Copla

ISO 27001
Compliance Explainer

→ What you need to know


ISO
27001
DORA
NIS2
DIRECTIVE
aws

What is ISO 27001

ISO/IEC 27001 is the foundational international standard for information security management systems (ISMS). It defines how to systematically identify, assess, and mitigate risks to both digital and physical information — covering confidentiality, integrity, and availability.

The goal isn't just to pass an audit — it's to embed security into the organization's culture and operations. ISO 27001 is applicable to any organization, regardless of size or sector, and is often a prerequisite for working with enterprise or regulated customers.

Many new frameworks — including DORA, GDPR, and NIS2 — build upon the core principles and controls introduced in ISO 27001.

This makes ISO a strategic foundation: if you already meet ISO 27001 requirements, you're often more than halfway toward complying with other regulations thanks to extensive cross-mapping between these frameworks.

Who needs to comply

While ISO 27001 is not legally required, many organizations pursue it for strategic reasons, including:

- SaaS & Fintech Companies handling sensitive customer data
- Startups seeking enterprise procurement eligibility
- Health Tech & Life Sciences managing protected information
- Any company preparing for future regulation (like NIS2 or DORA)
- Critical Infrastructure & Public Sector Vendors

In short, if your customers ask about security — ISO 27001 is your answer

Why it matters

A robust ISMS is more than a security tool — it's a market differentiator. Achieving ISO 27001 helps organizations:

- Build trust with customers, partners and regulators
- Demonstrate accountability for protecting data and assets
- Reduce the likelihood and impact of breaches
- Create internal structure for scalable, auditable security
- Align with modern procurement and compliance expectations

ISO 27001 compliance often opens the door to bigger deals, better vendor evaluations, and faster security reviews.

Manual compliance burden

Without structured guidance or automation, achieving ISO 27001 certification is complex and resource-intensive — especially for first-time implementations. The framework mandates deep documentation, formal processes, and verifiable evidence across every control.

Typical effort required includes*:

200+ hours

for business impact and gap analysis

200+ hours

writing, reviewing, and version-controlling mandatory policies (e.g. access, backup, incident response)

150+ hours

for initial risk assessment, risk treatment planning, and SoA (Statement of Applicability)

100+ hours

setting up monitoring and logging processes for audits

80+ hours

implementing & testing business continuity and disaster recovery procedures

50+ hours

writing, reviewing, mapping supply chain risks, creating contract templates with security clauses (highly dependent on number of vendors)

50+ hours

for filling out due diligence questionnaires for your vendors (highly dependent on number of vendors and their compliance status)

+

internal audits, awareness training, corrective actions, certification body coordination

*THE TIMELINE DEPENDS ON YOUR INFRASTRUCTURE, VENDOR LANDSCAPE, CURRENT COMPLIANCE STATUS, AND OVERALL SCOPE. DURING ONBOARDING WITH COPLA, WE'LL ASSESS THESE FACTORS AND PROVIDE A CLEAR ESTIMATE OF THE PROCESS DURATION.

This doesn't include time for maintaining compliance annually — which often becomes a rolling project involving quarterly updates and revalidation tasks.

In other words: ISO 27001 is not just about controls. It's about demonstrating **control governance** — which multiplies the time needed to document, implement, and prove your security posture.

Time and cost of achieving compliance

Implementation varies by size, scope, and internal maturity.
Here's a typical timeline and cost outline:

< 50 people	50-150 people	150+ people
ORGANIZATION SIZE	ORGANIZATION SIZE	ORGANIZATION SIZE
First-time ISO 27001 certification	First-time ISO 27001 certification	First-time ISO 27001 certification
TASK	TASK	TASK
4-6 months	6-9 months	9-12+ months
INTERNAL EFFORT	INTERNAL EFFORT	INTERNAL EFFORT
€30,000+	€60,000+	€100,000+
INTERNAL COST ESTIMATE*	INTERNAL COST ESTIMATE*	INTERNAL COST ESTIMATE*

40–70% faster and cheaper

*COSTS ASSUME BLENDED INTERNAL AND EXTERNAL RESOURCES AT ~€6K–€8K/ MONTH PER FTE, AND INCLUDE CONSULTING, AUDIT PREP, AND TOOL OVERHEADS.

Breakdown of ISO 27001 requirements

ISO 27001 certification isn't just about having policies in place — it's about implementing, maintaining, and continuously improving a full Information Security Management System (ISMS).

