Navigating EU IT-Compliance

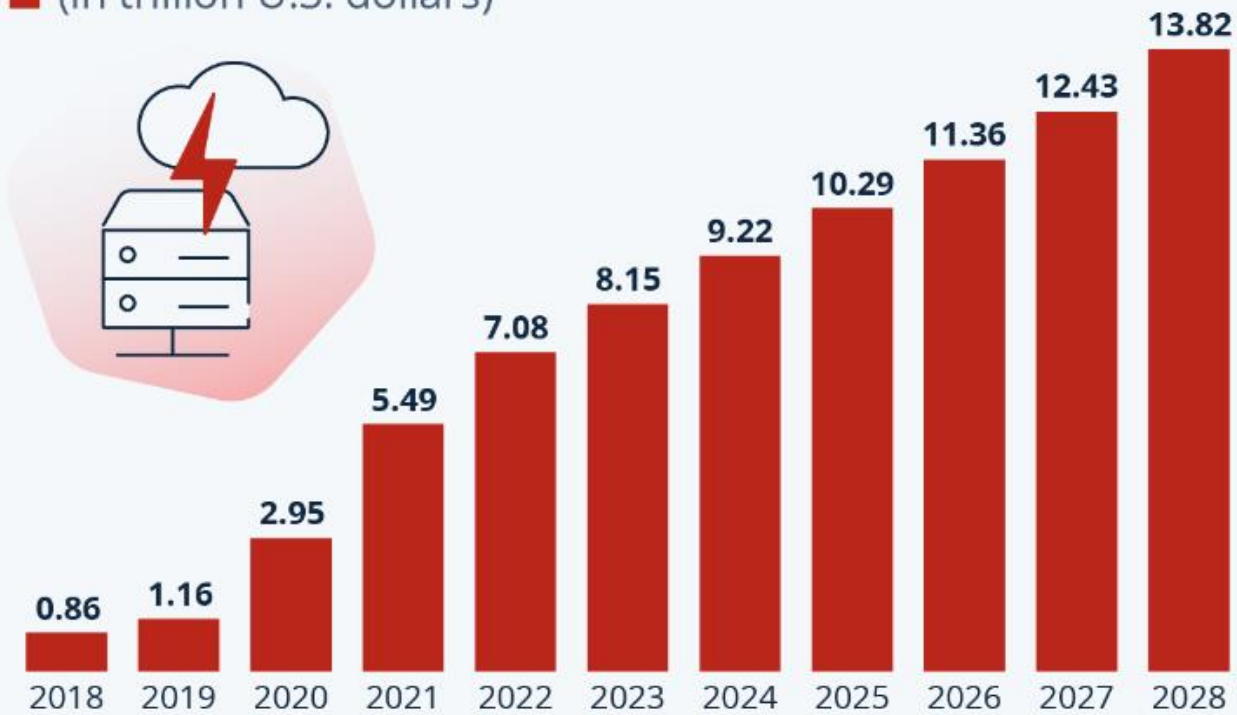
Mastering NIS-2 Requirements for Cybersecurity Excellence

Webinar | October 29th, 2024 | 11:00 – 12:10 am CET

華牌
CHINA BRAND®

Cybercrime Expected To Skyrocket

Estimated annual cost of cybercrime worldwide (in trillion U.S. dollars)



As of Sep. 2023. Data shown is using current exchange rates.
Source: Statista Market Insights

NIS-2-Directive (EU) 2022/2555

華牌
CHINA BRAND®

(First) NIS Directive **adopted in 2016**

The law was passed on **29.06.2017**

NIS-2-Directive published on **27.12.2022**

Belgian House of Representatives adopted the transposition law implementing the NIS2 Directive in **April 2024**

Member states must transpose the directive into national law by **Oct. 2024**

By 18 March 2025, essential and important entities are required to register with the Belgian Center for Cybersecurity.

