Any organization that processes, stores, or transmits customer data—especially data on behalf of another business—should consider SOC 2 compliance.

04 Key Terms in a SOC 2 Report

SOC reports involve multiple entities, each with a specific role. Understanding the terminology can help demystify the process:

User Organization

The client or customer that uses services provided by the service organization.

Service Organization

The company undergoing the SOC 2 audit and providing services to users.

User Auditor

The external auditor of the user organization.

Service Auditor

The independent CPA or audit firm performing the SOC 2 audit.

These roles are important because the user auditor relies on the SOC 2 report provided by the service auditor to evaluate whether the service organization has adequate controls in place.

05 Controllo for SOC 2 & Risk Management

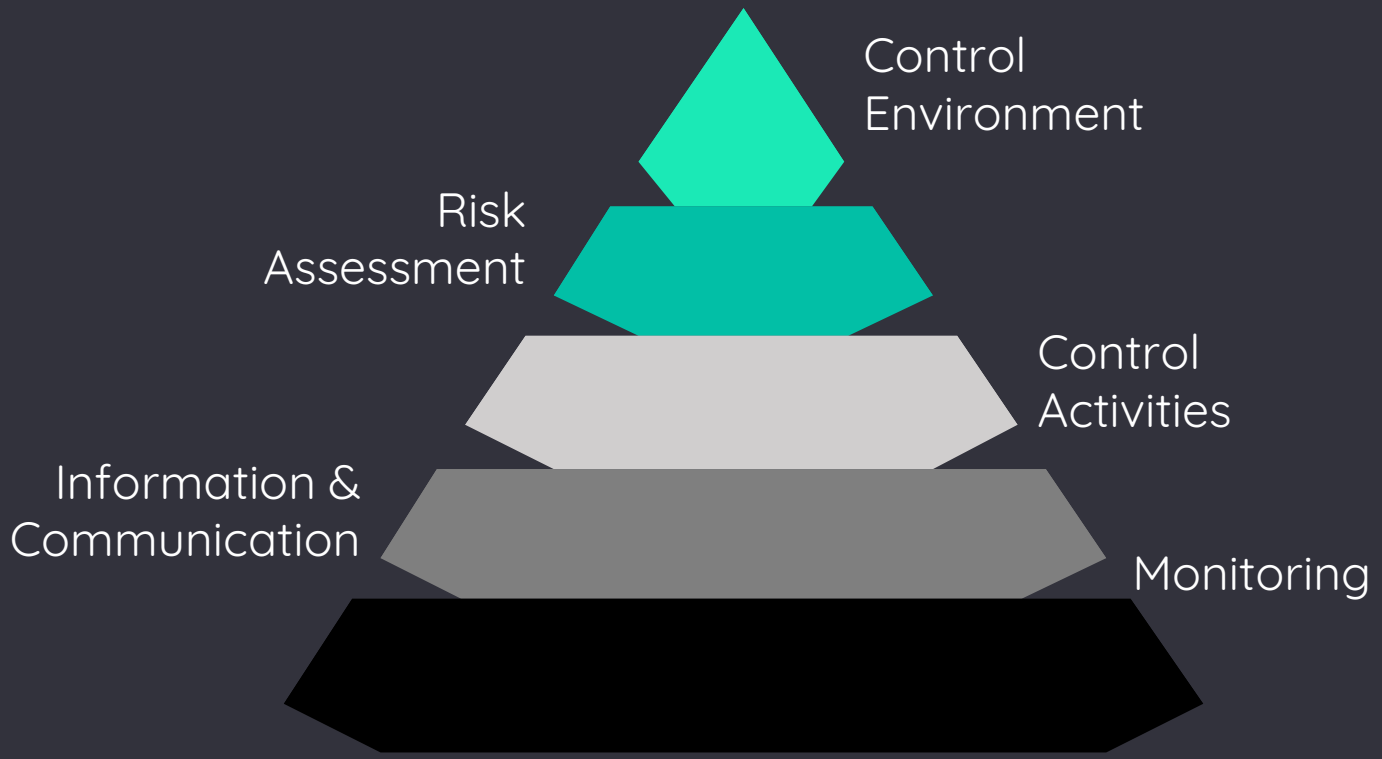
Controllo is an AI-powered compliance automation platform designed to automate and simplify SOC 2 compliance.

