

# NIS2 Readiness Checklist

A working document for Belgian SMEs

## KEY DATES AND TIMELINES

|                                    |                                                                                          |
|------------------------------------|------------------------------------------------------------------------------------------|
| CCB registration                   | Deadline passed on <b>18 March 2025</b>                                                  |
| Incident reporting to the CCB      | <b>24 hours</b> early warning, <b>72 hours</b> notification, <b>1 month</b> final report |
| Certification (essential entities) | Deadline <b>18 April 2027</b>                                                            |

## ORGANISATION

## START DATE

## SCOPE

Essential / Important / Not sure

Use this checklist to track your progress toward NIS2 compliance. Tick each item as it is completed and review it with your management team.

### 01 Foundation: Scope and Registration

- ☐ Verify with the CCB whether your organisation is essential, important, or outside NIS2 scope  
Contact: <https://atwork.safeonweb.be/nis2>
- ☐ If in scope, confirm you are registered with the CCB  
Registration deadline passed on 18 March 2025

### 02 Foundation: Risk-Based Approach

- ☐ Create an asset inventory (systems, data stores, services critical to your operations)
- ☐ Establish a risk register (threats, impacts, likelihoods, current controls)
- ☐ Document your incident response plan with:
  - ☐ Key roles and responsibilities
  - ☐ Escalation procedures
  - ☐ CCB reporting timeline (24 hours early warning, 72 hours notification, 1 month final report)
  - ☐ Contact information for national CSIRT

### 03 Technical Controls

- ☐ Implement access control:
  - ☐ Restrict system and data access based on job role
  - ☐ Use multi-factor authentication for remote access
  - ☐ Conduct access reviews (at least annually)
  - ☐ Remove access for departed employees immediately
- ☐ Segment your network:
  - ☐ Separate production from development/test systems
  - ☐ Separate guest networks from corporate networks
  - ☐ Monitor for unusual cross-segment traffic
- ☐ Deploy endpoint security:
  - ☐ Antivirus/antimalware on all endpoints
  - ☐ Regular patch management
  - ☐ Mobile device management for BYOD
- ☐ Encrypt sensitive data:
  - ☐ Data at rest (databases, file storage)
  - ☐ Data in transit (TLS for external communications)
  - ☐ Implement key management procedures

- ☐ Establish backup and recovery procedures:
  - ☐ Test backups regularly
  - ☐ Document recovery procedures
  - ☐ Verify recovery time objectives (RTO) and recovery point objectives (RPO)

## 04 Governance and Documentation

- ☐ Document security policies:
  - ☐ Information security policy
  - ☐ Incident response procedures
  - ☐ Access control procedures
  - ☐ Data handling procedures
  - ☐ Remote work security guidelines
- ☐ Establish management oversight:
  - ☐ Regular security reporting to senior leadership
  - ☐ Security budget allocation
  - ☐ Risk acceptance documentation
- ☐ Conduct regular security testing:
  - ☐ Vulnerability scans (at least quarterly)
  - ☐ Penetration testing (annually or after major changes)
  - ☐ Security configuration reviews for critical systems
- ☐ Track security metrics:
  - ☐ Incident detection time
  - ☐ Incident response time
  - ☐ Control effectiveness measures
- ☐ Provide employee training:
  - ☐ Phishing recognition
  - ☐ Secure password practices
  - ☐ Incident reporting procedures
  - ☐ Data handling

## 05 Certification (Optional)

If you choose a certification route:

- ☐ Understand CyFun levels: Small, Basic, Important, Essential (<https://atwork.safeonweb.be/tools-resources/cyberfundamentals-framework>)
- ☐ Or pursue ISO/IEC 27001 certification
- ☐ Deadline for certification if essential entity: 18 April 2027

## 06 Supply Chain Security

- ☐ Assess critical suppliers and service providers for security requirements
- ☐ Establish contractual security obligations with suppliers
- ☐ Recommend suppliers meet at least CyFun Basic

### SOURCES

Centre for Cybersecurity Belgium (CCB): <https://atwork.safeonweb.be/nis2> and <https://atwork.safeonweb.be/tools-resources/cyberfundamentals-framework>. Always check these pages for current deadlines and requirements.