Example Advisory SAMPLE

Cybersecurity assessment report

Kymora Logistics

Prepared for	Kymora Logistics
Prepared by	Example Advisory
Date	2 November 2026
Classification	Confidential

Contents

1. Executive summary 3

2. Scope and method 4

3. Compliance with Law 5160/2024 5

4. Maturity 8

5. Technical exposure 9

6. Internal network 11

7. Governance 12

8. Risk in money 13

9. Roadmap 14

10. Limitations 18

11. Sign-off 19

1. Executive summary

Attack paths to fix first

- **Account takeover path** (critical together, from findings rated high). 1 exposed credential on example.com, and a VPN endpoint at vpn.example.com. The Microsoft 365 tenant does not enforce a second factor. The surface is a remote access service, so a working credential is a session on the host.

The EAK gap analysis stands at 49.4% compliance, rated High risk by the authority's method.

The maturity assessment against NIS2 Article 21(2) averages 2.1 out of 5, with a target of 3.

The internet-facing exposure score is 4.1 out of 10 (Low). Live findings: 0 critical and 2 high.

Policies KYA 1689/2025 asks for that are approved and within their review date: 6 of 12.

The quantified risk register estimates an expected loss of €183,900 a year.

The roadmap lists 39 actions, 12 of them high priority.

Of the 143 EAK gaps, the roadmap holds the 15 largest. The rest are in the gap analysis workbook.

2. Scope and method

No ISMS scope statement is recorded.

Domains in scope: example.com, example.net.

Method

- The EAK gap analysis, answered by the organisation with its adviser and scored by the authority's documented method.
- A maturity assessment against NIS2 Article 21(2), each item answered on a scale of 0 to 5.
- Automated monitoring of the internet-facing estate by Vardion, on addresses the organisation approved.
- The internal network, read from host inventory, configuration checks and any internal sweep, scored on its own scale.
- The organisation's ISMS records: the policy index, the security officer, the programme and the risk register.

3. Compliance with Law 5160/2024

EAK gap analysis: 169 of 169 controls answered. Important entity.

COMPLIANCE	RISK BAND
49.4%	**High risk**

SECTION	COMPLIANCE	RISK BAND
1. Υποχρεώσεις & Ευθύνη των Ανωτάτων Οργάνων Διοίκησης	50.0%	High risk
2. Πλαίσιο Διαχείρισης Κινδύνων	38.2%	High risk
3. Πολιτικές και Διαδικασίες Ασφάλειας Πληροφοριών	60.7%	Medium risk
4. Ρόλοι, Αρμοδιότητες και Εξουσίες	64.5%	Medium risk
5. Ανεξάρτητος Έλεγχος Ασφάλειας Πληροφοριών	12.5%	Critical risk
6. Διαδικασίες Παρακολούθησης της Συμμόρφωσης	42.9%	High risk
7. Ασφάλεια Ανθρώπινου Δυναμικού	56.7%	Medium risk
8. Διαχείριση Υλικού και Λογισμικού	56.3%	Medium risk
9. Διαχείριση Ασφάλειας Αλυσίδας Εφοδιασμού	47.7%	High risk
10. Διαχείριση Ταυτότητας, Αυθεντικοποίηση και Έλεγχος Πρόσβασης	70.5%	Medium risk
11. Ασφαλής Παραμετροποίηση Υλικού, Λογισμικού, Υπηρεσιών και Δικτύων	60.9%	Medium risk
12. Αρχές Ασφαλούς Ανάπτυξης Εφαρμογών	48.9%	High risk
13. Διαχείριση Αλλαγών	32.4%	High risk
14. Διαχείριση και Γνωστοποίηση Ευπαθειών	51.3%	Medium risk
15. Αξιολόγηση της Αποτελεσματικότητας των Μέτρων Διαχείρισης Κινδύνων Κυβερνοασφάλειας	37.5%	High risk
16. Ασφάλεια Δικτύων, Υποδομών και Υπηρεσιών Νέφους	40.8%	High risk
17. Προστασία από Κακόβουλο Λογισμικό	68.8%	Medium risk
18. Εκπαίδευση και Ευαισθητοποίηση σε Θέματα Κυβερνοασφάλειας	50.0%	High risk
19. Χρήση Κρυπτογραφίας	42.4%	High risk
20. Φυσική & Περιβαλλοντική Ασφάλεια	57.6%	Medium risk
21. Διαχείριση Περιστατικών Ασφάλειας & Υποχρεώσεις Αναφοράς	39.9%	High risk
22. Ασφάλεια Τεχνητής Νοημοσύνης (AI Security)	Not applicable	
23. Ασφάλεια Λειτουργικής Τεχνολογίας, Διαδικτύου των Πραγμάτων και Ιατρικών Συσκευών (OT, IoT, IoMT Security)	31.3%	High risk