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 SOC 2 & Risk Management

SOC 2 and COSO – The Risk Management

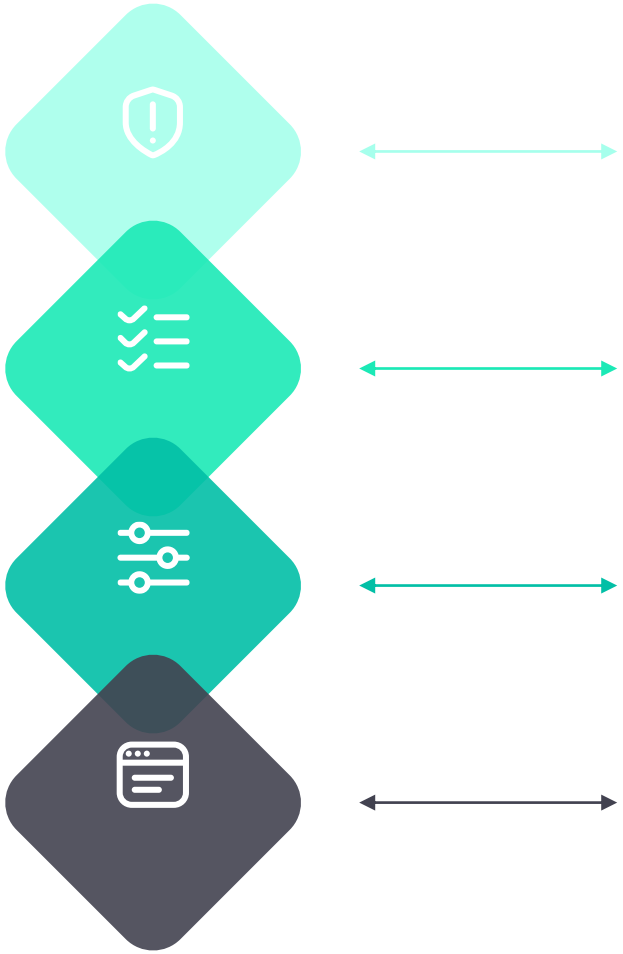
SOC 2 maps controls directly to COSO's five internal control components:



- SOC 2 is a control framework derived from the COSO (Committee of Sponsoring Organizations of the Treadway Commission) model for internal control.
- COSO provides the conceptual foundation for managing enterprise risks.
- To be SOC 2 compliant, an organization must demonstrate not just technical security controls, but also enterprise-wide risk awareness and mitigation mechanisms.
- Proper risk management is the backbone of SOC 2 compliance.

