ComplianceClaw
ISO 27001 | evidence packs | VDR governance

COMPLIANCECLAW

ISO 27001 Readiness Kit

A practical first-pass guide for SaaS teams that need to define scope, spot evidence gaps, and decide the right next step before they waste weeks on the wrong work.

What this guide is for

- Get clear on scope before the work sprawls.
- Spot the first evidence gaps worth fixing.
- Work out what matters now, what can wait, and what good enough looks like for a first pass.

A practical first-pass guide for understanding the work, spotting the weak points, and choosing a sensible next step.

ComplianceClaw
Contents

INSIDE THIS PDF

Contents

ComplianceClaw
Free readiness kit

ORIENTATION FIRST

What this kit helps you do

move from "we think it's secure" to "we can prove it".

WHAT THIS GUIDE SHOULD HELP YOU DO

Get to a sensible first working view

This guide is intentionally diagnostic. By the end of a first pass, you should have a sharper scope, named owners, and a more realistic view of what is actually missing instead of a vague feeling that everything is broken.

WHAT IT DELIBERATELY DOES NOT INCLUDE

No editable implementation layer

You will not get trackers, folder structures, response drafts, or tailored setup work here. That line matters because a useful free guide should help you think clearly, not pretend it replaces the build-out work.

Good enough for a first pass: you can explain scope, name the weak evidence, point to the next two or three actions, and say who owns them without hand-waving.

ComplianceClaw
How to use this kit

How to Use This Guide

Who this is for

This guide is for small SaaS teams, usually seed to Series A, where a founder, ops lead, or first security owner has heard some version of “we need ISO 27001” and now needs a sensible place to start.

It is especially useful when the team is small, engineering time is scarce, and nobody wants to burn the next month copying generic policy packs that do not fit the business.

What success looks like

A good first pass does not mean you are suddenly audit ready. It means the conversation stops being fuzzy.

That sounds small, but it is not. A surprising amount of wasted time comes from teams doing work they cannot yet explain.

By the end of the first working session, you should be able to say:

- what is actually in scope first
- which evidence gaps are real versus imagined
- which two or three fixes should happen next
- who owns them, and when you will check progress

That is enough to move forward. You do not need a perfect spreadsheet or a huge policy pack on day one.

What this guide covers

Inside this PDF you will find a readiness checklist, a minimum evidence pack summary, common failure patterns, and a next-step guide. The point is to help you think clearly before you start creating documents or buying help.

This is an orientation document. It helps you assess, prioritise, and explain the work internally. It is meant to make the first decisions easier, not to replace the heavier implementation work.

What this guide does not cover

This guide does not replace a formal gap analysis. It does not guarantee certification. It does not include editable policy templates, evidence trackers, customer questionnaire drafts, or a tailored

folder setup.

That boundary matters. The free document should help you understand the work, spot weak areas, and avoid wasting time. The paid offers start where most teams hit the setup problem: turning understanding into a clean working system.

Best way to run the first session

Use this guide in a 60 to 90 minute working session with the founder, the person who owns delivery or operations, and someone who knows how the stack really works.

Use the session to answer four practical questions:

1. What systems and teams are actually in scope first? 2. If a customer asked for proof next week, where would we be exposed? 3. Which policies or recurring processes are clearly missing or informal? 4. Who owns the first week of follow-up?

Do not try to solve every control in one sitting. That is where teams go sideways. If you leave with a clean map and a short action list, that is a good result.

I would much rather see a team leave that session with three honest decisions than twenty vague promises.

What to collect before that session

Bring these inputs into the room if you already have them:

- your cloud provider and key SaaS vendor list
- any existing security, access, or incident docs
- a rough asset list for product, customer data, laptops, and admin tools
- one recent customer security questionnaire, if you have one
- any current onboarding, offboarding, or access review process notes

Even partial material is useful. The point is to stop working from memory.

How to read the rest of this PDF

Do one fast read first. Do not try to complete the work in order while you are still understanding the shape of it.

Then come back through the sections with three questions in mind:

- why does this matter in our environment?
- what proof do we already have, even if it is messy?
- what would count as good enough for the next review, not forever?