Member states shall establish a list of essential and important entities by **Apr. 2025**

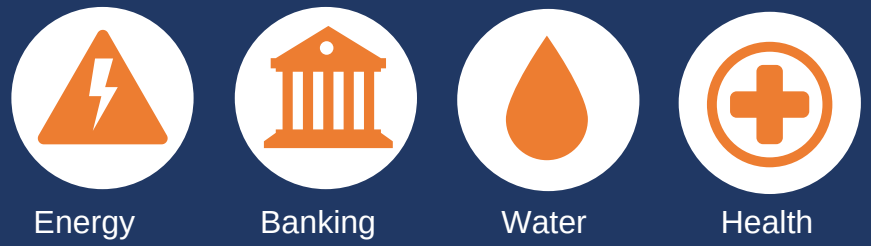
- strengthens and expands cybersecurity requirements for essential and important entities in the EU.
- aims to improve the resilience and security of digital infrastructure across the entire EU.
- establishes uniform standards for the management of cybersecurity risks and reporting obligations for cyber incidents.
- Member states are required to ensure that companies in critical sectors review, assess, officially approve, implement, and monitor their cybersecurity measures.

Article 2: Scope

- Applies to public or private entities (referred to in Annex I or II)
  - Which qualify as medium-sized enterprises (fewer than 250 employees **and** which have an annual turnover not exceeding EUR 50 million, **and/or** an annual balance sheet total not exceeding EUR 43 million.)
  - **OR** exceed the ceilings for medium-sized enterprises (> 50 employees or > annual turnover and/or annual balance sheet exceed EUR 10 million) (under Art. 2 of the Annex to Recommendation 2003/361/EC)
  - **AND** which provide their services or carry out their activities within the EU.
- Regardless of size: Critical entities under Directive - 2022/2557 - EN - CER - EUR-Lex (europa.eu)

Critical Infrastructure (since 2016)

Essential Entities



Who is affected?

NIS-2

Additionally Sectors (since 2022)

What is demanded?

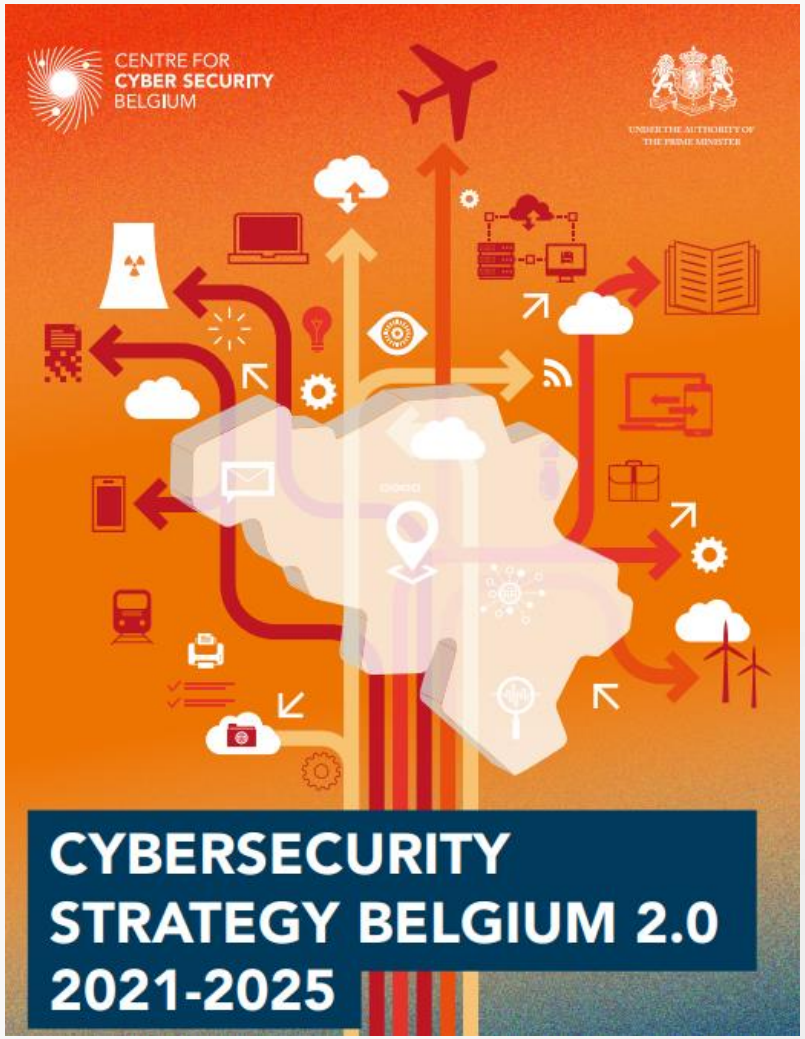
- Appropriate technical, operational, and organizational measures for IT security (risk management)
- Notifications and reporting of security incidents

What are the goals?

