NIS2/KSC CHECKLIST

NIS2 checklist for the Polish KSC Act: 40 questions before your audit

A NIS2 checklist for teams preparing their organisation for the requirements of the Polish National Cybersecurity System Act (KSC Act): 40 questions in six areas, each with its legal basis. Tick your answers on screen, then print the list or save it as a PDF - no email address required.

Checklist: innovix.pl/en/nis2/checklist/ · Innovix sp. z o.o., Aleja Śląska 1, 54-118 Wrocław, Poland · audyty@innovix.pl · +48 575 621 877

The questions follow the order in which organisations usually prepare: first your status and entry in the register, then the responsibilities of the head of the entity, the information security management system, significant incidents, documentation and, finally, the audit. Every “no” or “I don't know” is an item for your implementation plan - entities that met the criteria on the date the amendment entered into force have until 3 April 2027 to implement the obligations.

Not sure yet whether the Act applies to your organisation? Start with our NIS2 scope checker.

Status and registration

The starting point: whether and how the Act applies to your organisation.

1. ☐ Have you determined your organisation's status (essential entity, important entity or out of scope) and documented the reasoning: sector, type of entity and size, including linked and partner enterprises? (Art. 5)

2. ☐ Do you know which authority is competent for your sector and which CSIRT receives your incident notifications? (Arts. 41 and 41a; Art. 44 of the amending act)

3. ☐ Have you applied for entry in the register in the S46 system, or completed your data after being requested to do so by the Minister of Digital Affairs? (Art. 7c(1), Art. 7b(2))

4. ☐ Is the data in the register up to date, and do you notify changes within 14 days? (Art. 7c(3))

5. ☐ Does your organisation use the S46 system, and has it designated an account administrator? (Art. 9(1)(4), Art. 7(2)(11))

Head of the entity and organisational arrangements

The head of the entity is responsible for the obligations - even where they have been entrusted to others.

6. ☐ Has the head of the entity taken decisions on the preparation, implementation, review and supervision of the information security management system? (Art. 8c, Art. 8d(1))

7. ☐ Have adequate financial resources been planned for cybersecurity? (Art. 8d(2))

8. ☐ Have the head of the entity and the person to whom they have entrusted cybersecurity obligations completed documented training in this calendar year? (Art. 8e)

9. ☐ Have the tasks been assigned - to an internal structure or, under a contract, to a managed security service provider? (Art. 14)

10. ☐ Have the persons performing tasks under Arts. 8 and 11 submitted a certificate from the National Criminal Register before starting work? (Art. 8f)

Information security management system

The requirements of Art. 8(1) - entities that existed when the amendment entered into force must meet them by 3 April 2027.

11. ☐ Is the risk of an incident assessed and managed systematically, using a documented method? (Art. 8(1)(1))

12. ☐ Do you have information system security policies and topic-specific policies adopted by a management decision? (Art. 8(1)(2)(a))

13. ☐ Is security taken into account in the acquisition, development, maintenance and operation of systems, and are the systems tested - e.g. by penetration testing? (Art. 8(1)(2)(b))

14. ☐ Do physical access control and environmental safeguards cover server rooms and other places where data is processed? (Art. 8(1)(2)(c))

15. ☐ Do your processes for hiring, changes of role and staff departures cover the granting and revoking of access rights? (Art. 8(1)(2)(d))

16. ☐ Do you assess the security of suppliers of ICT products, services and processes, and do your contracts include security requirements? (Art. 8(1)(2)(e) and Art. 8(2))

17. ☐ Are business continuity, contingency and recovery plans implemented, documented and tested? (Art. 8(1)(2)(f))

18. ☐ Are backups separated from production systems, and are restores from them tested regularly? (Art. 8(1)(2)(f); Annex 4, Part I, points 10-11)

19. ☐ Is the information system monitored continuously? (Art. 8(1)(2)(g))

20. ☐ Do you have procedures for assessing the effectiveness of the technical and organisational measures implemented? (Art. 8(1)(2)(h))

21. ☐ Do staff receive cybersecurity training, and are basic cyber hygiene practices known and applied? (Art. 8(1)(2)(i)-(j))

22. ☐ Do you have rules for the use of cryptography, including encryption? (Art. 8(1)(2)(k))

23. ☐ Where appropriate, do you use multi-factor authentication and secure means of communication? (Art. 8(1)(2)(l))

