spotit
YOUR SECURITY & NETWORK LAYER

NIS2 Readiness

Bruno Van Wilder

10 February 2025

Agenda

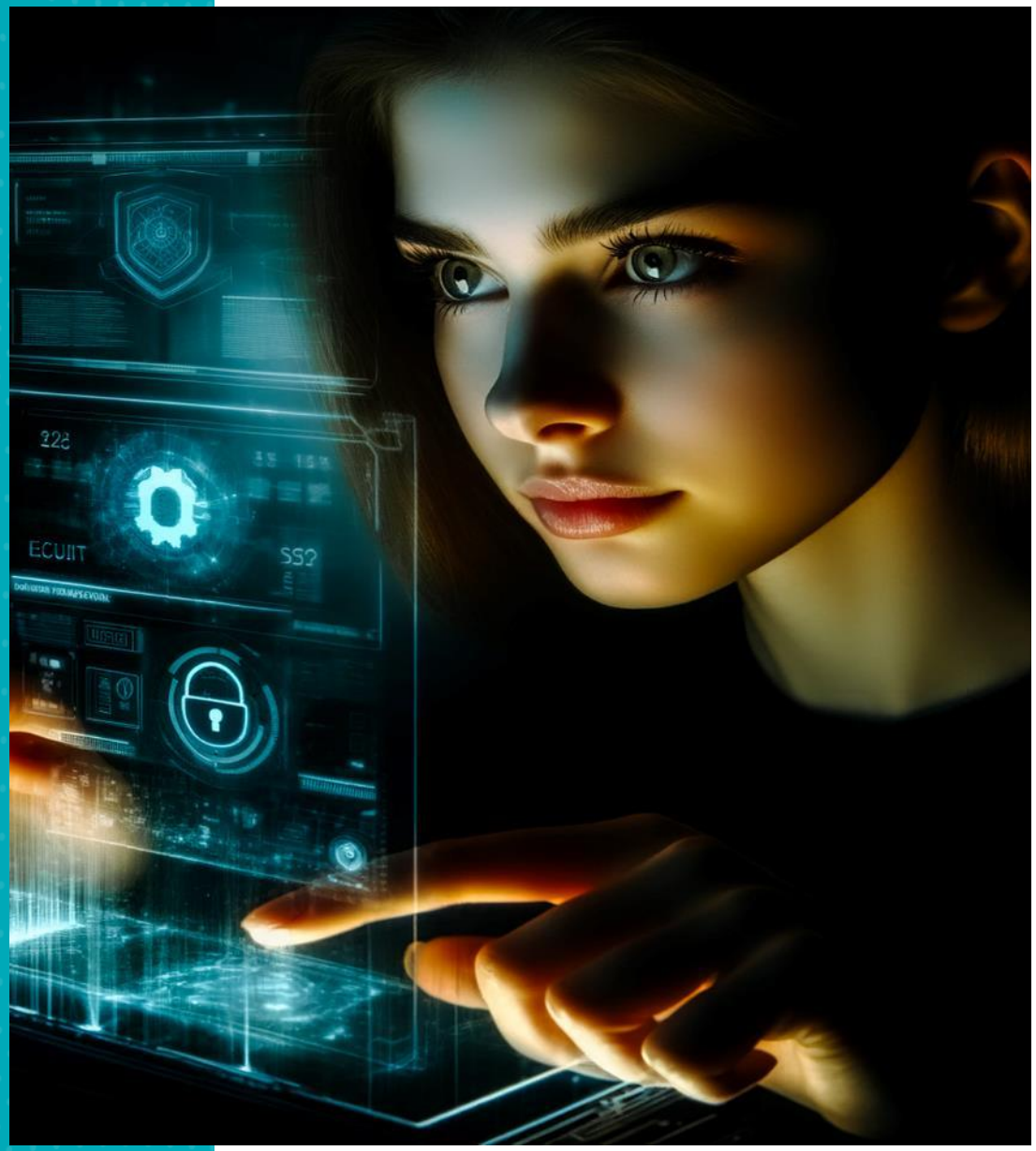
Information Security

NIS2 Law & Scope

Contents

Security Frameworks

Information Security



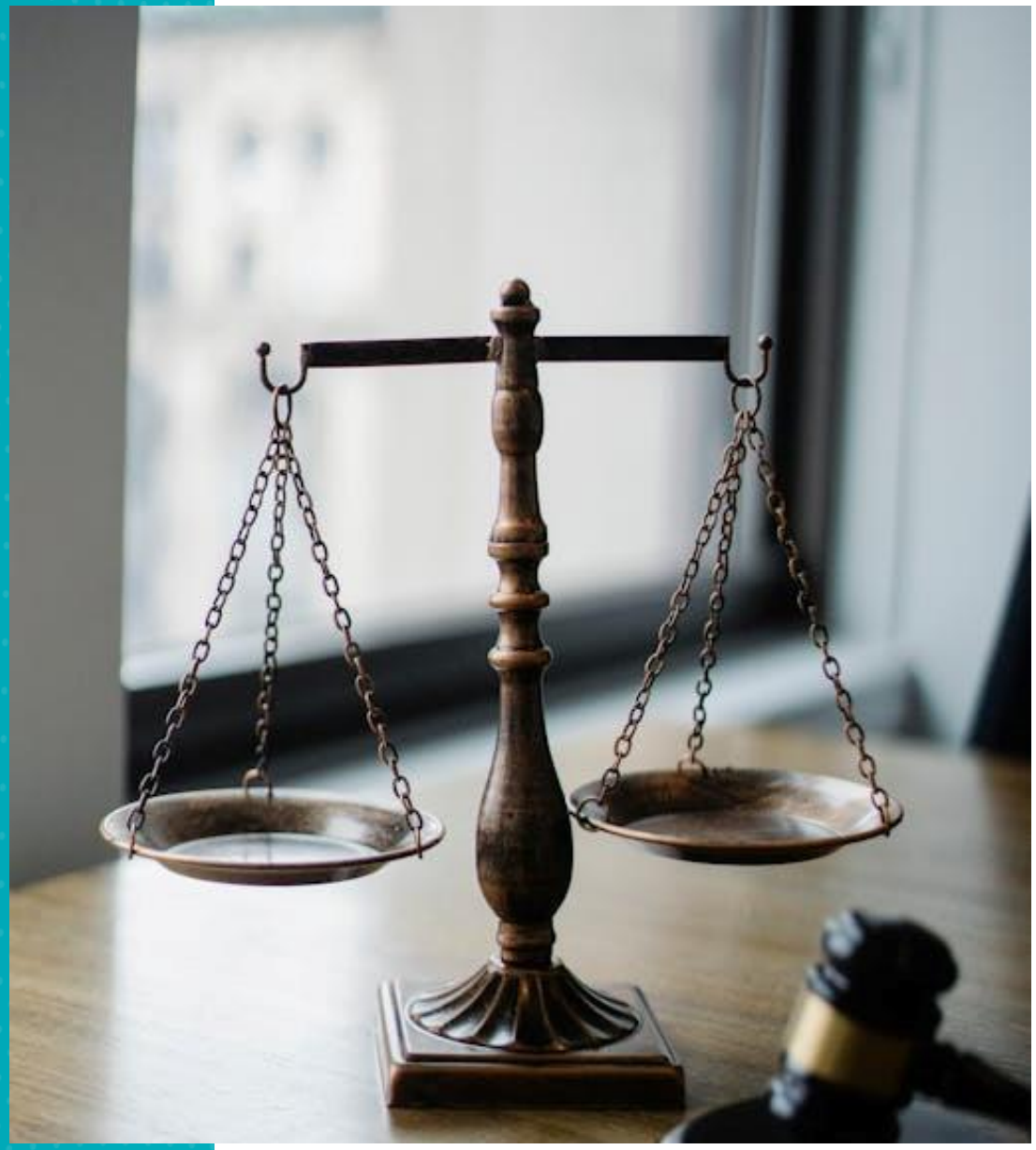
Information Security

- Information = business asset
  - Of high value to organisation
  - Must be suitably protected
- Information ~~Technology~~ Security
  - A process, not a product
  - Securing people, processes and technology
- Reduce risks
  - Confidentiality
  - Integrity
  - Availability

Business impact of a breach

- Direct money loss
  - Blackmail, ransomware
  - Money stolen from bank accounts
  - Goods stolen from warehouse, during transport, …
  - Fines (compliancy failure, contracts with customers, …)
  - Attorneys, extra marketing, notification costs, …
  - Recovery work and costs
- Indirect money loss
  - Reputation loss
  - Strategy setback

NIS2 Law & Scope



NIS2 Directive & Law

Network & Information Security

European Directive, transposed in Belgian Law

- EU adoption on 14 December 2022
- Goal: high common level of cybersecurity across the EU
- Belgian NIS law of 26 April 2024
  - applicable since 18 October 2024
- Rules depend on sector and size
  - “Important” or “Essential” entities
- Supervised by Centre of Cybersecurity for Belgium (CCB)
- CCB also manages security framework
  - Cyber Fundamentals (CyFun)