Security of the EU and effective functioning of economy and society by

- building cybersecurity capabilities
- ensuring continuity of essential services in critical infrastructures by mitigating threats

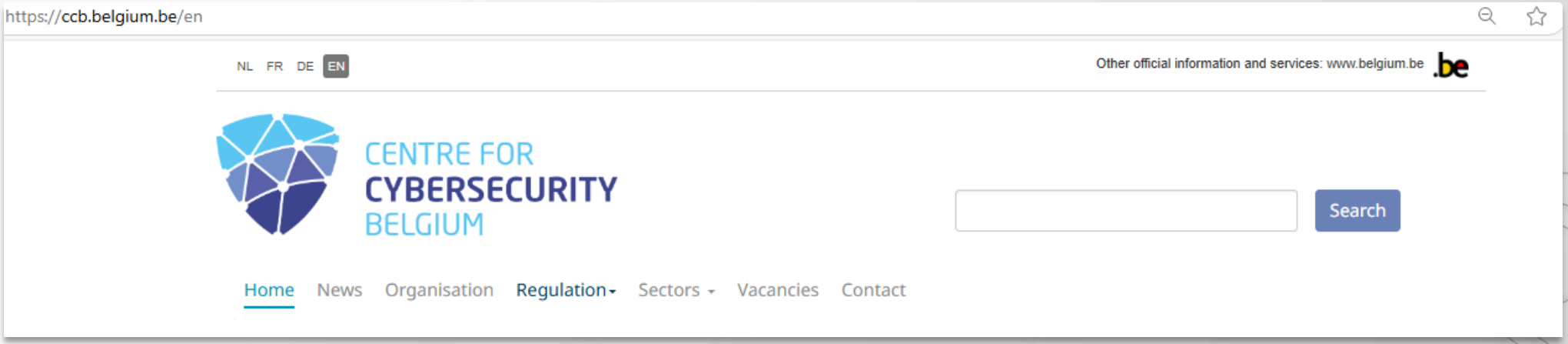
Article 7: National Cybersecurity Strategy



- Each state creates a national cybersecurity plan that outlines its main goals, the resources needed to meet those goals, and the necessary policies and regulations.
- to ensure and maintain a high level of cybersecurity.
  - This means that all EU Member States must take responsibility for minimizing cybersecurity risks and keeping their systems secure in order to ensure a high standard of security both nationally and within the EU.

Article 8: Responsible Authorities

- Each EU Member State establishes a single point of contact and one or more competent authorities for cybersecurity. These authorities monitor compliance with NIS2.
  - Companies should coordinate with the competent national authorities to ensure that cybersecurity practices comply with legal requirements and that cooperation with the authorities runs smoothly.
  - **Centre for Cyber-Security Belgium,** Brussels - CERT.be | Cert / Centre for Cyber security Belgium |



Article 20: Governance

Managers of key institutions:

- need to approve the cybersecurity risk management measures
- monitor their implementation
- must participate in cybersecurity training

- should regularly train employees to develop the necessary skills to identify and manage risks
- are responsible for breaches of these measures

– NIS 2 Directive stipulates that managing directors and other management positions of companies are liable for compliance with the security measures with their private assets.

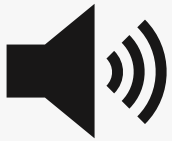
Article 21: Cybersecurity Risk-Management Measures

Requires companies to implement appropriate technical, operational, and organizational cybersecurity measures

- measures must be based on the latest technology and be proportionate to the risks, taking into account factors such as company size and risk potential.
- This includes
  - incident management
  - emergency plans
  - supply chain security
  - the use of multi-factor authentication

- Companies must continuously improve their cybersecurity practices and promptly take corrective action if any vulnerabilities are found

Article 23: Reporting Obligations



Requires companies to report *significant security incidents* promptly to their competent authority

What is a "significant security incident" under NIS2?

- event that causes major problems for a company's services
- results in big financial losses
- affects other people or businesses
  - For example: disruptions like DDoS attacks, ransomware demanding large payments, or data breaches affecting many customers.

Impact is judged based on the level of disruption, financial cost, and harm to others.

Article 23: Reporting Obligations

- An initial warning must be issued within 24 hours of becoming aware of the incident
- followed by a detailed report within 72 hours
- The reporting includes the severity and cross-border impact of the incident
- Companies must also inform affected customers
- authorities provide support and feedback to facilitate further response measures

REPORT AN INCIDENT

First port of call in the event of a cyberattack

Are you a victim of a cyber attackand do you think that the attack is still underway?