SECTION	COMPLIANCE	RISK BAND
24. Επιχειρησιακή Συνέχεια και Διαχείριση Κρίσεων	61.4%	Medium risk

Largest gaps

CONTROL	IMPLEMENTATION	POINTS SHORT
5.3 Εφόσον από τα αποτελέσματα του ανεξάρτητου ελέγχου προκύψει ανεπαρκής υλοποίηση των απαραίτητων τεχνικών, οργανωτικών και επιχειρησιακών μέτρων κυβερνοασφάλειας, το ανώτατο όργανο διοίκησης της οντότητας εκκινεί διαδικασίες διορθωτικών ενεργειών.	Not started	5.00
5.4 Οι ανεξάρτητοι έλεγχοι διενεργούνται σε προγραμματισμένα χρονικά διαστήματα, καθώς και όταν λαμβάνουν χώρα σοβαρά περιστατικά κυβερνοασφάλειας ή σημαντικές αλλαγές στις λειτουργίες της οντότητας ή εφόσον έχει μεταβληθεί το τρέχον διεθνές περιβάλλον κυβερνοαπειλών.	Not started	5.00
15.3 Η οντότητα υλοποιεί διαδικασίες αποκατάστασης των ελλείψεων που διαπιστώνονται στους εξωτερικούς ελέγχους παρείσδυσης, καθώς και διαδικασίες επικύρωσης των διορθωτικών μέτρων, με βάση συγκεκριμένο πλάνο προτεραιοποίησης, λαμβάνοντας υπόψη την κρισιμότητα των ευρημάτων.	Not started	5.00
21.11 Η οντότητα διασφαλίζει τακτικά (προτείνεται ετησίως) ότι στην υπηρεσία SOC περιλαμβάνονται το σύνολο των συστημάτων και των υποδομών.	Not started	5.00
23.4 Η οντότητα χρησιμοποιεί τεχνολογίες παρακολούθησης για την ανίχνευση ανωμαλιών, απειλών και επιθέσεων στις εξειδικευμένες υποδομές της.	Not started	5.00
24.5 Η οντότητα έχει υλοποιήσει εναλλακτικό τοποθεσία (Disaster Recovery Site) για όλες τις κρίσιμες υποδομές, λαμβάνοντας υπόψη τα αποτελέσματα της Ανάλυσης Επιχειρηματικών Επιπτώσεων (Business Impact Analysis - BIA). Η επιλογή των συστημάτων που υποστηρίζονται στο DR Site βασίζεται σε προκαθορισμένους δείκτες: Στόχο Σημείου Ανάκαμψης (Recovery Point Objective - RPO), Χρόνο Ανάκτησης (Recovery Time Objective - RTO) και Μέγιστο Ανεκτό Διάστημα Διακοπής (Maximum Tolerable Period of Disruption - MTPD) διασφαλίζοντας τη συνέχεια κρίσιμων επιχειρησιακών λειτουργιών σε περίπτωση σοβαρής διακοπής ή καταστροφής.	Not started	5.00
8.6 Η οντότητα εφαρμόζει ετικετοποίηση (labeling) όλων των αγαθών (υλικού και πληροφοριών), σύμφωνα με το σχήμα ταξινόμησης (classification scheme, π.χ., Δημόσια, Εσωτερικά, Εμπιστευτικά) των αγαθών και των δεδομένων.	Not started	4.00
13.4 Οι διαδικασίες διαχείρισης αλλαγών αξιολογούνται και επικαιροποιούνται σε περιοδική βάση (προτείνεται ετησίως), καθώς και όταν λαμβάνουν χώρα σοβαρά περιστατικά κυβερνοασφάλειας ή σημαντικές αλλαγές στις λειτουργίες της οντότητας.	Not started	4.00
16.1.10 Η οντότητα εφαρμόζει φιλτράρισμα της δικτυακής κίνησης μεταξύ των διακριτών υποδικτύων, με βάση τις απαιτήσεις ασφάλειας κάθε ζώνης.	Not started	4.00

CONTROL	IMPLEMENTATION	POINTS SHORT
16.1.12 Οι πολιτικές και διαδικασίες που αφορούν στην ασφάλεια δικτύων αξιολογούνται και, κατά περίπτωση, επικαιροποιούνται τακτικά σε προγραμματισμένα χρονικά διαστήματα (προτείνεται σε ετήσια βάση), καθώς και όταν λαμβάνουν χώρα σοβαρά περιστατικά κυβερνοασφάλειας ή σημαντικές αλλαγές στις λειτουργίες της οντότητας ή εφόσον έχει μεταβληθεί το τρέχον διεθνές περιβάλλον κυβερνοαπειλών.	Not started	4.00

Vardion calculates this score from your answers using the authority's published method. It is not the authority's determination or legal advice.

