SUMMARY OF THE ENISA GUIDE ON RISK MANAGEMENT MEASURES IN CYBERSECURITY (NIS2)

Summary for **decision-makers, compliance officers, CISOs and non-technical stakeholders.**

DOCUMENT OBJECTIVE

This document summarizes ENISA's recommendations on the implementation of cybersecurity risk management measures, as provided for in Regulation (EU) 2024/2690 under the NIS2 Directive. Its aim is to support entities in implementing good cybersecurity practices adapted to their context.

SUMMARY OF THE ENISA GUIDE

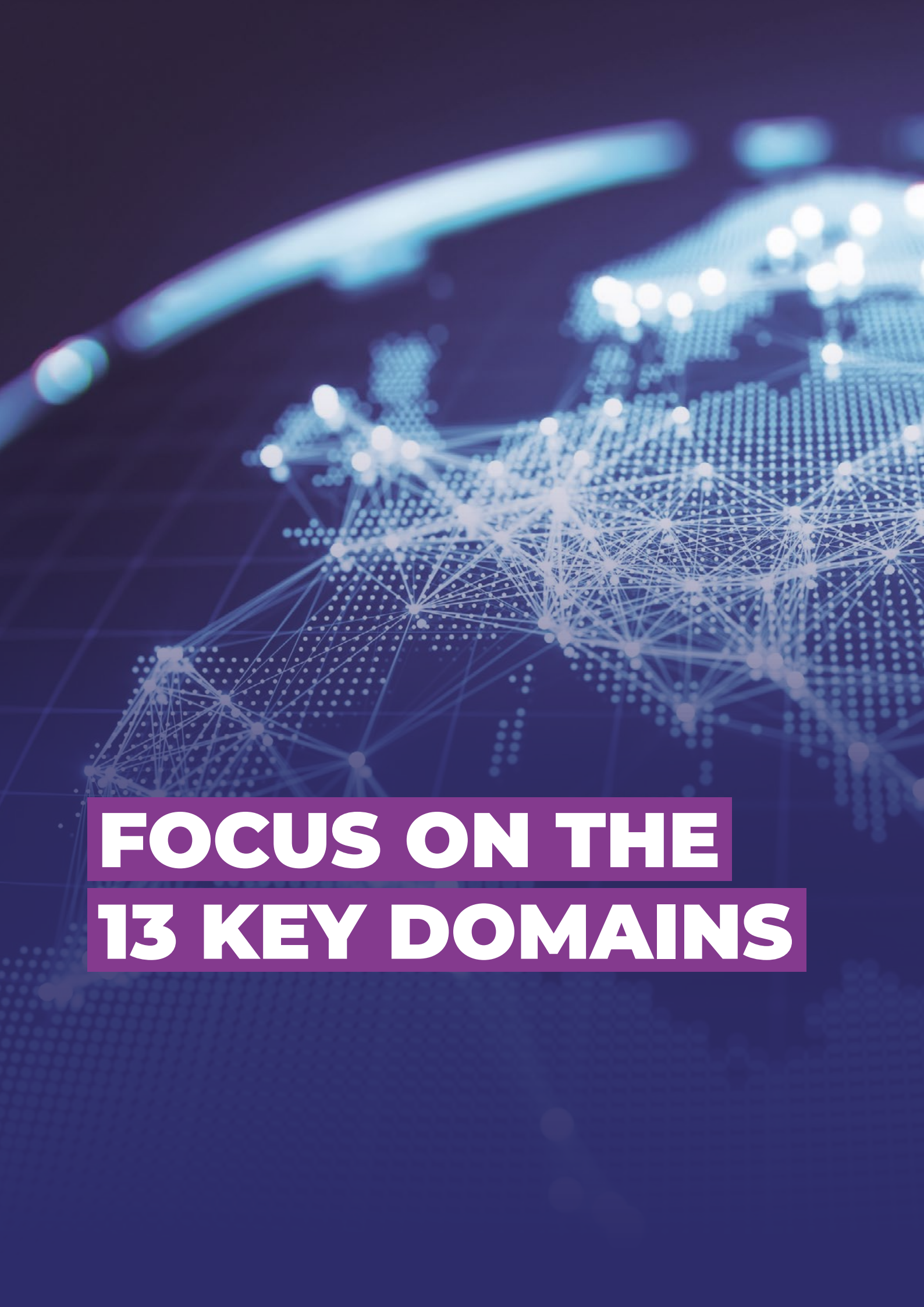
ON RISK MANAGEMENT MEASURES IN CYBERSECURITY (NIS2)

TARGET AUDIENCE

This guide is intended for essential or important entities subject to the NIS2 directive. This guide can also be used by public or private entities to improve their cyber maturity.