24. ☐ Do you have an up-to-date asset inventory and an access control policy based on least privilege? (Art. 8(1)(2)(m)-(n))

25. ☐ Do you gather information on cyber threats and vulnerabilities - e.g. advisories from CSIRTs and software vendors? (Art. 8(1)(3))

26. ☐ Is software updated regularly, with an impact analysis, and are detected vulnerabilities remediated without delay? (Art. 8(1)(5)(b) and (d))

27. ☐ Do you protect the confidentiality, integrity, availability and authenticity of data, including against unauthorised modification? (Art. 8(1)(5)(a) and (c))

28. ☐ If you are a digital provider (e.g. cloud, data centre, managed services), does your system include the measures set out in Commission Implementing Regulation (EU) 2024/2690? (Art. 8b(1))

29. ☐ If you are an important entity that is a public entity, does your system meet the requirements of Annex 4 to the Act, and is it reviewed at least once a year? (Art. 8(3); Annex 4, Part III)

Incidents

Notifications through the S46 system within 24 hours, 72 hours and one month.

30. ☐ Do you have an incident management procedure covering detection, recording, classification and handling? (Art. 8(1)(4), Art. 11)

31. ☐ Do you know when an incident is significant - according to the thresholds in the Council of Ministers regulation or, for digital providers, in Regulation 2024/2690? (Art. 2(7), Art. 11(4))

32. ☐ Can you report a significant incident through S46: an early warning within 24 hours, an incident notification within 72 hours and a final report within one month? (Art. 11(1)(4)-(4c))

33. ☐ Do users of your services have access to information on cyber threats and a channel for reporting incidents and vulnerabilities? (Art. 9(1)(2)-(3))

34. ☐ Does the procedure provide for informing users about significant cyber threats and incidents that affect the service? (Art. 11(2a)-(2b))

Documentation and contacts

Evidence that the system works - for audits and supervision.

35. ☐ Do you have normative and operational documentation (including logs), under version control and retained for at least 2 years after it is withdrawn from use? (Art. 10)

36. ☐ Have you designated persons to liaise with the entities of the national cybersecurity system (at least two, or at least one in micro and small enterprises and in public entities that are important entities)? (Art. 9(1)-(3))

37. ☐ Can documents and evidence (records, test reports, the incident log) be provided quickly to the authority on request during supervision? (Art. 53c)

Security audit (essential entities)

An important entity undergoes an audit only when the authority orders one - these questions will be useful then too.

38. ☐ Have you planned the first security audit (by 3 April 2028 for entities that were essential entities when the amendment entered into force) and subsequent ones - at least once every 3 years? (Art. 15(1), Art. 33(2) of the amending act)

39. ☐ Does the auditor meet the requirements of the Act (an accredited body, or at least two auditors with certificates or practical experience), and are they independent - i.e. have they not performed tasks under Arts. 8-13 in your organisation in the year before the audit? (Art. 15(2)-(2a))

40. ☐ Do you know that a copy of the audit report must be sent to the competent authority within 3 working days of receiving it? (Art. 15(1a))

THIS CHECKLIST IS NOT LEGAL ADVICE

The questions summarise the obligations under the National Cybersecurity System Act as amended. They do not replace a legal analysis or an assessment of whether your measures are appropriate to the risk - for that, see our NIS2 gap analysis.

Legal status as of 8 October 2026 · Source: Act of 23 January 2026 amending the National Cybersecurity System Act and certain other acts (Dz.U. 2026 item 252) (in Polish)

Frequently asked questions

Does the checklist replace a gap analysis or the Art. 15 audit?

Does the checklist also apply to important entities?

How do I know whether my organisation is subject to the Act at all?

Sources

- Act of 23 January 2026 amending the National Cybersecurity System Act and certain other acts (Dz.U. 2026 item 252) (in Polish) (8 October 2026)
- National Cybersecurity System Act - act metadata and amending acts (Sejm ELI API) (in Polish) (8 October 2026)
- Ministry of Digital Affairs - Q&A on the amendment to the KSC Act, October 2026 update (1 October 2026; explanatory document, not legally binding) (in Polish) (8 October 2026)
- Commission Implementing Regulation (EU) 2024/2690 - technical and methodological requirements of cybersecurity risk-management measures (6 October 2026)

Legal status as of 8 October 2026 · Updated 8 October 2026