GUIDE

How to Use This Kit

Adapt, approve and roll out your ISO 27001 starter policies in the right order

What is inside

This kit gives a small or mid-sized SaaS company the core documents most ISO 27001 programs start with. Each one is written for a company of 20 to 300 people that runs on cloud infrastructure, has remote staff and manages laptops with an MDM.

Document	Type	What it does
How to Use This Kit	Guide	Explains the order, placeholders, approval and evidence
Information Security Policy	Policy	Top level policy: objectives, commitment, roles, risk approach, policy framework
Access Control Policy	Policy	SSO, MFA, least privilege, joiners movers leavers, privileged access, access reviews
Acceptable Use Policy	Policy	Rules for staff on devices, data, AI tools, remote work and reporting
Incident Response Plan	Policy	Severity levels, roles, response phases, notification and evidence handling
Risk Management Procedure	Policy	Asset inventory, scoring scales, acceptance criteria, treatment, SoA
Risk register and Statement of Applicability	Spreadsheet	Working files that the Risk Management Procedure describes

The SoA, or Statement of Applicability, is the list of Annex A controls you chose, the reason for each choice, and whether each one is in place.

> **Warning:** These are templates. They are a starting point, not a finished ISMS. Every document must be adapted to how your company actually works, then reviewed and approved by your own management. An auditor tests what you do, not what a template says.

The order to adapt documents

Work in this order. Each step feeds the next.

1. **Define your ISMS scope first.** Write down which products, teams, locations and cloud accounts are in scope. The Information Security Policy refers to this scope, so you need it before anything else.
2. **Information Security Policy.** Set the objectives, the roles and the policy framework. This document tells everyone else which policies exist.
3. **Risk Management Procedure.** Agree on the scales and the acceptance level before you run the first risk assessment.
4. **Risk register and SoA.** Run the first assessment with the spreadsheet. The risks you find tell you which controls you need, and which policies must be stricter or lighter.
5. **Access Control Policy.** Match it to your real identity setup (for example Google Workspace or Okta, AWS IAM Identity Center, GitHub).
6. **Acceptable Use Policy.** Match it to your MDM, your approved tools and your AI tool rules.
7. **Incident Response Plan.** Fill in the contact list and run a tabletop exercise before you call it done.

> **Tip:** Do not try to finish all policies in one week. A realistic pace for a small team is one policy per week, with the risk assessment in parallel.

How to fill placeholders

Every text in square brackets is a placeholder. In the Word files it is highlighted so you can find it fast.

- **Names and roles:** replace [IT Manager], [Security Lead] or [CTO] with the role title used in your company. Use role titles, not personal names, so the policy survives staff changes.
- **Numbers:** replace [number] days with a value you can actually meet. If you write 24 hours to remove access but your offboarding takes three days, the auditor will raise a nonconformity.
- **Tools:** replace [ticketing tool], [MDM] or [identity provider] with the real product names.
- **Search before you publish:** search each file for an opening square bracket. No placeholder should remain in an approved document.
- **Delete what does not apply.** If you have no office, remove office rules. A short true policy is better than a long one you do not follow.

How to approve and communicate policies

1. **Review.** Send each draft to the owner named in the document control table and to the people who must follow it, for example engineering leads for the Access Control Policy.

2. **Approve.** Top management approves the Information Security Policy. The policy owner or the security committee can approve the others if the Information Security Policy says so. Record the approver, the date and the version in the document control table.
3. **Publish.** Put approved PDFs in one place everyone can reach, such as your intranet, a shared drive folder or your compliance platform (Vanta, Drata or Sprinto).
4. **Communicate.** Announce the policies in Slack or by email, explain what changed, and ask staff to acknowledge them.
5. **Collect acknowledgments.** New hires acknowledge during onboarding. All staff acknowledge again each year and after major changes.
6. **Review yearly.** Review every document at least once a year and after any significant change to the business, the infrastructure or the risks.

Evidence auditors expect

Auditors check that each document is approved, known and followed. Prepare this evidence for each one.

Document	Evidence auditors usually ask for
Information Security Policy	Approved and dated version, record of top management approval, staff acknowledgments, security objectives with measurements, management review minutes
Access Control Policy	SSO and MFA settings screenshots, onboarding and offboarding tickets, completed access reviews with sign-off, privileged account list, service account inventory
Acceptable Use Policy	Signed or recorded acknowledgments, MDM compliance report (encryption, screen lock, OS updates), security awareness training records, list of approved AI tools
Incident Response Plan	Incident log, at least one completed incident or tabletop exercise report, lessons learned with actions, updated contact list
Risk Management Procedure	Risk register with owners and dates, risk treatment plan, signed acceptance of residual risks, current SoA, records of the last risk review

> **Tip:** Save evidence when the activity happens, not the week before the audit. A quarterly access review with a dated sign-off is strong evidence. A screenshot taken the day before the audit shows only that today is fine.

Adaptation checklist

- [ ] ISMS scope is written and approved

- [ ] Company name, roles and tools replace all placeholders in every document
- [ ] Every number (days, hours, frequency) is one the company can meet
- [ ] Sections that do not apply are removed or rewritten
- [ ] Information Security Policy approved by top management
- [ ] Risk scales and acceptance level agreed before the first assessment
- [ ] First risk assessment done and recorded in the risk register
- [ ] SoA completed with a reason for every included and excluded control
- [ ] Incident contact list filled in and tested
- [ ] All policies published in one place staff can reach
- [ ] Staff acknowledgments collected and stored
- [ ] Annual review dates set in a calendar or the compliance platform

Next steps

To understand how these documents fit into a full ISMS, watch the free ISO 27001 Deep Dive on YouTube. If you want help adapting the kit or planning your certification, book a free 30 minute call.