Scope: entity

- Entities established in **Belgium**
  - For some sectors: entities with headquarters in Belgium

- That provide **services** or carry out their **activities** in the European Union

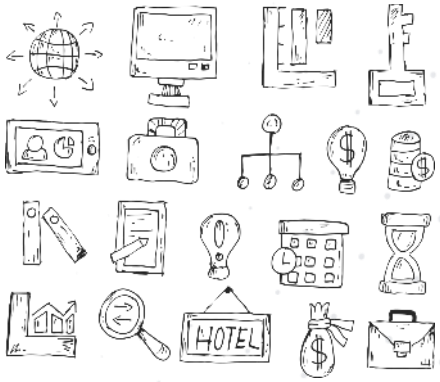
- **Medium entities:**
  > 50 employees **OR**
  > 10 M€ annual turnover or balance sheets exceeds 10 M€

- **Large entities:**
  > 250 employees **OR**
  > 50 M€ annual turnover or balance sheets exceeds 43 M€

- **Groups of entities:** quantities above are consolidated

Sectors

- Energy
- Transport
- Banking
- Financial Market Infrastructure
- Health
- Drinking water
- Waste water
- ICT service management
- Space
- Postal and courier services
- Waste management
- Chemicals
- Food
- Manufacturing
- Digital providers
- Research
- Public administration
- Digital Infrastructure



Example

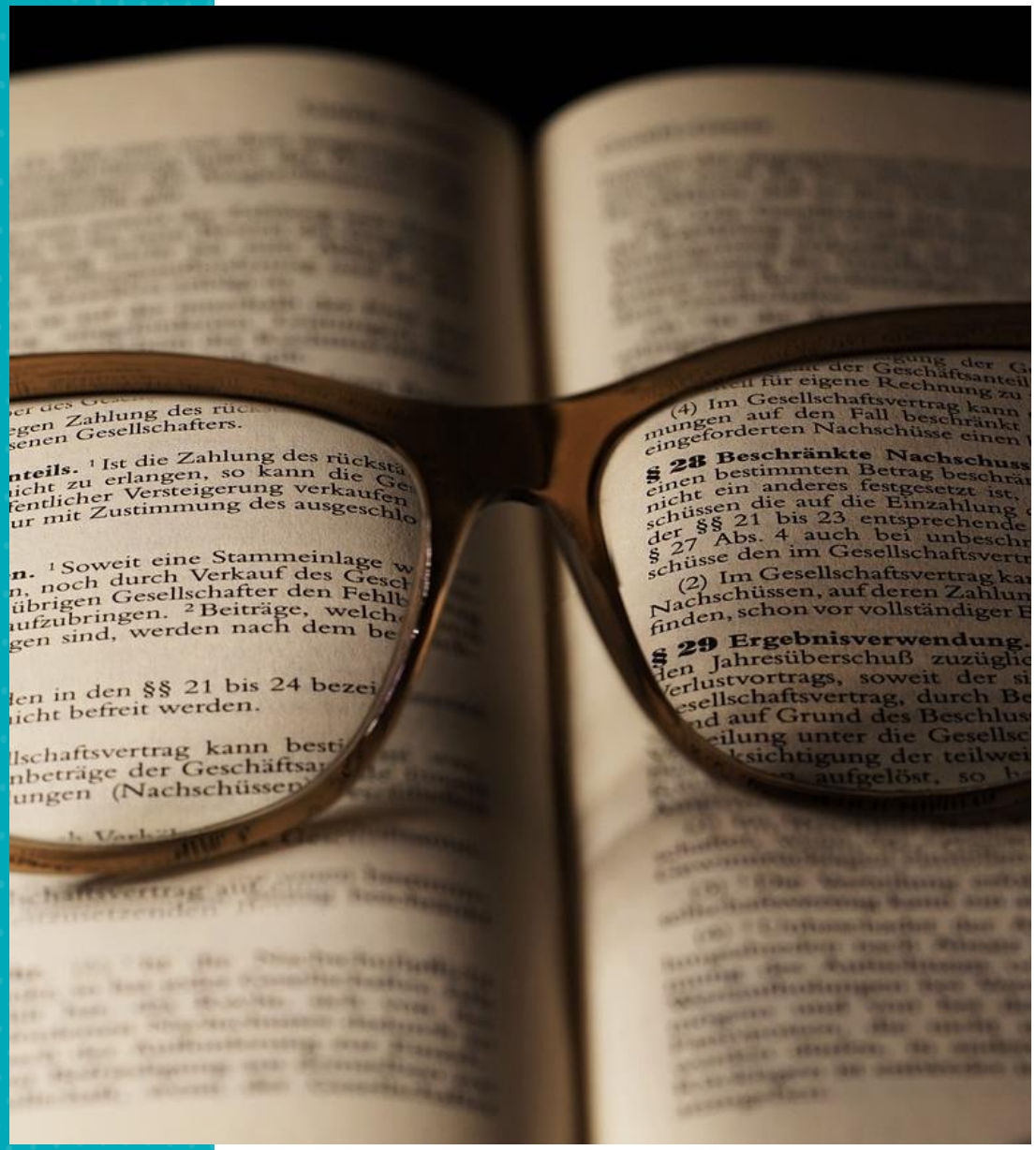
Sector	Size	Establishment
Manufacture of motor vehicles, trailers and semi-trailers → **In scope**	Majority owned by parent company → Consolidation → **Large enterprise**	Entity established in Belgium → **Important entity**