05 Controllo for SOC 2 & 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

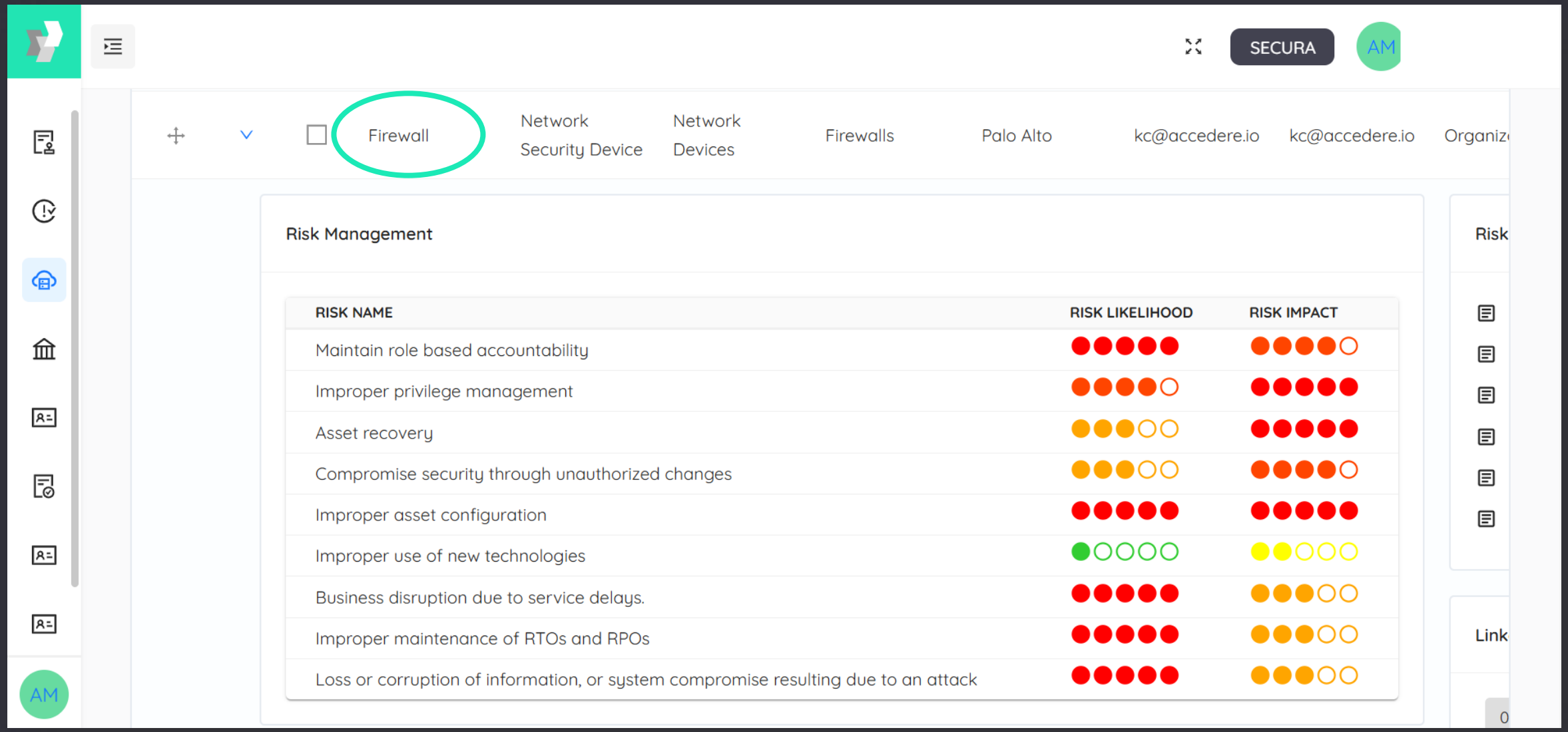
Link to Controls
Ensures traceability of risks to specific controls across frameworks

