ISO 27001 ONBOARDING CHEAT SHEET

From sign-up to a passed audit

Keep it to hand, or use it as a checklist if your ISMS is already under way. Each step shows where to find it in the app. Gapless proposes; your people decide.

Ready to go further? Upgrade to a paid plan inside the app whenever you are ready. It is all self-serve, preferably by direct debit through Stripe. See pricing at **getgapless.com/pricing**.

Set up

1 Connect your identity provider

Choose Google Workspace or Microsoft Entra ID (one only), then import your people.

IN APP: **Integrations**

2 Connect devices, cloud and code

Devices (Intune), cloud (AWS) and code (GitHub).

IN APP: **Integrations**

3 Upload your existing documents

Add current policies, diagrams and past audit reports. Some later steps need them.

IN APP: **Uploads**

4 Set your scope

Say what the ISMS covers, usually the company and its product.

IN APP: **Statement of Applicability, document details**

5 Know where to get help

Stuck at any point, or not sure what a step means? Raise a support ticket in the app and we will help.

IN APP: **Support**

Set your risk appetite

6 Name the owner and approver

An owner of risk governance (CRO, COO, CFO, CISO or founder) and an approver from leadership.

IN APP: **Risk appetite**

7 Fill it in together

Complete the wizard, including financials, or at least review it as a team.

IN APP: **Risk appetite**

8 Upload the minutes and sign off

Upload the meeting minutes (Word, PDF or similar), then the approver signs off.

IN APP: **Risk appetite**

Teach Gapless your business

9 Assign your stakeholders

Give each key ISMS area an owner (see the roles below).

IN APP: **Collaborators**

10 Answer the agent's questions

Each stakeholder answers for their own area. Gapless learns your business and records observations.

IN APP: **Chat**

11 Check your coverage

See which areas are covered and which questions are still open.

IN APP: **Dashboard**

12 Hold the workshop

Stakeholders meet, vote on each observation, then discuss and amend the doubtful ones.

IN APP: **Observations**

STAKEHOLDER ROLES (STEP 9)

Leadership: direction, governance, continuity, AI use.

IT Operations: devices, access, backups, incident response.

Engineering and Cloud: cloud, delivery, patching, encryption, logging.

Legal and Compliance: privacy, retention, suppliers, classification.

HR: joiners, leavers, training, discipline.

Facilities: offices, visitors, equipment.

This guide is offered for general information only and is not legal, regulatory or certification advice. Gapless does not audit or certify you; certificates are issued by your chosen certification body. Please take professional advice where needed.

Manage your risk

13 Generate the risk register
Generate it from your confirmed observations.
IN APP: **Risk Register**

14 Give each risk an owner and treatment
Assign an owner, choose a treatment and map it to Statement of Applicability controls.
IN APP: **Risk Register**

15 Check risks against your appetite
Make sure the register and appetite agree and the leftover risk is acceptable.
IN APP: **Risk Register and Risk appetite**

16 Turn treatments into tasks
Create tasks to close each gap, then work through them.
IN APP: **Tasks, traced on the Statement of Applicability**

Policies

17 Generate and assign policies
Generate the set and assign each policy to the right stakeholder.
IN APP: **Policies**

18 Customise and review
Edit each draft so it describes how you really work.
IN APP: **Policies**

19 Send to the team to read and sign
Distribute to everyone and track signatures.
IN APP: **Policies and People**

Get audited

20 Check readiness, review management
Check you are as audit-ready as you can be, and hold your management review (clause 9.3), keeping the minutes.
IN APP: **Audit review**

21 Choose your certification body
Raise a support ticket and we will talk it through with you.
IN APP: **Support**

22 Invite your auditor
Invite them in to review and comment.
IN APP: **Collaborators**

23 Fix findings and pass
Answer each nonconformity, talk to your auditor in the platform and receive your certificate.
IN APP: **Audit review**

FINISH LINE

Your ISO 27001 certificate

Issued by your certification body, not by Gapless.

KEEP THESE UP TO DATE

People, Devices, Vendors: the lists the auditor samples from.

Incidents: log them as they happen.

Training: staff awareness is something auditors ask to see.

AFTER YOU PASS

The audit has two stages: documents first, then how it works in practice.

Surveillance audit every year, recertification every three years.

Update your risk appetite and register when the business changes.

This guide is offered for general information only and is not legal, regulatory or certification advice. Gapless does not audit or certify you; certificates are issued by your chosen certification body. Please take professional advice where needed.