Decision Tree

NIS2 Decision Tree

- Determine scope and level of your entity
- No registration required
- https://www.spotit.be/
  - → Services
  - → Identify
  - →Governance
  - →Decision tree

Contents



Measures

- Policies on risk analysis and information system security
- Incident handling –mandatory reporting
- Business continuity (backup management, disaster recovery, crisis management)
- Supply chain security (incl. relationship between entity & supplier/provider)
- Security of information systems: authentication, access control, asset management, vulnerabilities, cryptography, etc.
- Policies and procedures to assess the measures
- Basic cyber hygiene practices and cybersecurity training

Management obligations

Approve cybersecurity risk management measures

Oversee the implementation of cybersecurity measures

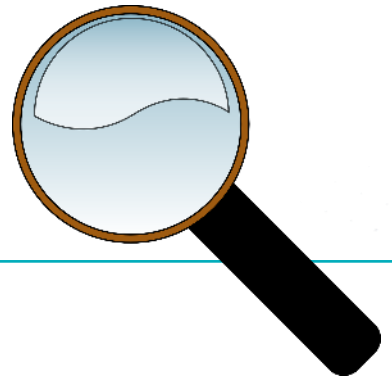
Follow training to gain skills to identify cybersecurity risks

Offer regular staff training

Management bodies and their members are liable!

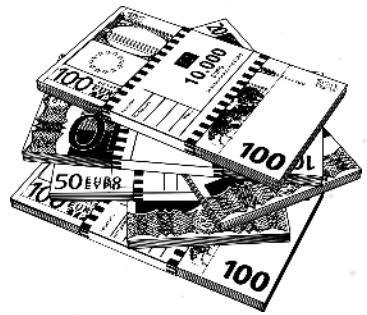
Supervision

Important entities	Essential entities
Ex-post = supervision after an incident, evidence of violations	Ex-ante and ex-post = proactively and reactively
Onsite inspections & offsite supervision	
Targeted security audits bases on risk assessments	
Security scans	
Request information	
Request evidence on implementing cybersecurity policies	
No mandatory conformity assessment	Mandatory regular conformity assessment



Sanctions

- **Administrative sanctions:**
  - **Notification** about violations
  - Order to remedy **shortcomings**
  - Possibility of **disclosure** of the violations
  - **Inform** natural or legal persons for whom they perform activities
  - Appointment of a **control officer**
  - **Fines** of up to € 7.000.000 or 1,4% of turnover
    - Double if reoccurrence within 3 years



Security Frameworks

Cyber Fundamentals

- Publicly available (www.cyfun.be)
- Based on NIST Cyber Security Framework (US)
- Expected to be used in other EU countries too
- Levels: Basic – Important – Essential
- Contains Controls (requirements) and Guidance
- Conformity starts with self-assessment
  - Self-Assessment can be verified by external accreditation body

CENTRE FOR CYBERSECURITY BELGIUM

ISO 27001

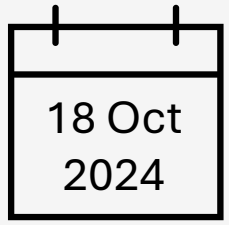
- ISO/IEC 27001 Information Security Management System (ISMS)
- Internationally established and recognised
- Certification according to Statement of Applicability (SoA) and scope:
  - Scope should cover entirely the entity
  - Statement of Applicability should cover NIS2 measures
- Less prescriptive on controls, heavier on documentation
- No granularity

