Offense-Informed Defense · Evidence-Driven Results

NIS2 Compliance Guide
for Belgian SMBs

What NIS2 Means for Your Business
7 Key Requirements Explained
90-Day Implementation Roadmap
Common Gaps & How to Fix Them
Penalties & Enforcement Timeline

Published: February 2026 | **Edition:** 1.0
Contact: cypra.be | Penetration Testing · Network Analysis · Digital Forensics

Executive Summary

The NIS2 Directive (EU 2022/2555) represents the European Union's enhanced framework for cybersecurity requirements across critical sectors. For Belgian SMBs, this directive introduces mandatory security measures, incident reporting obligations, and significant penalties for non-compliance.

Enforcement Date	October 17, 2026
Scope	Essential and important entities (most SMBs with 10+ employees)
Maximum Fine	€10 million or 2% of global revenue (whichever is higher)
Key Change	Mandatory security testing and incident reporting

■ This guide provides a practical roadmap for Belgian SMBs to achieve NIS2 compliance without unnecessary complexity or cost.

Who Is Affected by NIS2?

NIS2 applies to "essential" and "important" entities across specific sectors. In Belgium, this includes most SMBs with 10 or more employees operating in designated industries.

Affected Sectors

Sector	Classification	Typical Belgian SMBs
Energy	Essential	Utilities, renewable energy providers
Transport	Essential	Logistics, shipping, aviation services
Healthcare	Essential	Hospitals, clinics, medical device manufacturers
Digital Infrastructure	Essential	Cloud providers, data centers, ISPs
Manufacturing	Important	Industrial manufacturers, chemical producers
Food Production	Important	Food processing, distribution
Digital Services	Important	Online marketplaces, search engines, social networks
Postal Services	Important	Courier and postal operators

Size Thresholds

Medium-sized enterprises: 50-249 employees or €10-50M annual turnover
Small enterprises: 10-49 employees or €2-10M annual turnover
Micro enterprises: Under 10 employees (generally exempt, unless classified as essential)

> ■ **WARNING: Even if your company has fewer than 50 employees, you may still be classified as an 'essential entity' if you provide critical services. Check with the Belgian Centre for Cybersecurity (CCB) if unsure.**

The 7 Key NIS2 Requirements

NIS2 mandates specific cybersecurity measures across seven core areas. Each requirement has practical implications for how you operate your IT infrastructure and respond to incidents.

1. Risk Management & Security Policies

Implement risk management measures appropriate to your threat landscape.

What You Need:

- Documented cybersecurity policy
- Regular risk assessments (at least annually)
- Risk treatment plans with assigned ownership
- Board-level cybersecurity oversight

Common Gaps: *Many SMBs lack formal risk documentation or have outdated policies that don't reflect current threats.*

2. Incident Handling & Reporting

Establish procedures for preventing, detecting, and responding to incidents.

What You Need:

- Incident response plan (documented and tested)
- Early warning notifications within 24 hours of detection
- Incident reports within 72 hours
- Final reports within one month
- Designated incident response team or contact

Common Gaps: *No tested incident response plan. No clear escalation path. Unrealistic reporting timelines.*

3. Business Continuity & Crisis Management

Ensure operational resilience through backup systems and disaster recovery.

What You Need:

- Business continuity plan (BCP)
- Regular backups tested for restoration
- Disaster recovery procedures

- Crisis communication plan
- Defined Recovery Time Objectives (RTO) and Recovery Point Objectives (RPO)

Common Gaps: *Backups exist but are never tested. No documented RTOs. No crisis communication plan.*

4. Supply Chain Security

Assess and manage cybersecurity risks from suppliers and service providers.

What You Need:

- Vendor risk assessment process
- Security requirements in contracts
- Regular audits of critical suppliers
- Supply chain incident response coordination

Common Gaps: *No visibility into third-party security posture. Contracts lack cybersecurity clauses.*

5. Security in Network & Information Systems

Deploy appropriate technical and organizational measures to secure systems.

What You Need:

- Network segmentation
- Access controls (least privilege, MFA)
- Encryption for data at rest and in transit
- Secure configuration management
- Patch management process
- Logging and monitoring

Common Gaps: *Flat networks with no segmentation. Weak access controls. Inconsistent patching.*

6. Security Testing & Audits

Regularly test the effectiveness of your security measures.

What You Need:

- Penetration testing (at least annually)
- Vulnerability assessments
- Security audits (internal or external)

- Remediation tracking and validation

Common Gaps: *No external testing. Vulnerabilities identified but never fixed. No retesting after remediation.*

7. Training & Awareness

Ensure staff understand cybersecurity risks and responsibilities.

What You Need:

- Regular security awareness training
- Phishing simulations
- Role-specific training for IT staff
- Management cybersecurity briefings

Common Gaps: *One-time training during onboarding. No phishing tests. Executives not trained.*

90-Day Implementation Roadmap

This roadmap prioritizes the most critical NIS2 requirements and provides a realistic timeline for Belgian SMBs to achieve compliance. Adjust timelines based on your organization's size and resources.