If so, take these steps

Advice for transparent communication during a cyberattack.

Reporting form

I am: **a business, a government service, a (non-profit) organisation or an institution of vital importance**

I would like to report an incident or get support regarding an incident

I am an operator of essential services not subject to the control of the National Bank of Belgium or a digital service provider and I wish to report an NIS incident.

Report a suspicious message

I have received a suspicious message and want to report it. Forward the message to suspicious@safeonweb.be.

More information about suspicious@safeonweb

Report by e-mail

I want to **send an e-mail** to the CERT: use info[at]ccb.belgium.be

I want to **send an encrypted e-mail** to the CERT.

Exchange information securely?

Use the Traffic Light Protocol (TLP)

CHINA BRAND®

SUPERVISION AND ENFORCEMENT

Article 32: Supervisory and Enforcement Measures

Authorities are authorized to:

- Conduct on-site inspections and external audits
- Order security assessments by independent bodies or authorities
- Carry out ad-hoc inspections following significant security incidents
- Request access to data and documents
- Require evidence of cybersecurity measures being implemented.

In case of violations of the Directive, authorities can:

- Issue warnings
- Order measures to fix security deficiencies
- Require companies to inform affected users about cyber threats
- Impose fines or suspend certifications.

Article 32: Supervisory and Enforcement Measures

What is a “serious violation”?

- Repeated non-compliance
- Failure to report significant security incidents
- Failure to address deficiencies after an official order
- Obstructing audits

– **Personal Liability**: Responsible individuals can be held personally liable if entities fail to meet their obligations.

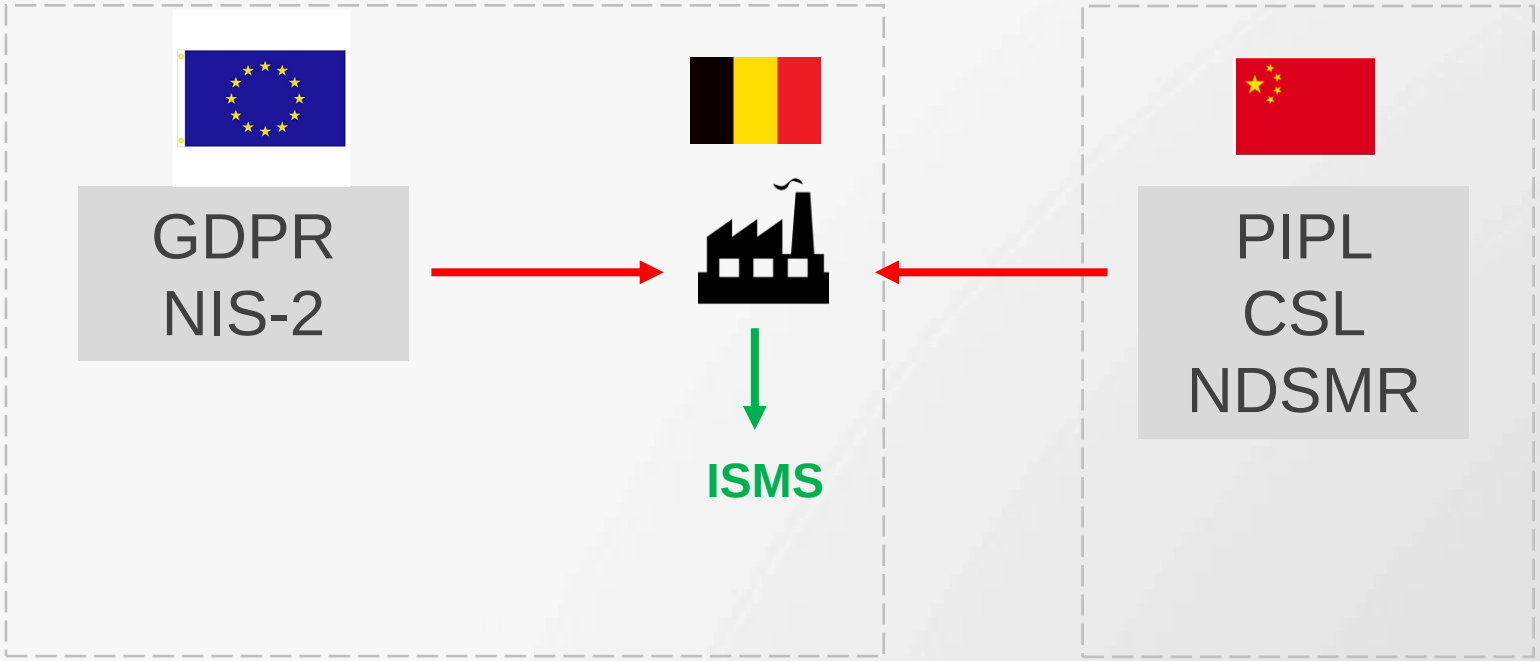
Article 35: NIS2 Directive related to GDPR