Visualize Everything
Live risk dashboard and heatmaps

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

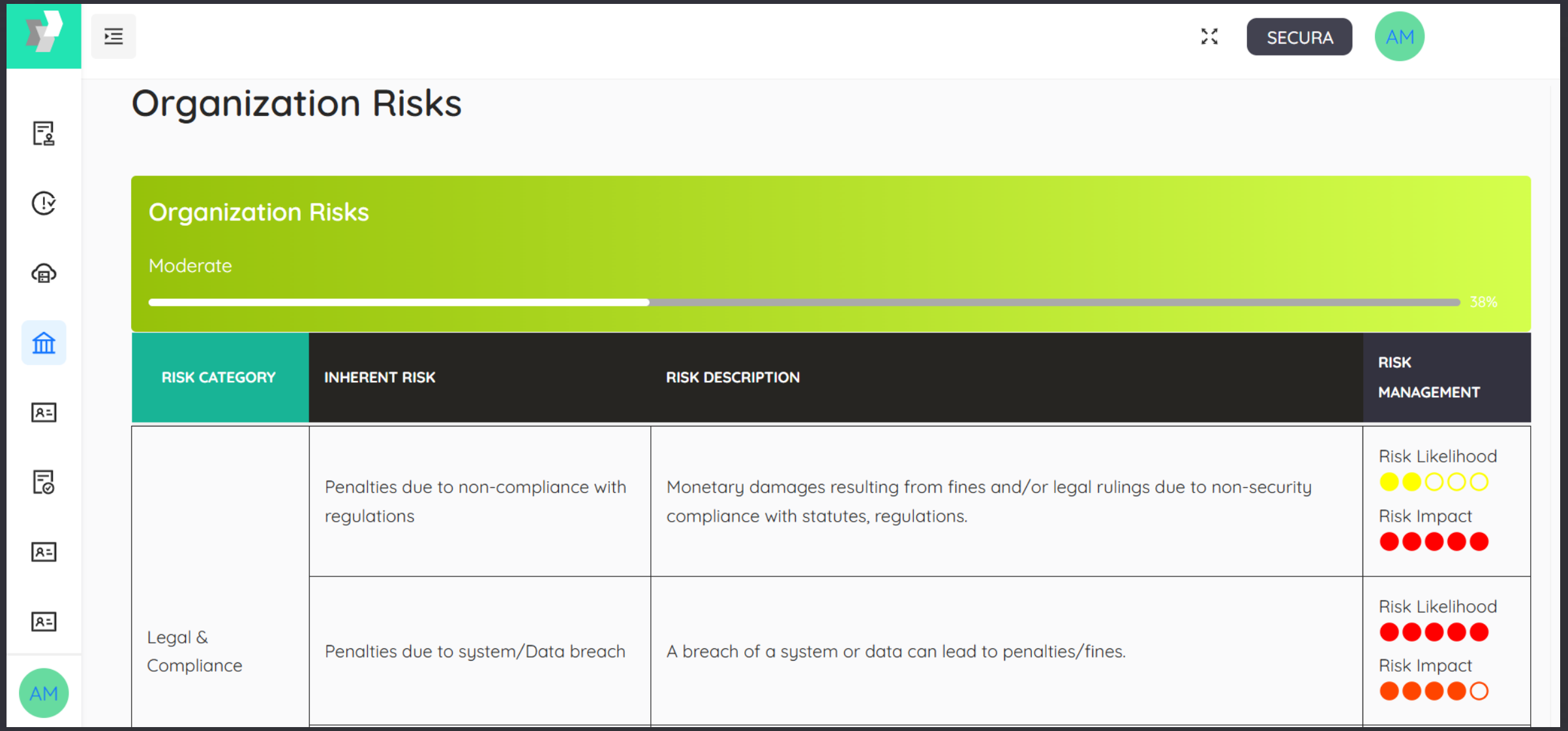
Asset Risk Management

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

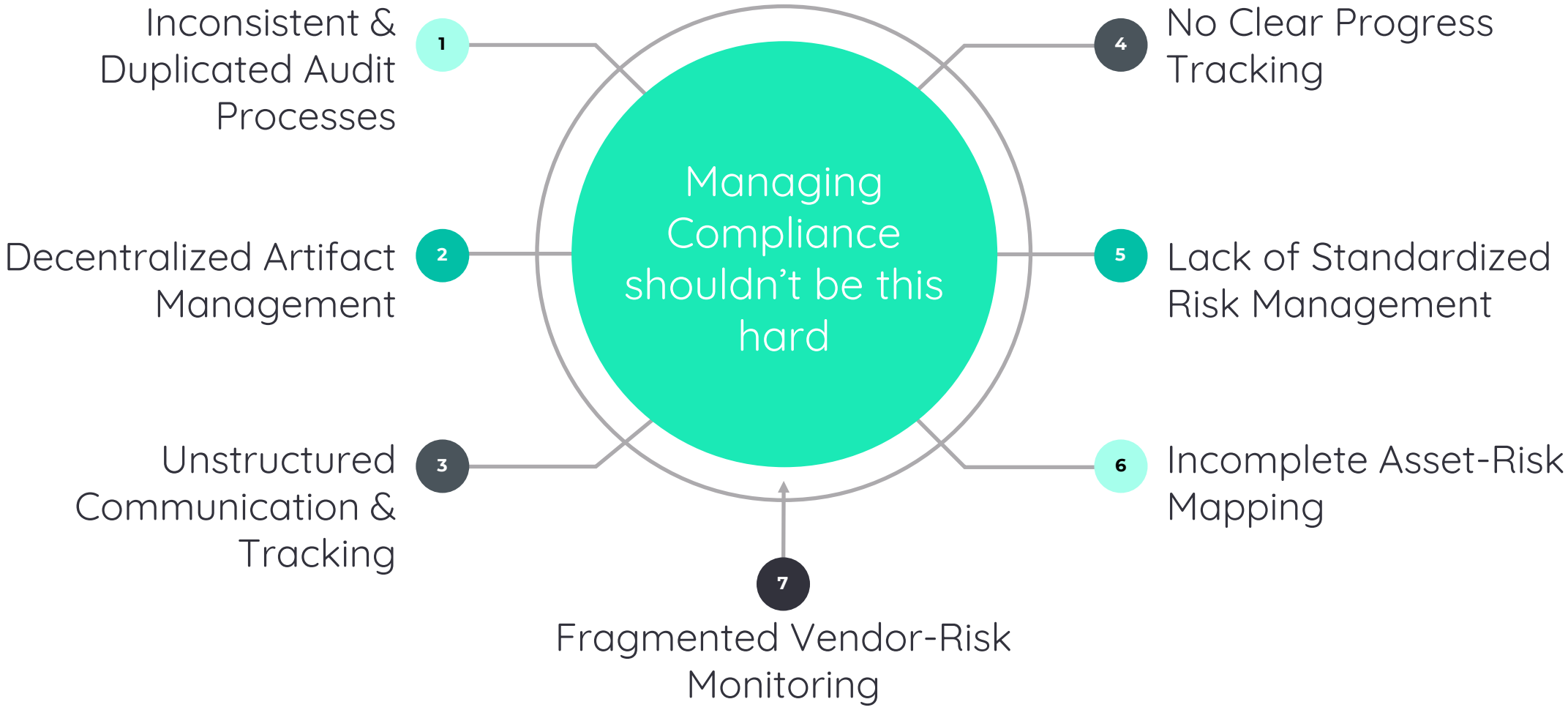


Organisational Risk Management

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

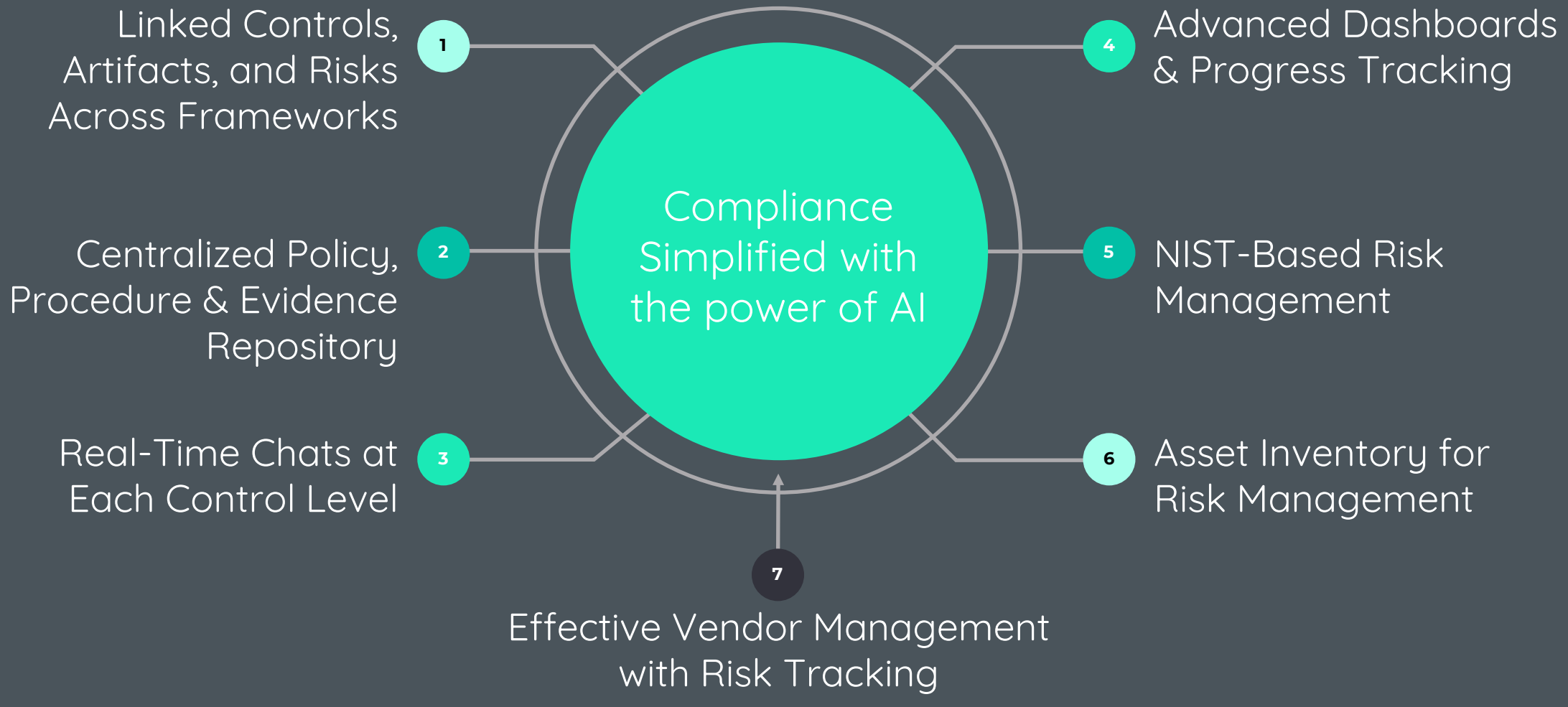


06 Common Compliance Challenges



06 Common Compliance Challenges

How Controllo Solves Compliance Challenges



07 SOC 2 Compliance Journey in Controllo

Accelerate Your SOC 2 Journey with Controllo

A smarter way to manage controls, evidence, and risk across teams—aligned with SOC 2 and beyond.

1