Conformity Assessment

- Essential entities
  - CyberFundamentals certification – Essential
  - ISO 27001 certification
    - with the relevant scope (!)
  - CCB inspection

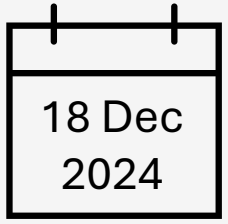
- Important entities – voluntary assessment:
  - CyberFundamentals verification – Important
  - ISO 27001 certification
    - with the relevant scope (!)
  - CCB inspection

Timeline

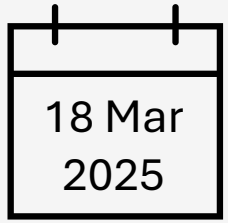


Belgian NIS2 law enters into force

Start of incident reporting

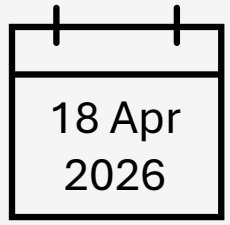


Registration deadline for most digital sectors in scope



Registration deadline for all other entities in scope

Management training (recommended)

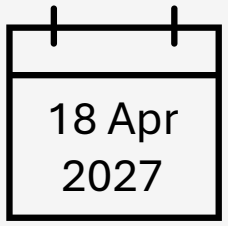


Essential only:

CyFun: Reach at least Basic

ISO: Send Scope and SoA

CCB: Send self-assessment



Essential only:

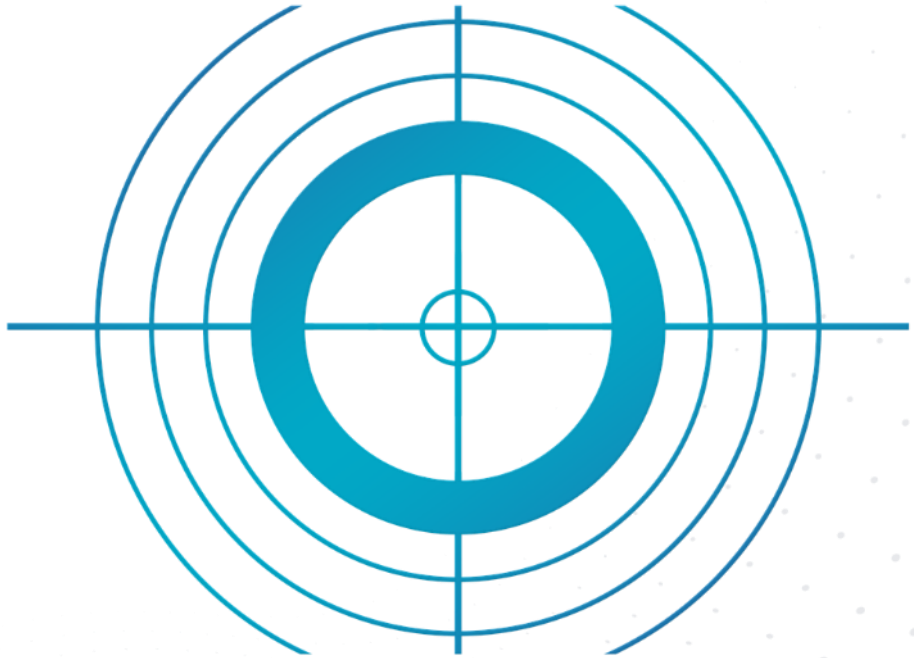
CyFun: verify / certify at target level

ISO: certify

CCB: Report on progress

Focus points

- Documentation: ensures continuity
- Incident handling: expect the unexpected
- Monitoring: know what is going on
- Risk assessment: prioritisation and efficiency
- Supply chain: can you rely on them?
- Training: make them your strongest assets
- Security by design: much cheaper than duct tape
- Management support: lead by example



Conclusion

- Many sectors in scope
- Emphasis on governance & liability for management
- Significant supervision and sanctions
- Tiered security requirements
- Open security framework

- Result = high common level of cybersecurity in the EU

Let’s connect

www.spotit.be

info@spotit.be

@spotitbv

Linkedin/company/spotit

Spotit Headquarters

Guldensporenpark 30 blok C
9820 Merelbeke
Belgium

+32 (0)9 394 44 41

Spotit Herk-De-Stad

Steenweg 3, Blok 402
3540 Herk-De-Stad
Belgium

+32 (0)9 394 44 41