Velox | Secure IT infrastructure

NIS2 SERIES · BOOKLET 2 OF 4

Are you ready for NIS2?

Self-assessment questionnaire:
117 questions in 15 areas

Assess | Score | Set your priorities

Velox Ltd · Sofia

www.velox-systems.com

How to use this questionnaire

1. **Get the team together.** Fill it in together: someone from management and the person responsible for IT. Allow 60–90 minutes.
2. **Answer honestly.** Mark how things stand today, not your plans. "Fully in place" means it works, is documented and is checked.
3. **Use "N/A" sparingly.** Only when a question genuinely does not apply to you. These questions are left out of the score.
4. **Score each area.** Add up the points and count the answered questions (excluding N/A). Score = total ÷ (4 × answered) × 100.
5. **Plot your results.** Copy the percentages into the summary and onto the radar chart at the end of the booklet.

0	No — nothing done yet
1	Starting — intention or first steps
2	Partly — about half done
3	Nearly there — minor items left
4	Fully in place — works, documented and checked
N/A	Not applicable — left out of the score

Organisation _____

Completed by _____

Date _____

The areas

Each area lists the NIS2 measures it covers (Article 21(2) and other articles) and the matching ISO/IEC 27001:2022 requirements and controls. That makes the questionnaire useful for organisations already working to ISO 27001.

01	Scope and registration	5 questions	4
02	Management and accountability	8 questions	5
03	Risk management and policies	8 questions	6
04	Assets and inventory	7 questions	7
05	Access control and MFA	10 questions	8
06	Network security	10 questions	9
07	Endpoints and email	8 questions	10
08	Monitoring, logging and SIEM	10 questions	11
09	Incidents and reporting	10 questions	12
10	Continuity and backups	9 questions	13
11	Vulnerabilities and updates	8 questions	14
12	Cryptography	5 questions	15
13	Suppliers	7 questions	16
14	People, training and cyber hygiene	7 questions	17
15	Checking effectiveness	5 questions	18
—	Score summary		19
—	Readiness radar		20
—	How to read your score		21

0 No · **1** Starting · **2** Partly · **3** Nearly there · **4** Fully in place · **N/A** Not applicable

01 Scope and registration

NIS2: Art. 2, 3, 27 · ISO 27001:2022: Cl. 4.3 · A.5.31

№	Question	0	1	2	3	4	N/A
1.1	Have you checked whether your activities fall under the sectors in Annex I or II?	☐	☐	☐	☐	☐	☐
1.2	Have you established whether you are a medium-sized or large enterprise, counting linked and partner enterprises?	☐	☐	☐	☐	☐	☐
1.3	Do you know whether you are an essential or an important entity?	☐	☐	☐	☐	☐	☐
1.4	Have you submitted your details to the competent authority, and are they up to date?	☐	☐	☐	☐	☐	☐
1.5	Is there a procedure for reporting changes to your details within the deadline (two weeks in Bulgaria)?	☐	☐	☐	☐	☐	☐

Score, area 01 **Total** _____ **Answered** _____ **%** _____

0 No · **1** Starting · **2** Partly · **3** Nearly there · **4** Fully in place · **N/A** Not applicable

02 Management and accountability

NIS2: Art. 20 · ISO 27001:2022: Cl. 5 · A.5.1, A.5.2, A.5.4

№	Question	0	1	2	3	4	N/A
2.1	Has management formally approved the cyber risk-management measures?	☐	☐	☐	☐	☐	☐
2.2	Is there a named person responsible for cybersecurity, with clear authority?	☐	☐	☐	☐	☐	☐
2.3	Are security roles and responsibilities set out in writing?	☐	☐	☐	☐	☐	☐
2.4	Does management receive regular reports on the state of cybersecurity?	☐	☐	☐	☐	☐	☐
2.5	Is there a dedicated cybersecurity budget?	☐	☐	☐	☐	☐	☐
2.6	Have members of management taken cybersecurity training in the last two years?	☐	☐	☐	☐	☐	☐
2.7	Does management discuss cybersecurity at least once a quarter?	☐	☐	☐	☐	☐	☐
2.8	Are management's cybersecurity decisions documented?	☐	☐	☐	☐	☐	☐

