FRANKFORD'S SOLUTIONS

As of July 2026

NIS2 Readiness Checklist for Companies in Austria

Find out if you are in scope, know your duties, start on time. The Austrian NISG 2026 takes effect on 1 October 2026.

This checklist is for companies in Austria that are unsure whether NIS2 applies to them and what to do next. Austria implemented the EU directive with the NISG 2026, adopted in December 2025 and entering into force on 1 October 2026. Information current as of July 2026. This checklist is a practical guide, not legal advice.

1. Check if you are in scope

- [ ] Check whether your business falls into one of the 18 NIS2 sectors.
  High-criticality sectors include energy, transport, banking, health, drinking water, waste water and digital infrastructure. Other critical sectors include postal services, waste, chemicals, food, manufacturing, digital providers and research.
- [ ] Check the size thresholds: you are in scope with 50 or more employees, or with more than EUR 10 million turnover and more than EUR 10 million balance sheet total, provided you operate in one of the 18 sectors.
  Smaller companies are only covered directly in special cases, for example DNS providers or qualified trust services.
- [ ] Determine whether you count as an essential or an important entity.
  Essential entities face stricter supervision. Fines go up to EUR 10 million or 2 percent of worldwide annual turnover, for important entities up to EUR 7 million or 1.4 percent. In each case the higher amount applies.
- [ ] Run the free WKO self-check at ratgeber.wko.at/NIS2 (in German).
- [ ] Check whether affected customers pass NIS2 requirements on to you through contracts.
  Through the supply chain, NIS2 also reaches companies that are not covered by the law themselves.

2. Management duties

- [ ] Put NIS2 on the management agenda.
  Management bodies must approve the risk management measures and oversee their implementation. This cannot be fully delegated to IT. Members of management can be held personally accountable for breaches of these duties.
- [ ] Schedule the mandatory cybersecurity training for management.
- [ ] Appoint a person responsible for information security, plus a deputy.
  Not an explicit legal requirement, but recommended so that responsibility is clear in day-to-day operations.
- [ ] Reserve budget and time for implementation in the 2026/27 financial year.

3. Implement risk management measures

- [ ] Carry out a risk analysis of your network and information systems and document the results.
- [ ] Write down an information security policy.

- [ ] Set up an incident response process.
  Who detects an incident, who decides, who communicates. This must be settled in advance.
- [ ] Maintain backups and emergency plans and test recovery regularly.
- [ ] Assess the security of your supply chain, especially IT service providers and software vendors.
- [ ] Build security requirements into procurement, development and maintenance of your systems, including vulnerability handling.
- [ ] Introduce multi-factor authentication and grant access rights on a need-to-know basis.
- [ ] Use encryption for sensitive data and communication.
- [ ] Train your staff regularly on cyber hygiene and current threats.
- [ ] Define how you will regularly review the effectiveness of your measures.

4. Registration and reporting duties

- [ ] Register your company between 1 October and 31 December 2026 via the Austrian business service portal (USP).
  If you fall into scope later, you have three months from that point to register.
- [ ] Define who reports security incidents to the authority and make sure they can be reached outside office hours.
- [ ] Align your reporting process with the three deadlines: early warning within 24 hours, incident notification within 72 hours, final report within one month.
  The deadlines apply to significant incidents. The early warning and the notification run from the moment you become aware of the incident. The final report is due within one month of the notification, and if the incident is still ongoing, a progress report is enough at that stage.
- [ ] Plan how you will inform affected customers if an incident disrupts your services.
- [ ] Note the self-declaration deadline: by 30 September 2027 you must report your implemented measures to the cybersecurity authority.
  According to the WKO, breaches of the registration or self-declaration duty can cost up to EUR 50,000, up to EUR 100,000 for repeat offences.

5. First steps before October 2026

- [ ] Run a gap analysis and turn it into an action plan with deadlines and owners.
- [ ] Review your contracts with IT service providers and add security and reporting obligations.
- [ ] Keep an eye on the regulations issued by the cybersecurity authority.
  Technical detail requirements and the self-declaration form may still be specified by regulation. Some points are still in flux.
- [ ] Document every step in a traceable way. In an audit, the evidence is what counts.

Frankford's IT-Solutions in Innsbruck can support you with the technical side, from MFA and secure software development to process automation. Just get in touch if you have questions.

Frankford's IT-Solutions GmbH · Fallmerayerstraße 14, 6020 Innsbruck, Austria · frankford-it.at · eduard.frankford@frankford-it.at · As of July 2026