SOC 2 Framework Preloaded

Choose the SOC 2 framework and Controllo comes with all five Trust Services Criteria built in. The platform guides you through every control, expectation, and evidence requirement.

2

Role Assignment

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

07 SOC 2 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 ISO 27001, NIST, and CCM. Implement once, reuse everywhere.

4

AI-Powered Control Mapping

Controls from SOC 2 automatically map to ISO 27001, 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 SOC 2 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 Trust Services Criteria with control-level drilldowns. Have visibility into your risk posture through a separate risk dashboard.

Stay Aligned,

Stay Ready

08 Benefits of Using Controllo

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.

Better Decision-Making
Gain real-time risk visibility & manage compliance gaps.

Scalability
Adapts to growing compliance demands, whether you're handling SOC 2, NIST, or multiple frameworks at once.

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.

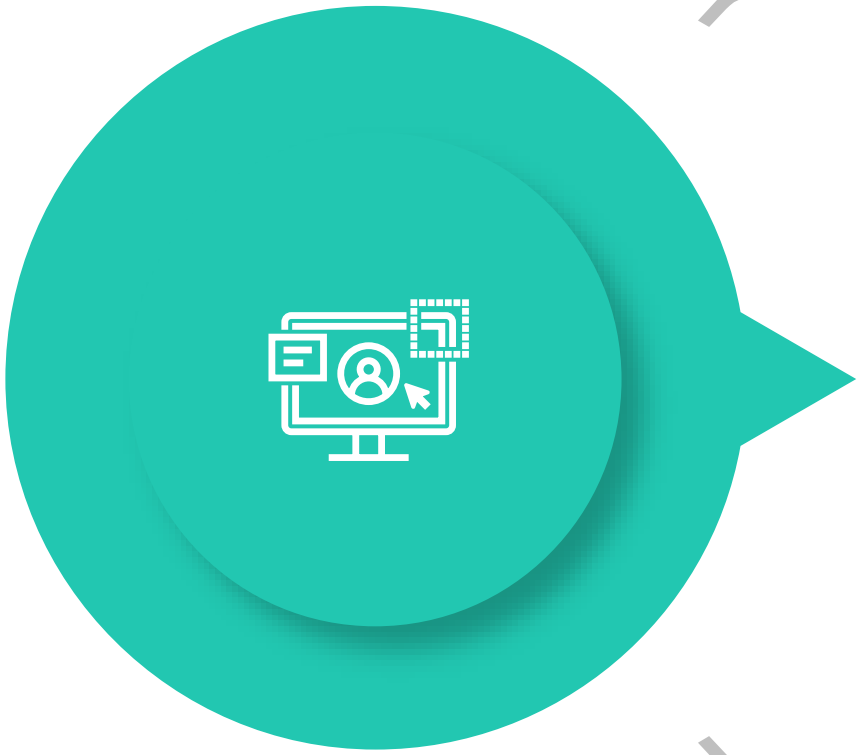
Faster Compliance Readiness

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 SOC 2 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 SOC 2. Scale with Confidence.

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

- ISO/IEC 27001
- 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