SUMMARY

13 KEY DOMAINS:



FOCUS ON THE 13 KEY DOMAINS

1 Policy on the security of network and information systems

OBJECTIVE

Define a clear cybersecurity strategy, validated by management with objectives, roles and appropriate dissemination.

KEY POINTS

- Develop a strategic document approved by the management.
- Integrate security objectives, roles and responsibilities, and allocated resources into it.
- Ensure that all relevant employees and partners are aware of it.
- Review this policy annually or after a major incident.

EXPECTED EVIDENCE

- Information systems security policy signed by management.
- Evidence of internal communication (emails, meetings)
- Acknowledgments of receipt signed by employees and partners.
- List of specific policies mentioned.
- Annual review of the policy.

2 Risk management policy

Implement a structured risk management process (analysis, treatment, acceptance), reviewed on a regular basis.

OBJECTIVE

Identify, assess and address risks to information systems.

KEY POINTS

- Define a methodology for analyzing risks (internal, external, linked to third parties).
- Create a risk treatment plan (reduction, transfer, acceptance).
- Carry out an annual assessment or when significant changes occur.
- Associate this policy with business issues and impact analyses.

EXPECTED EVIDENCE

- Documented risk management methodology.
- Risk treatment plan.
- List of identified risks and their criticality.
- Proof of annual update

3 | Incident handling

Implement detection, response, communication, and post-incident analysis procedures. Conduct regular tests.

OBJECTIVE

Be able to detect, respond and recover quickly from a cyber incident.

KEY POINTS

- Define a clear process to detect, contain, analyze and resolve incidents.
- Establish specific roles and communication plans (internal and external).
- Conduct crisis management exercises to prepare for incidents and in connection with business continuity and recovery plans

EXPECTED EVIDENCE

- Incident management policy.
- Incident communication plans.
- Incident classification and escalation procedures.
- Results and feedback from the exercises carried out.
- Record of past incidents

4 | Business continuity and crisis management

Ensure service continuity even in the event of a major incident, through Business Continuity Plan and Disaster Recovery Plan (BCP/DRP).

OBJECTIVE

Guarantee the resilience of activities even in the case of a cyberattack.

KEY POINTS

- Develop a recovery plan and a business continuity plan.
- Provide backup solutions, redundancy and alternatives in case of breakdown.
- Organize regular tests of these devices.

EXPECTED EVIDENCE

- Recovery and business continuity plans.
- Continuity test results.
- Mapping of critical systems.
- List of backup resources and redundancies.

5 | Supply chain security

Monitor critical suppliers, enforce security clauses, and continuously verify their compliance.

OBJECTIVE

Reduce risks related to suppliers, subcontractors and partners.

KEY POINTS

- Maintain a register of critical suppliers.
- Require security commitments in contracts (Insurance Plan Security).
- Monitor and audit suppliers regularly.
- Take into account software dependencies (open source included).

EXPECTED EVIDENCE

- Supplier contracts with security clauses.
- List of critical suppliers.
- Evidence of audits or compliance assessments of service providers.
- Third-party incident log.

6 | Security in network and information systems acquisition, development and maintenance

Integrate security by design and throughout the lifecycle of systems, including patching and network segmentation.

OBJECTIVE

Integrate security into the design of digital systems and services.

KEY POINTS

- Integrate cybersecurity into calls for tender, contracts, etc.
- Implement a secure development cycle.
- Manage configurations, changes, updates and patches.
- Malware protection and vulnerability management known.

EXPECTED EVIDENCE

- Secure acquisition policy.
- Change and configuration management procedures.
- Results of security tests (pentests, scans).
- Log of updates and patches applied.

7 Policies and procedures to assess the effectiveness of the cybersecurity risk-management measures

Regularly measure the performance of existing security measures and adjust plans accordingly.

OBJECTIVE

Regularly check that security actions are effective.