Πηγή: Εθνική Αρχή Κυβερνοασφάλειας, Υπόδειγμα εργαλείου gap analysis για τη συμμόρφωση με τον ν. 5160/2024 (Οδηγία NIS2), Σεπτέμβριος 2025, cyber.gov.gr, άδεια CC BY-ND 4.0.

4. Maturity

NIS2 measures, assessed against NIS2 Article 21(2) with a target of level 3.

DOMAIN	SCORE	TARGET	ANSWERED
Article 21(2)	2.1	3.0	10/10

Largest gaps

ITEM	LEVEL	TARGET
21.2.c Business continuity, such as backup management and disaster recovery, and crisis management	1	3
21.2.g Basic cyber hygiene practices and cybersecurity training	1	3
21.2.a Policies on risk analysis and information system security	2	3
21.2.d Supply chain security, including security-related aspects concerning the relationships between each entity and its direct suppliers or service providers	2	3
21.2.f Policies and procedures to assess the effectiveness of cybersecurity risk-management measures	2	3
21.2.h Policies and procedures regarding the use of cryptography and, where appropriate, encryption	2	3
21.2.j The use of multi-factor authentication or continuous authentication solutions, secured voice, video and text communications and secured emergency communication systems within the entity, where appropriate	2	3

5. Technical exposure

From the last full scan on 2 November 2026 and the checks run since.

EXPOSURE SCORE	CRITICAL	HIGH	MEDIUM
4.1 Low	0	2	2

LOW	INFO
3	3

Account takeover path: rated critical as a whole, because its findings give a way in only together. Each is listed below at its own severity.

Posture by area

EXPOSED SERVICES	PATCHING	ENCRYPTION	WEB CONFIGURATION
A	A	C	B

EMAIL	DOMAINS AND DNS	CREDENTIALS
A	C	D

Each area is graded by the risk of its open findings: A nothing open, B low, C medium, D high and F critical.

Changes that reduce the risk most

ACTION	WHERE	SEVERITY	FINDINGS
Reset the credentials on the account named in the finding, revoke its active sessions and confirm multi-factor authentication is enforced on the sign-in surface it names.	vpn.example.com (the details are in the console, under finding F-33FE27B430)	High	1
Turn on security defaults, or create a conditional access policy that requires multifactor authentication for all users.	Microsoft 365 tenant example.com	High	1
Reset the password on the account named in the finding and revoke its active sessions.	example.com (the details are in the console, under finding F-258E45A9D5)	Medium	1
Reissue the certificate to cover the hostnames served on this address, or serve the matching certificate for each name.	203.0.113.13	Medium	1
Remove the product version from the Server, X-Powered-By and X-AspNet-Version response headers.	203.0.113.10, 203.0.113.11	Low	2
Publish a CAA record naming the certificate authorities permitted to issue for the domain.	example.com	Low	1

ACTION	WHERE	SEVERITY	FINDINGS
Add the security response headers the finding lists to this service's responses.	203.0.113.10, 203.0.113.11	Info	2
Restrict this administrative interface to the addresses that need it, or place it behind the VPN.	vpn.example.com	Info	1

6. Internal network

This covers the internal network, from the internal sweep of 12 October 2026, ranked as the internet-facing findings are and never summed with them.

EXPOSURE SCORE	CRITICAL	HIGH	MEDIUM
0.9 Low	**0**	**0**	**2**

LOW	INFO
0	**0**

Changes that reduce the risk most

ACTION	WHERE	SEVERITY	FINDINGS
Restrict 3389/tcp to the hosts that need it, with a firewall rule or a separate network segment.	192.168.10.31	Medium	1
Restrict 445/tcp to the hosts that need it, with a firewall rule or a separate network segment.	192.168.10.20	Medium	1

7. Governance

Policies KYA 1689/2025 asks for that are held in the policy index and current: 6 of 12. The rest are listed below with where each stands.