Score, area 02 **Total** _____ **Answered** _____ **%** _____

0 No · **1** Starting · **2** Partly · **3** Nearly there · **4** Fully in place · **N/A** Not applicable

03 Risk management and policies

NIS2: (a) · ISO 27001:2022: Cl. 6.1, 8.2 · A.5.1, A.5.37

№	Question	0	1	2	3	4	N/A
3.1	Is there an approved information security policy?	☐	☐	☐	☐	☐	⬚
3.2	Has a cyber risk assessment been carried out in the last 12 months?	☐	☐	☐	☐	☐	⬚
3.3	Is there a risk register with an owner and a deadline for each risk?	☐	☐	☐	☐	☐	⬚
3.4	Is there a plan to reduce the main risks?	☐	☐	☐	☐	☐	⬚
3.5	Are the policies reviewed at least once a year?	☐	☐	☐	☐	☐	⬚
3.6	Have staff acknowledged the policies in writing?	☐	☐	☐	☐	☐	⬚
3.7	Are the key security procedures documented?	☐	☐	☐	☐	☐	⬚
3.8	Are risks reassessed whenever systems change significantly?	☐	☐	☐	☐	☐	⬚

Score, area 03 **Total** _____ **Answered** _____ **%** _____

0 No · **1** Starting · **2** Partly · **3** Nearly there · **4** Fully in place · **N/A** Not applicable

04 Assets and inventory

NIS2: (i) · ISO 27001:2022: A.5.9, A.5.10, A.5.12, A.8.9

№	Question	0	1	2	3	4	N/A
4.1	Is there a complete, up-to-date list of computers, servers and network devices?	☐	☐	☐	☐	☐	☐
4.2	Is there a list of the software and cloud services in use?	☐	☐	☐	☐	☐	☐
4.3	Does every asset have a named owner?	☐	☐	☐	☐	☐	☐
4.4	Is data classified by how important it is?	☐	☐	☐	☐	☐	☐
4.5	Do you know where your critical data is stored?	☐	☐	☐	☐	☐	☐
4.6	Are there rules for the acceptable use of company devices?	☐	☐	☐	☐	☐	☐
4.7	Are standard secure configurations for devices documented?	☐	☐	☐	☐	☐	☐

Score, area 04 **Total** _____ **Answered** _____ **%** _____

0 No · **1** Starting · **2** Partly · **3** Nearly there · **4** Fully in place · **N/A** Not applicable

05 Access control and MFA

NIS2: (i) (j) · ISO 27001:2022: A.5.15–5.18, A.8.2, A.8.5

№	Question	0	1	2	3	4	N/A
5.1	Does every user have their own account, with no shared accounts?	☐	☐	☐	☐	☐	☐
5.2	Are permissions granted on the principle of least privilege?	☐	☐	☐	☐	☐	☐
5.3	Is there a procedure for granting, changing and removing access?	☐	☐	☐	☐	☐	☐
5.4	Is access for leavers removed on their last working day?	☐	☐	☐	☐	☐	☐
5.5	Are access rights reviewed at least every six months?	☐	☐	☐	☐	☐	☐
5.6	Is MFA enabled for email and cloud services?	☐	☐	☐	☐	☐	☐
5.7	Is MFA enabled for VPN and remote access?	☐	☐	☐	☐	☐	☐
5.8	Do administrators use separate privileged accounts?	☐	☐	☐	☐	☐	☐
5.9	Is there a strong-password policy or a password manager?	☐	☐	☐	☐	☐	☐
5.10	Are phishing-resistant MFA methods in use?	☐	☐	☐	☐	☐	☐