Below is a breakdown of the typical effort involved per major requirement cluster, based on implementations across Copla clients. ISO 27001 compliance involves two main components:

01 - ISMS Core (Clauses 4–10)

02 - Annex A Controls (93 control items, mapped to risk)

ISMS Core (Clauses 4–10)

ESTIMATED EFFORT

400+ hours

Requirement Area	Clause	Typical Tasks	Time Estimate
Context & Scope	4	Define scope, stakeholders, internal/external issues	20+ hours
Leadership & Policy	5	Define roles, responsibilities, and the top-level security policy	40+ hours
Planning & Risk	6	Perform risk assessment, risk treatment, and maintain risk register	80+ hours
Support & Awareness	7	Document roles, competencies, awareness training, communication plans	40+ hours
Operations	8	Implement procedures, change management, and documented processes	60+ hours
Performance Evaluation	9	Conduct internal audits, define metrics, and run management reviews	20+ hours
Improvement	10	Create corrective action workflows, track continual improvement	30+ hours

Annex A Controls
93 Controls (ISO/IEC 27001:2022)

ESTIMATED EFFORT

300+ hours

Grouped into four themes, Annex A controls are selected based on your identified risks and form the backbone of your technical, organizational, and physical security practices.

Control Theme	Example Controls	Notes	Time Estimate
A.5 Organizational	Policies, roles, contact with authorities	Includes documentation and governance practices	80+ hours
A.6 People	Screening, awareness, responsibilities	Includes onboarding, training logs, HR alignment	40+ hours
A.7 Physical	Secure areas, equipment protection	Highly dependent on office access setup	30+ hours
A.8 Technological	Access control, encryption, monitoring	Involves cloud config mapping, logs, MFA, SIEM	100+ hours

700+ hours

total time without automation

This excludes recurring tasks such as internal audits, training refreshers, quarterly reviews, and evidence collection — which often require 20–30 hours per quarter to maintain certification.

How Copla helps

ISMS Core (Clauses 4–10)

Copla provides:

- Scope & stakeholder mapping templates
- Risk assessment workflows with pre-filled threat libraries
- Statement of Applicability (SoA)
- Policy templates aligned with ISO best practices
- Internal audit tooling and corrective action trackers

Annex A Controls (A.5-A.8)

Copla accelerates control implementation by:

- Mapping controls to your tools & systems (e.g. Google Workspace, AWS)
- Providing configuration guides and evidence templates
- Automating logs, access reviews, and documentation
- Tracking compliance status in real-time

EXAMPLE

Our ISO Password Policy pack includes default policy text, MFA standards, and audit controls — based on our public blog guidance.

The latest version (ISO/IEC 27001:2022) organizes 93 controls into 4 themes:

A.5 Organizational

Policies, roles, and planning

A.6 People

Background checks, awareness, responsibilities

A.7 Pysical

Secure areas, equipment handling

A.8 Technological

Encryption, access control, monitoring

Achieving ISO 27001 certification manually can easily exceed 800 hours of internal effort — not including the ongoing work required to maintain compliance over time. Copla was designed to turn ISO 27001 from a burdensome project into a streamlined, repeatable process.

Here's how we help teams reduce complexity, save time, and stay audit-ready:

We help you handle all of the above and cut time to compliance by 40–70%.

Success Stories

Evergrowth reached ISO 27001 compliance in record time.

PROBLEM

Evergrowth needed ISO 27001 for enterprise deals in both the EU and US.

SOLUTION

Copla's automation and pre-built controls streamlined the process.

OUTCOME

Achieved ISO 27001 in record time, accelerating customer onboarding and cutting compliance hours by 60%.

evergrowth

As an innovative AI-driven customer intelligence platform operating in both the EU and the U.S., Evergrowth needed to ensure their data security met the highest industry standards. Their customers required proof of compliance with certifications like ISO 27001 in Europe and SOC2 in the U.S. Without these certifications, sales cycles would slow down, and trust-building with enterprise clients would become increasingly difficult.

Crossmapping compliance frameworks cut Popcorn's workload by 90%.

PROBLEM

Popcorn needed to meet ISO 27001 and other frameworks fast, but had no internal compliance team.

SOLUTION

Copla delivered hands-on support and leveraged crossmapping to streamline multi-framework compliance.

OUTCOME

Achieved certification in weeks, cut compliance workload by 90%, and avoided hiring delays.

Popcorn

Like many scale-ups, Popcorn faces the classic startup challenge: how to move fast while remaining compliant without a dedicated internal compliance team. Compliance quickly became a business-critical concern. By combining hands-on support with strategic crossmapping, Copla helped Popcorn move through complex compliance frameworks with speed and confidence. What normally takes months of internal effort was completed in weeks—without hiring, delays, or disruption.