That last question matters more than people think. Teams often stall because they assume every document needs to be polished before it is useful. It does not. First-pass evidence can be rough, as long as it is real, current, and owned.

A sensible order for the first two weeks

Most teams move faster if they work in this order:

Week 1: get the shape of the work right 1. define scope 2. name the first evidence gaps 3. agree the minimum policy baseline 4. assign owners for the obvious missing pieces

Week 2: make the work visible 1. set up one place to collect proof 2. gather the easiest real evidence first 3. clean up any access or ownership blind spots you already know about 4. book the next review before the work goes stale

That is not glamorous, but it is what gets motion started. A lot of ISO 27001 work is like that. The flashy part is rarely the part that saves you.

A useful rule of thumb before you move on: if you can explain the work but still do not have the actual working files or structure, you have probably reached the edge of what a guide like this should do.

ComplianceClaw
First-pass checklist

FIRST-PASS CHECKLIST

The five early moves that matter most

These are the highest-leverage actions for a team that is still trying to get organised, not trying to look mature on paper. Each one exists to reduce confusion, expose the real gaps, and make the next review easier.

1. Scope and boundary

- Choose the first systems, people, and suppliers that belong inside scope. Start with the customer-facing product environment rather than every internal process at once.
- Write down what is intentionally out of scope for now so the team does not argue about it in every meeting.

2. Risk and control baseline

- Identify the assets that matter most, the real threats against them, and the controls you already have.
- Rate likelihood and impact simply. You need a usable risk view, not a perfect spreadsheet on day one.

3. Statement of Applicability and core docs

- Draft the Statement of Applicability around the controls that really fit your environment, including justified exclusions.
- Set the first policy baseline: access control, incident response, secure development, and backup or continuity expectations.

4. Ownership and repeatability

- Appoint one person to drive the work, even if ISO 27001 is only part of their role right now.
- Turn joiners, leavers, reviews, and incidents into repeatable routines rather than one-off cleanups.

5. Evidence collection

- Collect proof as you go: access reviews, incident notes, onboarding records, vendor decisions, and system inventory updates.
- Set up one central evidence room early so customer reviews and later audit prep do not become a file-hunt.

What success looks like after this pass: you know what is in scope, what evidence is weak, which baseline docs are missing, who owns the next week of follow-up, and what can wait until later. That is enough to move forward.

ComplianceClaw
Three realistic starting points

THREE REALISTIC STARTING POINTS

What this work looks like in the wild

A lot of ISO 27001 advice becomes clearer once you attach it to a real situation. These are simplified examples, but they are close to how teams usually arrive at this work.

Small SaaS team, no security owner yet

This is the most common starting point. The useful move here is not to pretend you have a full security function. Keep scope tight, choose one operating owner, and gather the evidence you already create without noticing, such as access decisions, onboarding steps, vendor choices, and backup checks.

Enterprise prospect already asking questions

In this situation, speed matters more than completeness. You do not need every document in perfect form. You need to know where the obvious gaps are, what you can answer honestly now, and what evidence needs to be made easier to find this week.

Certification is coming, but not immediately

This is the sweet spot for using the guide properly. There is enough time to do the groundwork in the right order. Focus on scope, policy baseline, ownership, and evidence discipline before you worry about making everything look polished.

ComplianceClaw
Minimum useful proof

MINIMUM USEFUL PROOF

Your first evidence pack summary

You do not need every document on day one. You do need enough proof to show that the work is real, owned, and likely to hold up under customer scrutiny. The question is not “is this perfect?” It is “would this survive a reasonable follow-up question?”

EVIDENCE ITEM	WHY IT MATTERS	PRIORITY
Security policy baseline	A short usable policy set covering access control, incidents, acceptable use, secure development, and backup expectations.	Must-have
Asset register	A living list of systems, apps, laptops, data stores, and critical vendors that sit inside scope.	Must-have
Risk register	The main threats, impact, treatment decision, owner, and target date.	Must-have
Statement of Applicability	A clean map of relevant controls, what is implemented, and any justified exclusions.	Must-have
Access review evidence	Proof that privileged and sensitive-system access is reviewed and excess access is removed.	Must-have
Joiner and leaver process	A documented onboarding and offboarding checklist with ownership and sign-off.	Should-have
Incident log	Even minor events should be recorded, investigated, and closed out with notes.	Should-have
Backup or continuity proof	Enough to show critical data and service recovery is defined and testable.	Should-have
Supplier review notes	A lightweight review trail for critical third-party providers and processors.	Should-have
Security awareness evidence	Proof that staff were briefed on security expectations and handling responsibilities.	Nice-to-have