Score, area 05 **Total** _____ **Answered** _____ **%** _____

0 No · **1** Starting · **2** Partly · **3** Nearly there · **4** Fully in place · **N/A** Not applicable

06 Network security

NIS2: (e) (i) · ISO 27001:2022: A.8.20–8.23

№	Question	0	1	2	3	4	N/A
6.1	Is the network protected by a next-generation firewall (NGFW)?	☐	☐	☐	☐	☐	☐
6.2	Are the NGFW's security subscriptions active (IPS, antivirus, web filtering)?	☐	☐	☐	☐	☐	☐
6.3	Is the network divided into segments (office, servers, guests, IoT)?	☐	☐	☐	☐	☐	☐
6.4	Is the guest network kept separate from the corporate network?	☐	☐	☐	☐	☐	☐
6.5	Is remote access possible only through a VPN?	☐	☐	☐	☐	☐	☐
6.6	Are management interfaces and RDP closed to the internet?	☐	☐	☐	☐	☐	☐
6.7	Is WPA2/WPA3-Enterprise used for the corporate wireless network?	☐	☐	☐	☐	☐	☐
6.8	Are the firewall rules reviewed at least once a year?	☐	☐	☐	☐	☐	☐
6.9	Are dangerous websites and DNS requests filtered?	☐	☐	☐	☐	☐	☐
6.10	Have default passwords been changed on all network devices?	☐	☐	☐	☐	☐	☐

Score, area 06 **Total** _____ **Answered** _____ **%** _____

0 No · **1** Starting · **2** Partly · **3** Nearly there · **4** Fully in place · **N/A** Not applicable

07 Endpoints and email

NIS2: (b) (e) (h) · ISO 27001:2022: A.6.7, A.8.1, A.8.7, A.8.19

№	Question	0	1	2	3	4	N/A
7.1	Is EDR protection installed on all computers?	☐	☐	☐	☐	☐	☐
7.2	Is EDR protection installed on all servers?	☐	☐	☐	☐	☐	☐
7.3	Are mobile devices managed centrally (MDM)?	☐	☐	☐	☐	☐	☐
7.4	Are laptop disks encrypted?	☐	☐	☐	☐	☐	☐
7.5	Is software installation by users restricted?	☐	☐	☐	☐	☐	☐
7.6	Is there filtering against phishing and malicious attachments?	☐	☐	☐	☐	☐	☐
7.7	Are SPF, DKIM and DMARC set up for your domain?	☐	☐	☐	☐	☐	☐
7.8	Are there rules for remote working and personal devices?	☐	☐	☐	☐	☐	☐

Score, area 07 **Total** _____ **Answered** _____ **%** _____

08 Monitoring, logging and SIEM

NIS2: (b) (f) · ISO 27001:2022: A.8.15–8.17

№	Question	0	1	2	3	4	N/A
8.1	Are the availability and health of servers and the network monitored?	☐	☐	☐	☐	☐	☐
8.2	Are there automatic alerts when something fails?	☐	☐	☐	☐	☐	☐
8.3	Are logs from the firewall, servers and cloud services collected in one place?	☐	☐	☐	☐	☐	☐
8.4	Are logs protected against alteration and deletion?	☐	☐	☐	☐	☐	☐
8.5	Is there a defined retention period for logs?	☐	☐	☐	☐	☐	☐
8.6	Is a SIEM used to analyse and correlate events?	☐	☐	☐	☐	☐	☐
8.7	Is time synchronised across all systems (NTP)?	☐	☐	☐	☐	☐	☐
8.8	Is there a named person or service that responds to alerts?	☐	☐	☐	☐	☐	☐
8.9	Does monitoring also run outside working hours?	☐	☐	☐	☐	☐	☐
8.10	Are failed logins and suspicious activity reviewed regularly?	☐	☐	☐	☐	☐	☐

