



Community Library

ISO 27001 Incident Response Plan Checklist

Ten checks so the plan, the decision, and the lesson are already in place.

4

The plan

4

The first hours

2

After it closes

1.0 · 2026-10

itrygg.com

How to use this checklist

An incident is easier to run when the names, the phone numbers, and the decision are already written down. Give this list to the people who would be called. Each step also names the proof your ISO/IEC 27001 program should already be able to show.

- 1. Work the parts in order: write the plan, act in the first hours, then learn from it.
- 2. The Proof line is the record your program keeps. If you cannot produce it, the task is not done.
- 3. References point to ISO/IEC 27001:2022 Annex A controls, for example A.5.24.
- 4. This is guidance. Confirm who you must tell, and by when, with your counsel. Keep one printed copy where the team can reach it if email is down.

The plan	The first hours	After it closes
Before anything happens	When something is happening	When the immediate work is done

Write the plan

Who decides, how people report, who you call, and a practice run.

- ☐ Name who is in charge, who decides that something is an incident, and who is allowed to speak outside the company. A.5.24

Proof: The named roles, and the last time those names were checked.

- ☐ Write how anyone reports something that looks wrong, including outside office hours, and where that report lands. A.6.8

Proof: The reporting path staff were given, and one example of a report that arrived.

- ☐ Keep a list of who you may need: your IT provider, insurer, counsel, and the authority you would call. Store the numbers where the team can reach them if email is down. A.5.5, A.5.6

Proof: The contact list, with the date it was last checked, and where the offline copy is kept.

- ☐ Practice the plan at least once a year. Include who you would tell and how the business would keep working. A.5.24, A.5.30

Proof: The date of the last practice, who took part, and what you changed afterward.

The first hours

A written decision, a stop to the spread, evidence kept, and one voice outside.

- ☐ Decide whether it is an event or an incident, and how serious it is. Write the decision and who made it. A.5.25

Proof: The decision, the time, and the name of the person who made it.

- ☐ Stop it spreading. Isolate the affected account or system, and record what you changed. A.5.26

Proof: What was isolated, when, and by whom.

- ☐ Keep the evidence. Do not wipe a machine, or reset an account, before someone who knows how has a copy. A.5.28

Proof: What was kept, where it is stored, and who is allowed to handle it.

- ☐ Tell the people who need to know, inside and outside, from the list you already wrote. One person speaks for the company. A.5.26, A.5.5

Proof: Who was told, when, and by whom.

After it closes

The lesson is written, and the business can still run.

- ☐ Write what happened, what it affected, and what you will change. Share that lesson with the people who would spot it next time.

A.5.27, A.6.3

Proof: The written lesson, the change you made, and who it was shared with.

- ☐ Confirm the business can keep running while the fix is unfinished, and that a backup you would restore from still works.

A.5.29, A.8.13

Proof: How work continued, and the date of the last successful restore test.

Want the plan, the decision, and the lesson to live in the program?

Trygg keeps the incident record, the decision, and the proof in one place.

[Book a demo](https://itrygg.com/#demo) (itrygg.com/#demo)

[ISO 27001 Preparation Checklist](https://itrygg.com/community/library/iso-27001-preparation-checklist) (itrygg.com/community/library/iso-27001-preparation-checklist)

Portal demos follow a mutual NDA.

isms@itrygg.com

This checklist is guidance, not a substitute for the ISO/IEC 27001:2022 standard. Purchase the standard from ISO or your national standards body. Certification decisions are made only by accredited certification bodies.

© 2026 Trygg, Inc.