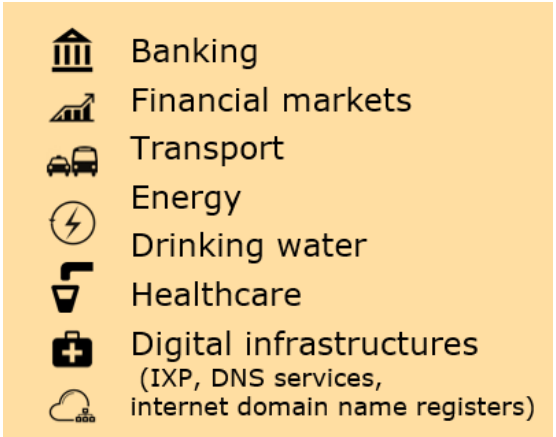
How to get prepared for the Network and Information Security (NIS) Directive ?

Belgian Act is published !!

NIS Directive

The Directive on security of Network and Information Systems (NIS Directive) is a cybersecurity legislation passed by the European Union (EU) on July 6, 2016. Its aim is to achieve a high common standard of network and information security across all EU Member States.

The NIS sets a range of network and information security requirements which apply to operators of essential services and digital service providers (DSPs). The “operators of essential services” (OES) referred to in the legislation include enterprises in the energy, transport, banking, financial market infrastructures, health, drinking water supply and distribution, and digital infrastructure sectors. The NIS Directive requires each EU Member State to put together a list of organisations within those sectors that they consider to be essential service providers.



You can find the published Belgian act on:
http://www.dekamer.be/FLWB/PDF/54/3340/54K3340005.pdf

European security network

The Directive will create a network of Computer Security Incident Response Teams (CSIRTs) in each Member State. Member States are also required to designate National Competent Authorities (NCAs) and Single Points of Contact (SPoC) for cybersecurity monitoring, reporting, incident response, and cross-border coordination. CSIRTs are also required to have access to “adequate resources and equipment” including a secure and resilient infrastructure.

The Member States need to appoint at least one Computer Security Incident Response Team (CSIRT).

The CSIRTs role is to:

- monitor incidents at national level;
- provide early warnings, alerts and information to relevant stakeholders about risks and incidents;
- respond to incidents;
- provide dynamic risk and incident analysis and increase situational awareness;
- participate in a network of the CSIRTs across Europe.

National Cyber Security Strategy

Member States are required to implement a national cybersecurity strategy defining security goals as well as relevant policy and regulations needed to enforce the strategy.

The strategy should include:

- Strategic objectives, priorities and governance framework;
- Identification of measures on preparedness, response and recovery
- Cooperation methods between the public and private sectors;
- Awareness raising, training and education;
- Research and development plans related to NIS Strategy;
- Risk assessment plan;
- List of actors involved in the strategy implementation;
- Member States are also required to designate a minimum of one NCA (National Competent Authority) to monitor the impact and implementation of the NIS Directive at national level. Each Member State SPoC must communicate with other Member State SPoCs to enhance cooperation.

Cooperation Group

In addition to the other bodies established by the NIS Directive, there is a further requirement to create a Cooperation Group whose purpose is to facilitate collaboration around cybersecurity between Member States.

Security requirements

Under the NIS Directive, identified operators of essential services (OES) will have to take appropriate security measures and to notify serious cyber incidents to the relevant national authority. The security measures include:

- Preventing risks
- Ensuring security of network and information systems
- Handling incidents

The table below lists the security requirements:

#	Security requirements	Sectors?
A	Take appropriate and proportionate technical and organisational security measures → Information security policies → Security plan and incident management → Business continuity plan → Control, monitoring and audit (yearly audit (1))	All
B	Provide information needed to assess NIS security → Contact point at OES	All
C	Provide evidence of effective implementation →ISO 27001 certification (3-yearly audit (1))	All, except digital
D	Execute binding instructions received by the NCA to remedy operations	All, except digital
E	Remedy any failure to fulfil NIS requirements	Digital
F	Designate an EU representative, when not established in EU	Digital

(1) Audit report to be transmitted within 30 days to the NCA (National Competent Authority)

The table below lists the notification requirements:

#	Notification requirements	Sectors?
A	Notify any incident (1) having a "significant" (2) or "substantial" impact (confidentiality, integrity and availability) to NCA and CSIRT(3) without delay	All
B	Notify significant impact due to 3rd Party Digital Service Providers	Digital
C	Notify impact of incident when relying on critical 3rd Party Digital Service Providers	All, except digital
D	Inform public about incident if required by the notified authority: NCA or CSIRT	Digital

(1) A secured notification platform will be created

(2) Significance will be determined by

- Number of users affected
- Duration of incident
- Market share of the OES
- Geographical spread
- Extent of disruption (for digital providers only)
- Extent of impact (for digital providers only)

(3) Financial institutions notify to the NBB, who will inform the NCA & CSIRT (BE)

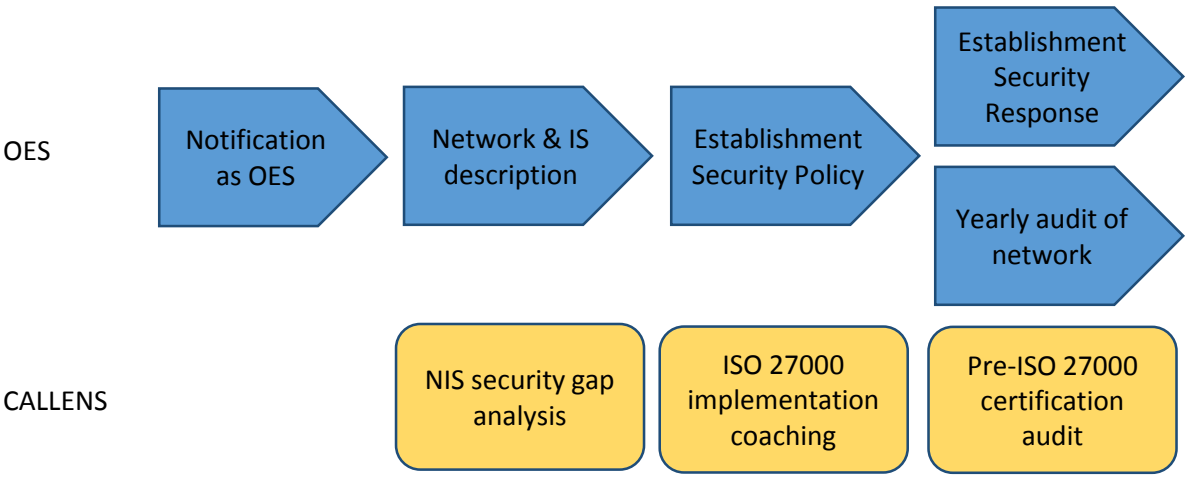
Service offering

Callens, Pirenne, Theunissen & C° can assist your organisation with the preparation and the organisation of the NIS requirements by offering following services:

- **NIS security gap analysis**, allowing you to identify which security requirements need to be implemented;
- **ISO 27001 implementation coaching,** where we assist your staff by coaching them and reviewing the policies and security procedures;
- **Pre ISO 27001 certification audit,** where we assess the effectiveness of the security policies and procedures, ensuring your organization is adequately prepared for the certification audit.

We also assist third party service providers who as an EOS contractor need to comply with the NIS Directive.

In a nutshell, what you have to do and how we can help you:



Crowe
Callens, Pirenne, Theunissen & C°
Independent member of Crowe Global

About Callens, Pirenne, Theunissen & C°

Since 1936 Callens, Pirenne, Theunissen & C° has been a major player in **Belgium's top 10** audit and accountancy firms with a strong sector-oriented approach. Known for the personal approach and integrity and independence the company is highly valued by its customers.

About Crowe Global

Crowe Global is the **8th largest network** of public accounting, consulting and technology firms worldwide. Under its core purpose of "**Smart Decisions – Lasting Value**" Crowe uses its deep industry expertise to provide audit services to public and private entities while also helping clients reach their goals with audit, tax, risk and advisory services. The network consists of more than 220 independent accounting and advisory services firms with 33.000 professionals in more than 130 countries around the world. For almost 100 years, Crowe Global distinguishes itself in the market by bringing **smart decisions** that deliver **lasting value** to clients and the communities where we live and work.

For more information, contact:

Laurent Janssens,
IT audit Director at laurent.janssens@callens.be