Score, area 08 **Total** _____ **Answered** _____ **%** _____

09 Incidents and reporting

NIS2: (b) · Art. 23 · ISO 27001:2022: A.5.24–5.28, A.6.8

№	Question	0	1	2	3	4	N/A
9.1	Is there a written incident response plan?	☐	☐	☐	☐	☐	☐
9.2	Are incident roles and deputies defined?	☐	☐	☐	☐	☐	☐
9.3	Are there criteria for when an incident is significant?	☐	☐	☐	☐	☐	☐
9.4	Do you know which CSIRT you report to (in Bulgaria, the sectoral SERIKS team)?	☐	☐	☐	☐	☐	☐
9.5	Are templates ready for the 24-hour and 72-hour notifications?	☐	☐	☐	☐	☐	☐
9.6	Do staff know how and to whom to report a suspicious event?	☐	☐	☐	☐	☐	☐
9.7	Is there a procedure for preserving evidence?	☐	☐	☐	☐	☐	☐
9.8	Is there a process for notifying the data protection authority when personal data is affected?	☐	☐	☐	☐	☐	☐
9.9	Has the incident plan been tested in the last 12 months?	☐	☐	☐	☐	☐	☐
9.10	Are incidents reviewed after they are closed?	☐	☐	☐	☐	☐	☐

Score, area 09 **Total** _____ **Answered** _____ **%** _____

0 No · **1** Starting · **2** Partly · **3** Nearly there · **4** Fully in place · **N/A** Not applicable

10 Continuity and backups

NIS2: (c) · ISO 27001:2022: A.5.29, A.5.30, A.8.13, A.8.14

№	Question	0	1	2	3	4	N/A
10.1	Are all critical data and systems backed up automatically?	☐	☐	☐	☐	☐	☐
10.2	Is there a copy outside the office or outside the main cloud?	☐	☐	☐	☐	☐	☐
10.3	Is there an immutable or offline copy?	☐	☐	☐	☐	☐	☐
10.4	Is access to the backup system protected with MFA?	☐	☐	☐	☐	☐	☐
10.5	Are restores tested at least once a quarter?	☐	☐	☐	☐	☐	☐
10.6	Are RTO and RPO defined for critical systems?	☐	☐	☐	☐	☐	☐
10.7	Is there a business continuity plan?	☐	☐	☐	☐	☐	☐
10.8	Is there a crisis management and communication plan?	☐	☐	☐	☐	☐	☐
10.9	Are critical components redundant (internet, power, key servers)?	☐	☐	☐	☐	☐	☐

Score, area 10 **Total** _____ **Answered** _____ **%** _____

0 No · **1** Starting · **2** Partly · **3** Nearly there · **4** Fully in place · **N/A** Not applicable

11 Vulnerabilities and updates

NIS2: (e) · ISO 27001:2022: A.8.8, A.8.25, A.8.32

№	Question	0	1	2	3	4	N/A
11.1	Are critical operating system updates installed within days?	☐	☐	☐	☐	☐	⬚
11.2	Are applications kept up to date (browsers, office suites, PDF readers)?	☐	☐	☐	☐	☐	⬚
11.3	Is firmware updated on the firewall, VPN and network devices?	☐	☐	☐	☐	☐	⬚
11.4	Is there regular vulnerability scanning?	☐	☐	☐	☐	☐	⬚
11.5	Do you follow vulnerability bulletins for the products you use?	☐	☐	☐	☐	☐	⬚
11.6	Is there a change management procedure?	☐	☐	☐	☐	☐	⬚
11.7	Have systems no longer supported by the vendor been replaced?	☐	☐	☐	☐	☐	⬚
11.8	Is security checked when buying or developing new software?	☐	☐	☐	☐	☐	⬚