What weak evidence usually looks like

An undocumented routine, a half-remembered process, a screenshot with no date, or a policy nobody can explain. It

What usable first-pass evidence looks like

Something current, real, and owned. It can be simple. A dated access review note, a short incident log, or a clear vendor

may be better than nothing, but it will not hold up for long.

decision record is often enough to move the conversation forward.

A useful first-pass evidence set is real, current, and easy to explain. It does not need to be beautiful yet. If the problem becomes “we understand this, but we still need the working structure and files,” that is the point where the €49 Starter Pack becomes relevant.

ComplianceClaw
Avoidable mistakes

AVOIDABLE MISTAKES

Common ways teams burn time

These are the mistakes that usually waste more time than the controls themselves. Most of them come from doing work in the wrong order, not from a lack of effort.

Trying to document everything before deciding scope

Teams often produce policy sprawl before they agree what the first ISMS boundary even is. That creates rework and weak ownership. Practical takeaway: lock the first scope boundary early, even if it is narrower than the final ambition.

Using generic templates that nobody can defend

A large copied policy pack looks impressive until someone asks how it matches your actual tooling and processes. Practical takeaway: prefer fewer documents that match reality over more documents that sound enterprise-grade but are not lived.

Waiting until audit pressure to start collecting proof

The late-stage scramble is usually an evidence problem, not a theory problem. Practical takeaway: start collecting access reviews, onboarding records, incident notes, and vendor decisions as part of normal operations now.

Leaving ownership fuzzy

Controls fail when everyone assumes someone else owns them. Practical takeaway: each gap from this guide should end with one named owner, one next action, and one review date.

ComplianceClaw
What to do next

What To Do Next

You have the checklist. The next decision is not whether ISO 27001 matters. It is how much of the next layer you want to build yourself.

Most teams do not get stuck because the checklist is weak. They get stuck when the work stops being conceptual and turns into setup, cleanup, and proof. That is the part that quietly eats time.

When this free guide is enough

Stay with the free guide for now if all of these are true:

- you mainly need orientation, not deliverables
- your timeline is measured in months, not weeks
- someone on the team can own document cleanup and evidence collection
- you are comfortable building your own trackers, templates, and folder structure

This route can work well. Just be honest about the trade-off: you save money, but you spend more operator time and there is more room for avoidable mess. There is nothing wrong with that trade if the timeline is loose and somebody genuinely owns it.

When the €49 Evidence Room Starter Pack is the right next step

For most readers, this is the practical next move.

Choose it if you now understand the work but can already see the setup burden ahead. The pack gives you the implementation layer this guide deliberately avoids: folder structures, trackers, editable working files, naming standards, setup guidance, and a cleaner route through the messy middle.

That matters because ISO 27001 readiness usually slows down in one of two places: people are unsure what acceptable evidence looks like, or nobody wants to build the working system from a blank page. The €49 pack is meant to solve that very ordinary, very annoying middle layer.

Evidence Room Starter Pack, €49 **https://complianceclaw.app/complianceclaw-offer-start/starter-pack**

When the €299 Tailored Evidence Setup is justified

Choose Tailored Evidence Setup if your situation is more urgent or more specific than a generic pack can cover.

That usually means at least one of these is true:

- a customer review is already in motion
- your stack or data flows are unusual enough that generic structure will create rework
- the team has very little tolerance for trial and error
- you want the starting point shaped around your actual environment, not retrofitted later

This is not the €49 pack with a higher price. It is the faster route when the cost of getting the setup wrong is already high. In other words, when trial and error has become expensive.

Learn more about Tailored Evidence Setup **https://complianceclaw.app/tailored-evidence-setup**

Simple rule of thumb

Use this guide if you still need clarity. Use the €49 pack if the next problem is setup. Use the €299 setup if the next problem is speed or specificity.