



Community Library

# ISO 27001 Ransomware Readiness Checklist

Ten checks that decide whether ransomware costs you a day or a month.

**4**

Prevent

**4**

Recover

**2**

Respond

1.0 · 2026-10

[itrygg.com](https://itrygg.com)

# How to use this checklist

Ransomware is a day or a month depending on whether the backup, the contacts, and the decision are already in place. Give this list to the people who would have to act. Each step also names the proof your ISO/IEC 27001 program should already be able to show.

- 1. Work the parts in order: prevent, recover, then respond.
- 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.8.13.
- 4. This is guidance. Work with your IT provider, insurer, and counsel. Keep one printed copy offline.

| Prevent           | Recover                  | Respond         |
|-------------------|--------------------------|-----------------|
| Before it happens | If you have to come back | When it happens |

## Prevent

Sign-in, patches, admin rights, and endpoint alerts are already in place.

- ☐ Turn on MFA everywhere people sign in, including email, VPN, remote access, and admin tools. Admins use phishing-resistant MFA. A.8.5, A.5.17

Proof: A record of where MFA is on, and which admin accounts use phishing-resistant MFA.

- ☐ Patch exposed systems fast. Fix critical flaws in VPNs, firewalls, and remote access tools within days, not months. A.8.8

Proof: Patch record for those systems, with the date the critical fix was applied.

- ☐ Limit admin rights. Few admins, separate admin accounts, and no email or browsing while signed in as admin. A.8.2

Proof: Admin account list, and the rule that admin accounts are not used for email or browsing.

- ☐ Watch every endpoint. Endpoint detection on every laptop and server, with alerts someone watches around the clock. A.8.7, A.8.16

Proof: Coverage list of laptops and servers, and the name of who watches the alerts.

## Recover

A backup they cannot encrypt, a restore you have timed, targets leaders agreed, and a paper contact list.

- ☐ Keep at least one backup copy offline or immutable, protected by separate credentials. A.8.13

Proof: Backup record naming the offline or immutable copy and the separate credentials.

- ☐ Restore a critical system end to end at least twice a year, and record how long it took. A.8.13, A.5.30

Proof: Restore test record with the system, the date, and the time it took.

- ☐ Agree how long each critical system can be down, and how much data you can lose. A.5.29, A.5.30

Proof: Written recovery targets for each critical system.

- ☐ Print the contact list: incident lead, IT or provider, insurer, legal counsel, bank, and key staff. Email may be down. A.5.24, A.5.5

Proof: A printed copy stored offline, with a date.

## Respond

Someone is named to decide, and the leaders have practiced once this year.

- ☐ Name who can shut systems off, call the insurer, and decide what to do about a ransom demand. A.5.24, A.5.26

Proof: Named decision makers on the incident plan.

- ☐ Run a ransomware tabletop with leaders once a year, then fix the gaps it finds. A.5.24, A.5.27

Proof: Exercise record with the date, who came, and the gaps that were fixed.

## **Want the backup test and the decision to live in the program, not in a binder no one opens?**

Trygg keeps the restore test, the contact list, 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](mailto: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.