Score, area 11 **Total** _____ **Answered** _____ **%** _____

0 No · **1** Starting · **2** Partly · **3** Nearly there · **4** Fully in place · **N/A** Not applicable

12 Cryptography

NIS2: (h) · ISO 27001:2022: A.8.24

№	Question	0	1	2	3	4	N/A
12.1	Is there a policy on the use of encryption?	☐	☐	☐	☐	☐	⬚
12.2	Is data encrypted in transit (TLS, VPN)?	☐	☐	☐	☐	☐	⬚
12.3	Is sensitive data encrypted at rest?	☐	☐	☐	☐	☐	⬚
12.4	Are keys and certificates managed and protected?	☐	☐	☐	☐	☐	⬚
12.5	Is SSL/TLS certificate expiry monitored?	☐	☐	☐	☐	☐	⬚

Score, area 12 **Total** _____ **Answered** _____ **%** _____

0 No · **1** Starting · **2** Partly · **3** Nearly there · **4** Fully in place · **N/A** Not applicable

13 Suppliers

NIS2: (d) · ISO 27001:2022: A.5.19–5.23

№	Question	0	1	2	3	4	N/A
13.1	Is there a list of suppliers with access to your systems or data?	☐	☐	☐	☐	☐	⬚
13.2	Has the risk from key suppliers been assessed?	☐	☐	☐	☐	☐	⬚
13.3	Do contracts include security requirements?	☐	☐	☐	☐	☐	⬚
13.4	Do contracts require suppliers to notify you of incidents?	☐	☐	☐	☐	☐	⬚
13.5	Is suppliers' remote access restricted and monitored?	☐	☐	☐	☐	☐	⬚
13.6	Is supplier compliance with the requirements checked periodically?	☐	☐	☐	☐	☐	⬚
13.7	Has the security of the cloud services you use been assessed?	☐	☐	☐	☐	☐	⬚

Score, area 13 **Total** _____ **Answered** _____ **%** _____

14 People, training and cyber hygiene

NIS2: (g) (i) · ISO 27001:2022: A.6.1–6.6

№	Question	0	1	2	3	4	N/A
14.1	Do all staff receive cybersecurity training when they join?	☐	☐	☐	☐	☐	☐
14.2	Is there refresher training at least once a year?	☐	☐	☐	☐	☐	☐
14.3	Are phishing simulation campaigns run?	☐	☐	☐	☐	☐	☐
14.4	Do employment contracts include confidentiality obligations?	☐	☐	☐	☐	☐	☐
14.5	Are candidates for key positions screened?	☐	☐	☐	☐	☐	☐
14.6	Is there a leaver procedure (returning equipment, removing access)?	☐	☐	☐	☐	☐	☐
14.7	Do staff follow the basic rules: locked screens, strong passwords, caution with suspicious emails?	☐	☐	☐	☐	☐	☐

Score, area 14 **Total** _____ **Answered** _____ **%** _____

0 No · **1** Starting · **2** Partly · **3** Nearly there · **4** Fully in place · **N/A** Not applicable

15 Checking effectiveness

NIS2: (f) · ISO 27001:2022: Cl. 9.1–9.3 · A.5.35

№	Question	0	1	2	3	4	N/A
15.1	Do you track security metrics (number of incidents, time to patch, etc.)?	☐	☐	☐	☐	☐	☐
15.2	Are internal security audits carried out?	☐	☐	☐	☐	☐	☐
15.3	Has there been an external audit or penetration test in the last two years?	☐	☐	☐	☐	☐	☐
15.4	Are identified gaps tracked until they are fixed?	☐	☐	☐	☐	☐	☐
15.5	Does management review the results at least once a year?	☐	☐	☐	☐	☐	☐