KEY POINTS

- Establish indicators and periodic reviews.
- Carry out audits, tests, or use control tools.
- Correct the deviations noted and formalize their processing.

EXPECTED EVIDENCE

- Internal or external audit reports.
- Security performance indicators (KPIs).
- Continuous review and improvement procedures.
- Documented patch deployment action plans.

8 Basic cyber hygiene practices and security training

Train staff and promote good security practices (phishing awareness, password management, etc.).

OBJECTIVE

Raise employee awareness and strengthen knowledge of cyber risks within the entity.

KEY POINTS

- Regularly train all employees, according to their level of responsibility and their role.
- Set up regular reminders on good practices (passwords, phishing, etc.).
- Integrate cybersecurity into HR processes (e.g. movement of staff).

EXPECTED EVIDENCE

- Training programs and materials used during sessions.
- Attendance sheets or certificates of participation.
- Awareness campaigns (posters, emails, newsletters).

9 | Cryptography

Use encryption to protect sensitive data. Manage keys and algorithms rigorously.

OBJECTIVE

Protect sensitive data using appropriate encryption methods.

KEY POINTS

- Use appropriate encryption solutions for data sensitive.
- Manage keys securely.
- Apply recognised standards, avoid obsolete algorithms.

EXPECTED EVIDENCE

- Documented encryption policy.
- List of tools or algorithms used.
- Key management log.
- Checks of compliance with standards.

10 | Human resources security

Regulate HR security practices: background checks, offboarding procedures, and confidentiality.

OBJECTIVE

Integrate cybersecurity into employee management.

KEY POINTS

- Conduct background checks for sensitive positions.
- Provide clear procedures for employee arrival and departure.
- Raise awareness of compliance with internal policies and provide a framework disciplinary (e.g. IT charter).

EXPECTED EVIDENCE

- Staff movement procedures (arrival, transfer and departure).
- Contracts with confidentiality clauses.
- History of disciplinary actions (if any).
- Background checks (if required).

11 | Access control

Restrict access based on need, enable multi-factor authentication, and manage privileged accounts.

OBJECTIVE

Ensure that each user only accesses the resources necessary.

KEY POINTS

- Implement an access management policy based on the principle of "need to know".
- Manage privileged accounts with enhanced protections (eg MFA, supervision).
- Carry out regular reviews of access rights.

EXPECTED EVIDENCE

- Access management policy.
- Register of access rights and accounts.
- Results of periodic access reviews.
- Implementation of strong authentication (MFA)

12 | Asset management

Inventory and classify IT assets, control the use of removable media, and manage equipment returns.

OBJECTIVE

Maintain a clear and up-to-date view of critical equipment and data.

KEY POINTS

- Maintain an inventory of assets (hardware, software, data).
- Define their level of criticality.
- Manage removable media.
- Manage the return or destruction of equipment.

EXPECTED EVIDENCE

- Inventory of assets (hardware, software, data).
- Policy on the use of removable media.
- Procedures for returning or removing equipment.

13 | Environmental and physical security

Secure access to premises and prevent physical incidents (fires, outages, intrusions).

OBJECTIVE

To protect premises, equipment and installations against unauthorized access or physical incidents.

KEY POINTS

- Control access to buildings (badges, video surveillance, register).
- Provide measures against fires, floods or power cuts power supply.
- Secure critical areas (server rooms, network equipment).

EXPECTED EVIDENCE

- Diagrams or plans of access to the offices.
- Physical devices installed (badge, cameras, alarms).
- Test or incident simulation reports (e.g. fire).

FRANCE CYBER MARITIME

Le Grand Large,
Quai de la douane, 2ème éperon,
29200 BREST (FRANCE)

CONTACT US

+33 (0)2 57 52 09 87
contact@france-cyber-maritime.eu

www.france-cyber-maritime.eu/en

SUPPORTED BY

RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

ANSSI

Brest Métropole

MINISTÈRE DE LA TRANSITION ÉCOLOGIQUE, DE LA BIODIVERSITÉ, DE LA FORÊT, DE LA MER ET DE LA PÊCHE
Liberté
Égalité
Fraternité

Région BRETAGNE

PREMIER MINISTRE
Liberté
Égalité
Fraternité

Secrétariat général de la mer