NIS2 incident reporting checklist

What to prepare before an incident, and what to send to the CCB within 24 hours, 72 hours and one month after a significant incident.

NIS2 Aware · nis2aware.eu · November 2026

Before an incident: be ready

- [ ] **Write a one-page incident procedure**
  Who to call, who decides, who notifies, and how to reach them outside normal channels.
- [ ] **Define what a significant incident is for you**
  Translate the criteria (severe disruption, financial loss, damage to others) into concrete thresholds for your services.
- [ ] **Name the people who notify the CCB, with back-ups**
  The early warning is due within 24 hours, including weekends and holidays.
- [ ] **Keep contacts and the procedure available offline**
  Email and systems may be down during an incident.
- [ ] **Make sure logs are kept long enough**
  You will need them to understand the incident and write the reports.
- [ ] **Prepare message templates**
  For the CCB, for affected clients and for staff.
- [ ] **Test the procedure with an exercise**
  A short tabletop exercise once a year shows the gaps.

Within 24 hours: early warning

- [ ] **Send the early warning to the CCB**
  Within 24 hours of becoming aware of the significant incident.
- [ ] **Indicate whether it may be caused by unlawful or malicious acts**
  A first impression is enough at this stage.
- [ ] **Indicate whether it could have a cross-border impact**
  For example if services in other EU countries are affected.

Within 72 hours: incident notification

- [ ] **Send the incident notification**
  Within 72 hours of becoming aware of the incident, updating the early warning.
- [ ] **Give an initial assessment of severity and impact**
  Which services, how many users, how long.
- [ ] **Share indicators of compromise where available**
  For example suspicious IP addresses, domains or files.

Within one month: final report

- [ ] **Describe the incident in detail**
  Including its severity and impact.
- [ ] **Explain the type of threat or root cause**
  What happened, how the attacker got in, or what failed.
- [ ] **List the mitigation measures applied and ongoing**
  What you did to stop it and to prevent it from happening again.
- [ ] **Mention any cross-border impact**
  Where applicable.
- [ ] **If the incident is still ongoing, send a progress report**
  The final report then follows within one month after the incident has been handled.

After the incident

- [ ] **Inform the recipients of your services where needed**
  Clients affected by the incident, and the measures they can take.
- [ ] **Hold a lessons-learned session**
  What worked, what didn't, what to change.
- [ ] **Update your risk analysis, measures and procedure**
  And report back to the management body.

General information on the Belgian NIS2 framework as of November 2026, not legal advice. Always check the latest guidance from the CCB (ccb.belgium.be and atwork.safeonweb.be).