Score, area 15 **Total** _____ **Answered** _____ **%** _____

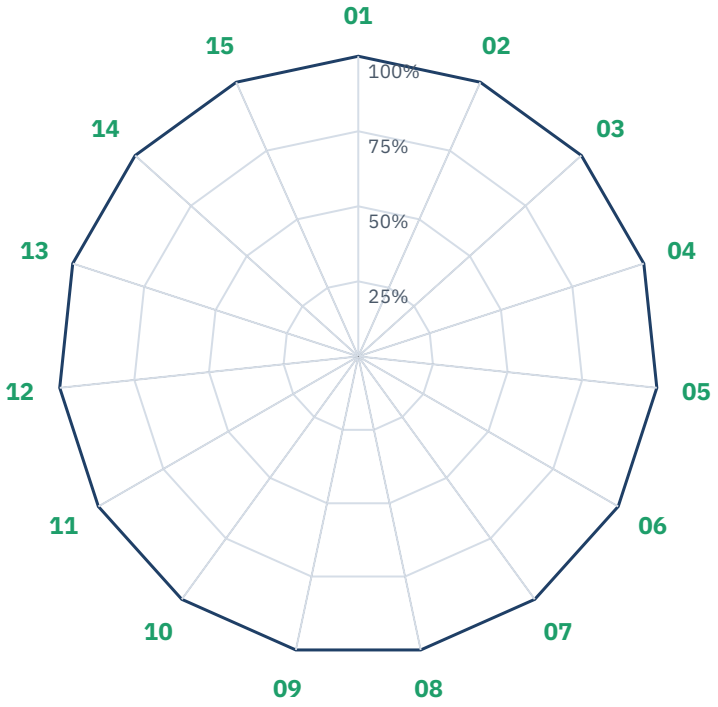
Score summary

№	Area	Total	Max.	%
01	Scope and registration			
02	Management and accountability			
03	Risk management and policies			
04	Assets and inventory			
05	Access control and MFA			
06	Network security			
07	Endpoints and email			
08	Monitoring, logging and SIEM			
09	Incidents and reporting			
10	Continuity and backups			
11	Vulnerabilities and updates			
12	Cryptography			
13	Suppliers			
14	People, training and cyber hygiene			
15	Checking effectiveness			
	Overall			

How to calculate: Max. = 4 × the number of answered questions (excluding N/A). % = Total ÷ Max. × 100. Work out the overall score from the overall totals, not as an average of the percentages.

Readiness radar

Mark each area's percentage on its axis and join the points. The dips show your weak spots.



01 Scope and registration
02 Management and accountability
03 Risk management and policies
04 Assets and inventory
05 Access control and MFA
06 Network security
07 Endpoints and email
08 Monitoring, logging and SIEM
09 Incidents and reporting
10 Continuity and backups
11 Vulnerabilities and updates
12 Cryptography
13 Suppliers
14 People, training and cyber hygiene
15 Checking effectiveness

How to read your score

Below 40% · Serious gaps

The basics are missing. You need a plan with clear priorities and a budget; start with the lowest-scoring areas.

40–69% · In progress

There is a good foundation, but also gaps. Close the gaps in your weakest areas and document what you have done.

70% and above · Good readiness

Most measures are working. Focus on evidence, regular checks and continuous improvement.

A PRIORITY WHATEVER YOUR OVERALL SCORE

If area 05 (Access control and MFA), 09 (Incidents and reporting) or 10 (Backups) is below 50%, start there. These areas decide whether an attack is a nuisance or a crisis.

This self-assessment is a guide and does not replace an audit or legal advice. It shows where to focus your efforts first.

Notes

Velox | Secure IT infrastructure

The next step

The self-assessment shows where you are. We help you get to where you need to be. Velox is ISO 27001 certified and applies the same requirements in its own work.

Results review
We go through your completed questionnaire and agree on priorities.

Readiness assessment
An on-site review and a detailed list of gaps.

Technical measures
NGFW, SIEM, system monitoring, MFA, backups.

Subscription support
Ongoing care for your systems, updates and monitoring.

GET IN TOUCH

www.velox-systems.com

office@velox-systems.com

NIS2 SERIES

Short, practical booklets for leaders who want to understand NIS2 and act on it.

1 · NIS2 · introduction

2 · Self-assessment questionnaire

3 · Implementation guide

4 · Incident response

Velox | Secure IT infrastructure

www.velox-systems.com
office@velox-systems.com

© 2026 Velox Ltd. For information only; not legal advice.