Phase 1: Foundation (Days 1-30)

Week 1	**Gap Analysis**	• Assess current security posture against NIS2 requirements • Identify critical gaps • Prioritize remediation efforts
Week 2	**Documentation**	• Draft cybersecurity policy • Document current risk register • Create incident response plan template
Week 3	**Technical Assessment**	• Conduct vulnerability scan • Review network architecture • Audit access controls and permissions
Week 4	**Planning**	• Define implementation roadmap • Assign responsibilities • Set budget and timeline

Phase 2: Implementation (Days 31-60)

Week 5-6	**Critical Controls**	• Implement MFA for all privileged accounts • Deploy network segmentation • Configure centralized logging • Establish backup procedures
Week 7-8	**Processes & Policies**	• Finalize incident response plan • Complete business continuity plan • Conduct tabletop exercise • Train incident response team

Phase 3: Validation & Improvement (Days 61-90)

Week 9-10	**Testing**	• Conduct penetration test • Test backup restoration • Validate incident response plan • Review vendor contracts
Week 11-12	**Remediation & Documentation**	• Address findings from pentest • Complete compliance documentation • Conduct staff training • Prepare for external audit

Penalties & Enforcement

NIS2 introduces significant penalties for non-compliance, with enforcement beginning October 17, 2026. Belgian authorities have broad powers to inspect, audit, and sanction non-compliant organizations.

Financial Penalties

Violation Type	Essential Entities	Important Entities
Major violations (e.g., no incident reporting, inadequate security measures)	€10M or 2% of global turnover	€7M or 1.4% of global turnover
Minor violations (e.g., failure to cooperate with authorities)	€7M or 1.4% of global turnover	€5M or 1% of global turnover

Beyond Fines: Real Business Impact

1. Personal Liability for Management: Directors and senior management can be held personally liable for failing to implement adequate cybersecurity measures.

2. Operational Shutdown: Authorities may suspend operations during investigations or until critical vulnerabilities are remediated.

3. Reputational Damage: Non-compliance reports may be made public, damaging customer trust and competitive position.

4. Loss of Contracts: Many public sector and enterprise contracts now require NIS2 compliance as a condition for doing business.

■ ENFORCEMENT TIMELINE
October 17, 2024: NIS2 entered into force (EU level)
October 17, 2024 - October 17, 2026: Transposition period for member states
October 17, 2026: Enforcement begins in Belgium
Post-October 2026: Audits, inspections, and penalties for non-compliance

Common Gaps We Find During Pentests

Based on penetration tests conducted across Belgian SMBs in 2024-2025, these are the most frequent vulnerabilities that leave organizations non-compliant with NIS2 requirements.

1. Misconfigured Network Segmentation

Description	Flat network architecture allows lateral movement from guest WiFi to production systems.
Frequency	74% of tested organizations
Impact	Critical
How to Fix	Implement VLANs, firewall rules, and zero-trust network access (ZTNA).

2. Weak or Missing Multi-Factor Authentication (MFA)

Description	Privileged accounts protected only by passwords, vulnerable to credential stuffing and phishing.
Frequency	68% of tested organizations
Impact	High
How to Fix	Deploy MFA for all admin accounts, VPN access, and cloud services.

3. Unpatched Vulnerabilities

Description	Critical CVEs remain unpatched months after disclosure, especially on legacy systems.
Frequency	61% of tested organizations
Impact	Critical
How to Fix	Establish patch management SLA (critical patches within 14 days) and asset inventory.

4. Inadequate Logging & Monitoring

Description	No centralized logging, retention periods too short, no alerting on suspicious activity.
Frequency	82% of tested organizations
Impact	High
How to Fix	Deploy SIEM or centralized logging with 12+ month retention and automated alerts.

5. Untested Backup & Recovery

Description	Backups exist but have never been tested for restoration; RPO/RTO undefined.

Frequency	77% of tested organizations
Impact	Critical
How to Fix	Quarterly restore tests, document RTOs, implement offline/immutable backups.

6. Weak Access Controls

Description	Overly permissive access rights, shared admin accounts, no regular access reviews.
Frequency	71% of tested organizations
Impact	High
How to Fix	Implement least privilege, disable unused accounts, quarterly access reviews.

Next Steps: How Cypra Can Help

NIS2 compliance doesn't require a six-figure security budget. It requires a clear assessment of where you stand, a prioritized remediation plan, and expert guidance to implement it efficiently.

Our Approach

Service	What We Do	Timeline
NIS2 Gap Assessment	Evaluate your current posture against all 7 NIS2 requirements. Identify critical gaps and prioritize remediation.	2-3 weeks
Penetration Testing	Simulate real-world attacks to validate your defenses. Test network segmentation, access controls, and incident detection.	2-4 weeks
Network Analysis	Map your network architecture, identify misconfigurations, and recommend segmentation strategies.	1-2 weeks
Remediation Roadmap	Provide a step-by-step plan with cost estimates, timelines, and vendor recommendations.	1 week
Ongoing Support	Annual retesting, incident response support, and compliance monitoring.	Ongoing

BOOK A FREE 30-MINUTE SECURITY ASSESSMENT

We'll walk you through:

- Where you currently stand relative to NIS2 requirements
- The 3-5 highest-priority gaps to address first
- A realistic timeline and budget estimate

Visit cypra.be to schedule your assessment

Cypra
Penetration Testing | Network Analysis | Digital Forensics
Web: cypra.be
Email: info@cypra.be
Tagline: Offense-informed defense. Evidence-driven results.