POLICY	STATE
Acceptable use policy	Review overdue
Removable media policy	Missing
Supply chain security policy	Missing
Security testing policy	Missing
Cryptography policy	Missing
Physical and environmental security policy	Missing

The security officer is Nikos Example, reporting to Managing director.

The last management review was held on 9 August 2026.

These programme duties are overdue or have never been done.

- Security awareness campaign
- Privileged access review
- Critical supplier review

8. Risk in money

EXPECTED LOSS A YEAR	ONE YEAR IN 10
€183,900	**€693,000**

1. Ransomware stops dispatch €153,800 a year
2. Customer data stolen from the portal €30,100 a year

An estimate simulated from ranges entered by officer, last changed on 8 September 2026. It is a judgement, not a measurement.

9. Roadmap

An action keeps the priority you set. Otherwise it comes from the source: severity for a technical change, missing points for an EAK control, missing levels for a maturity item.

An action with no owner falls to the security officer. One with no date is due by the deadline of the findings it closes, or else within 30 days at high priority, 90 at medium and 180 at low. A date already past shows as the report's date, with the date it was due.

Of the 143 EAK gaps, the roadmap holds the 15 largest. The rest are in the gap analysis workbook.

#	ACTION	SOURCE	PRIORITY	OWNER	DUE
1	Close the gap in EAK control 21.11: Η οντότητα διασφαλίζει τακτικά (προτείνεται ετησίως) ότι στην υπηρεσία SOC περιλαμβάνονται το σύνολο των συστημάτων και των υποδομών.	EAK 21.11	High	Security officer	1 January 2027
2	Complete and test the continuity plan, and keep tested backups of the critical systems.	EAK 24.5	High	IT manager	2 December 2026
3	Write the change management procedure and have it approved.	EAK 13.4	High	IT manager	17 December 2026
4	Close the gap in EAK control 21.9: Η οντότητα διασφαλίζει την αποτελεσματική λειτουργία του Κέντρου Επιχειρήσεων Ασφαλείας (SOC) μέσω της αξιοποίησης σύγχρονων Συστημάτων Διαχείρισης Πληροφοριών και Συμβάντων Ασφαλείας (SIEM), Ορχήστρωσης και Αυτοματοποιημένης Απόκρισης (SOAR) ή/και Εκτεταμένης Ανίχνευσης και Απόκρισης (XDR), με στόχο την αυτοματοποίηση διαδικασιών και την ταχεία απόκριση σε περιστατικά ασφαλείας σε πραγματικό χρόνο.	EAK 21.9	High	Security officer	1 January 2027
5	Schedule cybersecurity training for the management body and briefings for all staff.	EAK 1.6	High	Managing director	1 January 2027
6	Write the risk treatment plan and have the managing director approve it.	EAK 2.3	High	Security officer	17 December 2026
7	Raise 21.2.c Business continuity, such as backup management and disaster recovery, and crisis management to level 3	Maturity	High	Security officer	2 December 2026
8	Raise 21.2.g Basic cyber hygiene practices and cybersecurity training to level 3	Maturity	High	Security officer	2 December 2026