- The GDPR (Regulation (EU) 2016/679) regulates the protection of personal data in the EU and applies to all companies that process data of EU citizens, regardless of whether they are based in the EU or not.

- If a company provides essential or important services and a cyberattack or security incident affects personal data, both GDPR and NIS2 apply.

➢ Incidents are addressed from both a data protection and cybersecurity perspective.

Chinese Requirements for Data Protection abroad



PIPL = Personal Information Protection Law

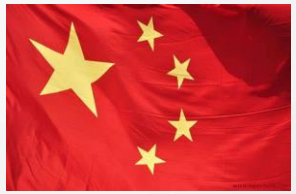
CSL = Cybersecurity Law

NDSMR = Network Data Security Management Regulations

ISMS =
Information Security Management System

華牌
CHINA BRAND®

PIPL and CSL in China



The PIPL

- China's primary data protection law
- governing how personal data is collected, processed, and stored
- has extraterritorial reach (applies to Chinese companies operating abroad if they process data of Chinese individuals

For Chinese businesses in the EU, complying with both NIS2 and PIPL can be challenging, especially when there are conflicting obligations, such as cross-border data transfer restrictions.

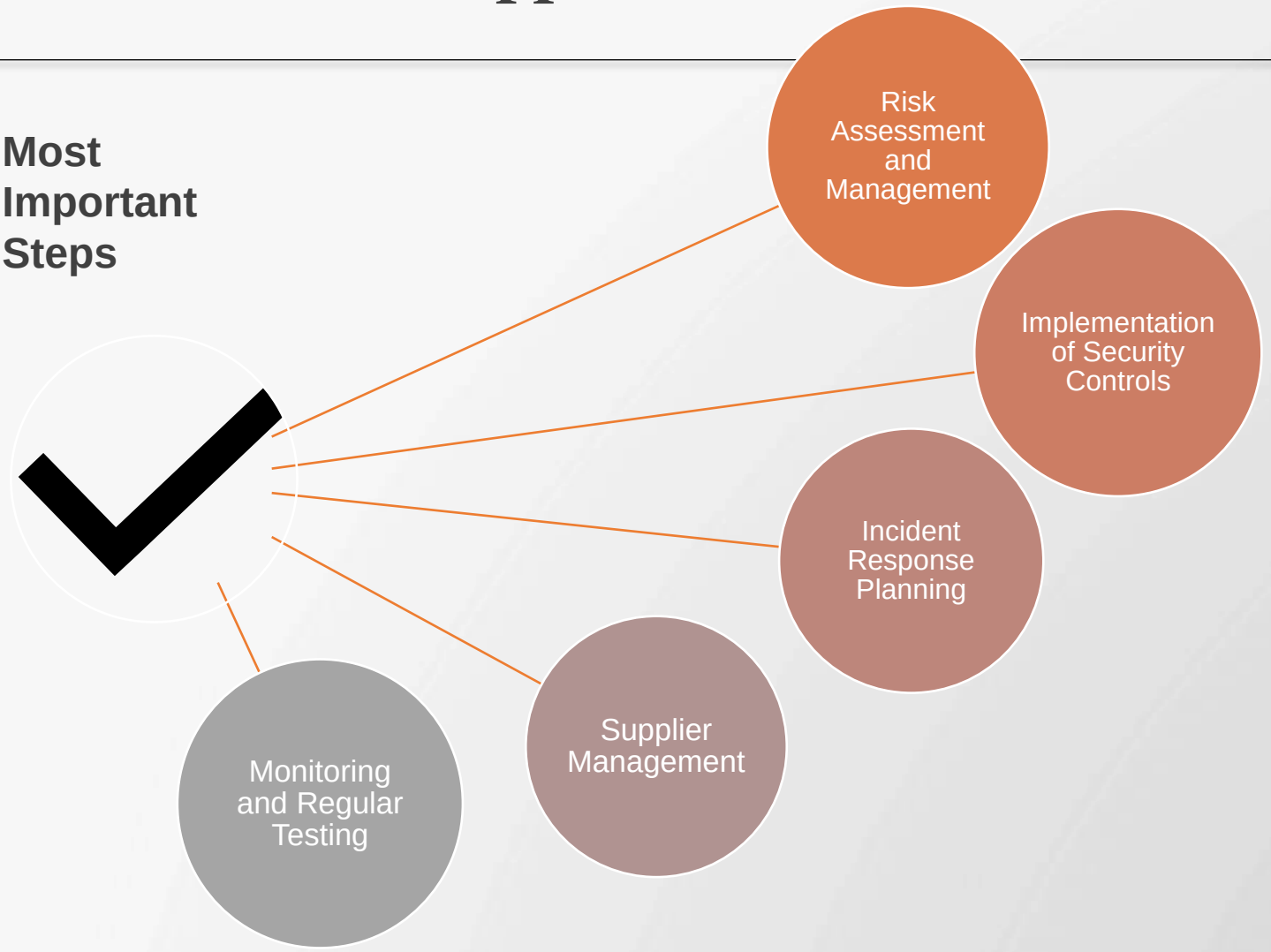
The CSL

- focuses on cybersecurity

Chinese companies in the EU need to align their cybersecurity measures with both EU requirements (NIS2) and Chinese requirements (CSL), especially in terms of protecting data and responding to cyber incidents.

Recommended Approach

Most Important Steps



華牌
CHINA BRAND®

Determine if your organization falls within the scope of Belgian NIS2 Law here:

[NIS 2 Quickstart Guide | CCB Safeonweb]

- Yes
- I am not sure
- I might have a “critical supply chain”
- No, but I still want to be sure

Register your entity as soon as possible:

[Register my organisation | CCB Safeonweb]

Step 1: Risk Assessment and Management

Central element:
Implementation of Comprehensive Risk Management.

First:
conduct a thorough assessment of existing IT infrastructure to identify vulnerabilities and potential threats.

Key questions:
"Which systems are essential for operations?"
"Where are the greatest security gaps?"

Based on this assessment, tailored security measures should be developed and implemented.

Step 2: Implementation of Security Controls

Implementation
of
Security Controls

Based on the risk assessment, specific security controls must be introduced. These include technical and organizational measures such as:

- the encryption of sensitive data
- the introduction of multi-factor authentication (MFA)
- regular security updates
- training employees on cybersecurity best practices

Step 3: Incident Response Planning

Companies must ensure they are prepared for potential security incidents. This involves:

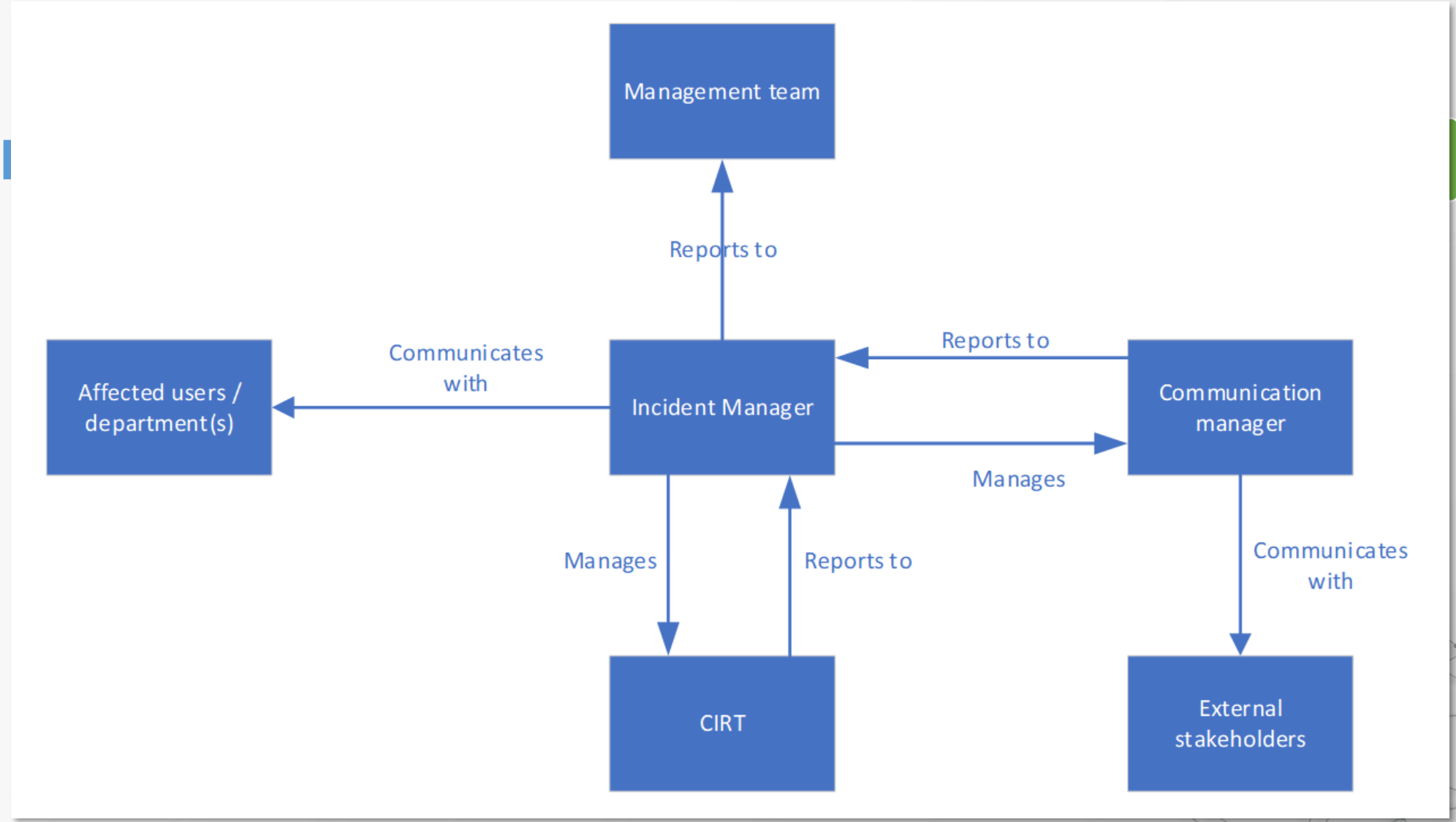
- developing incident response plans
- regularly reviewing incident response plans
- establishment of clear processes and responsibilities to respond quickly and effectively in the event of a cyberattack.

A key question is:
"How do we respond in an emergency, and who is responsible?"

華牌
CHINA BRAND®

Prepare

- Planning
- Monitoring
- Alerting
- Test
- Exercise



Step 4: Supplier Management

To comply with NIS2, businesses must pay close attention to **supplier management** because third-party suppliers often pose cybersecurity risks:

1. Supplier Risk Assessment
2. Supply Chain Security Policies (also important: digital supply chain!)
3. Monitoring and Auditing
4. Incident Response with Suppliers
5. Supplier Onboarding and Offboarding
6. Supply Chain Continuity
7. Legal and Regulatory Compliance

By focusing on these areas, businesses under NIS2 can mitigate risks introduced through their supply chain and maintain a strong cybersecurity posture.

Step 5: Monitoring and Regular Testing

Monitoring and Regular Testing

- Continuous monitoring of IT systems
- regular security audits
- penetration tests

are essential to verify the effectiveness of implemented measures and to detect vulnerabilities early.

"Are our systems truly secure, or are there undiscovered weaknesses?"

Belgium: 11 Required Security Measures

1. **Risk Management and Security Policies** for information systems.
2. **Incident Management** for rapid and effective response to security incidents.
3. **Business Continuity and Crisis Management**, including backup management and disaster recovery.
4. **Supply Chain Security** to minimize security risks from suppliers and service providers.
5. **Security in Procurement, Development, and Maintenance of Networks and Information Systems**, including vulnerability management.
6. **Policies and Procedures for Evaluating the Effectiveness of Cybersecurity Measures**.
7. **Cyber Hygiene and Security Training** for employees.
8. **Procedures for Using Cryptography and, where applicable, Encryption**.
9. **Personnel Security, Access Control Policies, and Asset Management**.
10. **Multi-factor Authentication and Secure Communication**, where appropriate.
11. **Coordinated Vulnerability Disclosure** to ensure secure information sharing.

華牌
CHINA BRAND®

華牌
CHINA BRAND®

Rely On Our 20+ Years Of Experience To Help You Achieve Full Compliance In Both The European And Chinese Markets.

Q&A