Why automation + expert CISO guidance wins

Manual compliance often leads to versioning chaos, misaligned stakeholders, and “policy shelfware.” With Copla, you get best of both worlds with:

- Pre-built documentation and rapid tailoring
- Evidence automation across your stack
- Built-in updates for ISO 27001:2022 control changes
- Control-by-control implementation tracking
- Team assignments and audit readiness dashboards
- Expert CISO guiding you on your compliance journey

WE STREAMLINE ISO WHILE ALSO LAYING THE FOUNDATION FOR NIS2, DORA, AND GDPR — **ALL FROM ONE PLATFORM**

“Copla has a model that every company should consider when dealing with compliance. They act as an extension of our team, allowing us to focus on what we do best. Trusting them with our compliance processes has helped us optimize resources, delivering both cost savings and efficiency.”

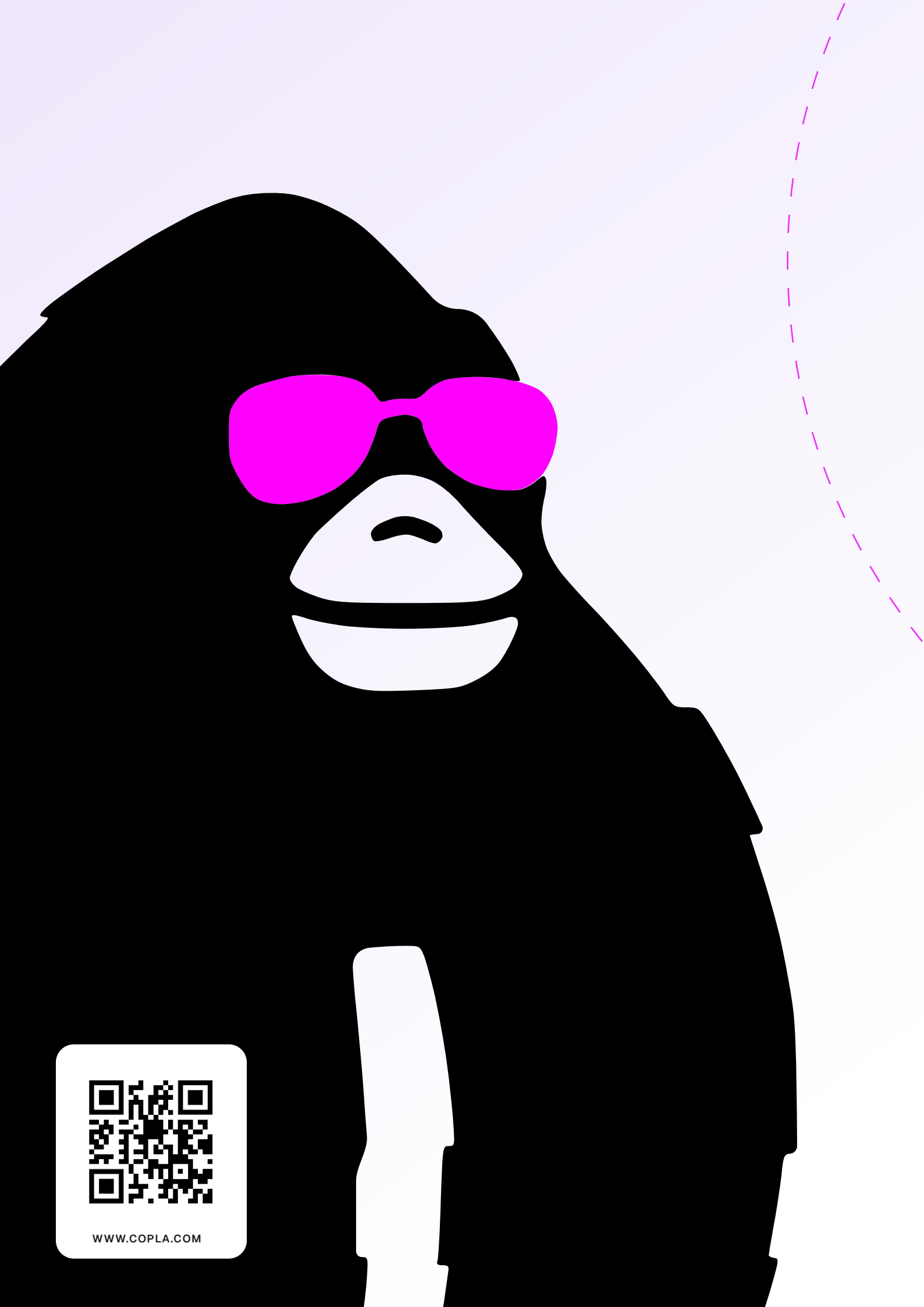
Audrius Dumbliauskas, Product Manager @ HeavyFinance

Assess your ISO 27001 readiness

Not sure where your organization stands with ISO 27001 compliance?

To deepen your understanding and stay up to date with evolving ISO 27001 best practices, explore our in-depth blog series. We regularly publish practical insights, CISO perspectives, and implementation tips based on real-world ISO 27001 journeys:

Scan QR code to read our ISO 27001 blog posts


WWW.COPLA.COM