#	ACTION	SOURCE	PRIORITY	OWNER	DUE
9	Reset the credentials on the account named in the finding, revoke its active sessions and confirm multi-factor authentication is enforced on the sign-in surface it names. Where: vpn.example.com (the details are in the console, under finding F-33FE27B430)	Technical	High	Security officer	26 November 2026
10	Turn on security defaults, or create a conditional access policy that requires multifactor authentication for all users. Where: Microsoft 365 tenant example.com	Technical	High	IT manager	27 November 2026
11	Catch up on the overdue duty: Security awareness campaign Overdue since 4 October 2026	Programme	High	HR	2 November 2026
12	Catch up on the overdue duty: Privileged access review Overdue since 24 October 2026	Programme	High	IT manager	2 November 2026
13	Appoint an independent auditor and set the audit schedule.	EAK 5.3, 5.4, 5.1	Medium	Managing director	31 January 2027
14	Schedule the yearly security test and the yearly self-assessment.	EAK 15.3	Medium	Security officer	1 January 2027
15	List the warehouse scanners and cameras, put them on a network of their own and watch it.	EAK 23.4	Medium	IT manager	2 March 2027
16	Label the assets in the register and monitor the capacity of the critical systems.	EAK 8.6	Medium	IT manager	2 March 2027
17	Close the gap in EAK control 16.1.10: Η οντότητα εφαρμόζει φιλτράρισμα της δικτυακής κίνησης μεταξύ των διακριτών υποδικτύων, με βάση τις απαιτήσεις ασφάλειας κάθε ζώνης.	EAK 16.1.10	Medium	IT manager	31 January 2027
18	Close the gap in EAK control 16.1.12: Οι πολιτικές και διαδικασίες που αφορούν στην ασφάλεια δικτύων αξιολογούνται και, κατά περίπτωση, επικαιροποιούνται τακτικά σε προγραμματισμένα χρονικά διαστήματα (προτείνεται σε ετήσια βάση), καθώς και όταν λαμβάνουν χώρα σοβαρά περιστατικά κυβερνοασφάλειας ή σημαντικές αλλαγές στις λειτουργίες της οντότητας ή εφόσον έχει μεταβληθεί το τρέχον διεθνές περιβάλλον κυβερνοαπειλών.	EAK 16.1.12	Medium	IT manager	31 January 2027
19	Encrypt the critical data and review the cryptography procedure.	EAK 19.5	Medium	IT manager	2 March 2027
20	Raise 21.2.a Policies on risk analysis and information system security to level 3	Maturity	Medium	Security officer	31 January 2027
21	Raise 21.2.d Supply chain security, including security-related aspects concerning the relationships between each entity and its direct suppliers or service providers to level 3	Maturity	Medium	Security officer	31 January 2027

#	ACTION	SOURCE	PRIORITY	OWNER	DUE
22	Raise 21.2.f Policies and procedures to assess the effectiveness of cybersecurity risk-management measures to level 3	Maturity	Medium	Security officer	31 January 2027
23	Raise 21.2.h Policies and procedures regarding the use of cryptography and, where appropriate, encryption to level 3	Maturity	Medium	Security officer	31 January 2027
24	Raise 21.2.j The use of multi-factor authentication or continuous authentication solutions, secured voice, video and text communications and secured emergency communication systems within the entity, where appropriate to level 3	Maturity	Medium	Security officer	31 January 2027
25	Reset the password on the account named in the finding and revoke its active sessions. Where: example.com (the details are in the console, under finding F-258E45A9D5)	Technical	Medium	Security officer	28 December 2026
26	Reissue the certificate to cover the hostnames served on this address, or serve the matching certificate for each name. Where: 203.0.113.13	Technical	Medium	IT manager	3 January 2027
27	Restrict 3389/tcp to the hosts that need it, with a firewall rule or a separate network segment. Where: 192.168.10.31	Internal network	Medium	Security officer	10 January 2027
28	Restrict 445/tcp to the hosts that need it, with a firewall rule or a separate network segment. Where: 192.168.10.20	Internal network	Medium	Security officer	10 January 2027
29	Review and reapprove: Acceptable use policy	Policy	Medium	Security officer	31 January 2027
30	Adopt and approve: Removable media policy	Policy	Medium	Security officer	31 January 2027
31	Adopt and approve: Supply chain security policy	Policy	Medium	Security officer	31 January 2027
32	Adopt and approve: Security testing policy	Policy	Medium	Security officer	31 January 2027
33	Adopt and approve: Cryptography policy	Policy	Medium	Security officer	31 January 2027
34	Adopt and approve: Physical and environmental security policy	Policy	Medium	Security officer	31 January 2027
35	Carry out for the first time: Critical supplier review	Programme	Medium	Security officer	31 January 2027
36	Remove the product version from the Server, X-Powered-By and X-AspNet-Version response headers. Where: 203.0.113.10, 203.0.113.11	Technical	Low	Web contractor	13 February 2027

#	ACTION	SOURCE	PRIORITY	OWNER	DUE
37	Publish a CAA record naming the certificate authorities permitted to issue for the domain. Where: example.com	Technical	Low	Security officer	31 January 2027
38	Add the security response headers the finding lists to this service's responses. Where: 203.0.113.10, 203.0.113.11	Technical	Low	Web contractor	1 May 2027
39	Restrict this administrative interface to the addresses that need it, or place it behind the VPN. Where: vpn.example.com	Technical	Low	IT manager	1 May 2027

10. Limitations

- The EAK and maturity answers are the organisation's own, recorded with its adviser. They are not independently verified.
- This report is an assessment. It is not a certification or an audit opinion.

11. Sign-off

Signed by those who prepared, reviewed and accepted this report.

ROLE	NAME	SIGNATURE	DATE
Prepared by			
Reviewed by			
Accepted by			