

NIS2 & CIRCIA incident reporting readiness checklist

Tracknosis · tracknosis.com · October 2026

General information, not legal advice. Requirements vary by country, sector and organisation, and national NIS2 laws add their own detail. Check what applies to you with your legal or compliance team. Current as of October 2026.

Tracknosis helps with 17 of the 33 items, including every item in the 72-hour notification.

Items marked **Tracknosis helps** are the evidence-heavy ones: they usually take longest during an incident, and they are where reports most often fall short.

BEFORE Be ready before an incident

Most reporting problems start before the incident: nobody knows who decides, or there is no evidence to report from.

- ☐ Confirm whether NIS2 applies to you (sector and size), and whether you are an essential or important entity.
- ☐ Know which national authority or CSIRT you report to, and how (portal, email, phone).
- ☐ Check whether CIRCIA will apply to you as US critical infrastructure, and track the final rule.
- ☐ Decide who declares an incident "significant", who writes the reports and who approves them, including out of hours.
- ☐ Make sure your management body has approved your cyber risk measures and knows its NIS2 responsibilities.
- ☐ Prepare report templates for the early warning, notification and final report.
Tracknosis helps
- ☐ Take a baseline of key systems now, so you can later show exactly what changed.
Tracknosis helps
- ☐ Make sure logging and auditing are switched on, and that you would notice if they were switched off or cleared. **Tracknosis helps**

- ☐ Make sure evidence records who collected it, when, and from which machine.

[Tracknosis helps](#)

- ☐ Run a tabletop exercise against the 24-hour, 72-hour and one-month clock.

24 HOURS NIS2 early warning

Within 24 hours of becoming aware of a significant incident.

- ☐ Record the time you became aware of the incident: this starts the clock.

- ☐ State whether the incident is suspected to be caused by unlawful or malicious acts. [Tracknosis helps](#)

- ☐ State whether it could have a cross-border impact.

- ☐ List the systems known to be affected so far. [Tracknosis helps](#)

- ☐ Preserve evidence before rebuilding or restoring anything: scan first, then fix.

[Tracknosis helps](#)

72 HOURS NIS2 incident notification

Within 72 hours of becoming aware, updating the early warning.

- ☐ Give an initial assessment of the incident, including its severity and impact.

[Tracknosis helps](#)

- ☐ Include indicators of compromise where available: files, registry keys, auto-starts, accounts, addresses. [Tracknosis helps](#)

- ☐ Establish what changed on affected machines and when it started.

[Tracknosis helps](#)

- ☐ Check for signs of tampering, such as cleared event logs or switched-off auditing.

[Tracknosis helps](#)

- ☐ Be ready to give intermediate status updates if the authority or CSIRT asks for them. [Tracknosis helps](#)

1 MONTH NIS2 final report

Within one month of the incident notification.

- ☐ A detailed description of the incident, including its severity and impact.

[Tracknosis helps](#)

- ☐ The type of threat or likely root cause. [Tracknosis helps](#)
- ☐ The mitigation measures applied and still under way. [Tracknosis helps](#)
- ☐ Any cross-border impact.
- ☐ If the incident is still ongoing at one month, send a progress report, then the final report within one month of handling it.
- ☐ Confirm the attacker's foothold is gone before closing: auto-starts, services and recent changes checked. [Tracknosis helps](#)

CIRCIA

US critical infrastructure

Deadlines are set in the law; the final rule decides who is covered and what reports contain.

- ☐ Report a covered cyber incident within 72 hours of reasonably believing it occurred.
- ☐ Report a ransom payment within 24 hours of making it.
- ☐ Send supplemental reports if substantial new or different information becomes available. [Tracknosis helps](#)
- ☐ Preserve data relating to the incident. [Tracknosis helps](#)

OTHER

Other clocks that may run at the same time

- ☐ UK GDPR: personal data breaches reported to the ICO within 72 hours.
- ☐ DORA: EU financial firms send an initial notice within 4 hours of classifying an incident as major.
- ☐ UK Cyber Security and Resilience Bill: proposes 24-hour and 72-hour reporting; currently in Parliament.

Tracknosis shows every file and registry change on your Windows machines between scans, flags signs of tampering, stamps each scan with machine, operator and time, and drafts incident reports from that evidence for your team to review. tracknosis.com · info@tracknosis.com