

The added value of internal audit in strengthening cyber resilience in the public sector



BE-CYBER, 08/10/2024



WHO ARE WE?

- The Federal Internal Audit conducts audits on the **effectiveness of organizational control systems and risk management** within several federal public services,
- The central focus of our **evaluations** is to enhance the functioning of the federal administration.
- By formulating **recommendations** and ensuring their follow-up, we assist the organisations in achieving their objectives
- Focus on **operational, IT and financial audits**
- Forensic audit activities (whistle blower directive)



- We are an independent organisation administratively hosted by the **FPS Chancellery of the Prime Minister.** Created in **2016** by Royal Decree.
- The **Audit Committee of the Federal Administration** plays a supervision role by monitoring the performance & quality level of our activities.
- Our audits follow the principle of the '**single audit.**' We collaborate with other oversight bodies, including the Court of Auditors and the Inspection of Finances.

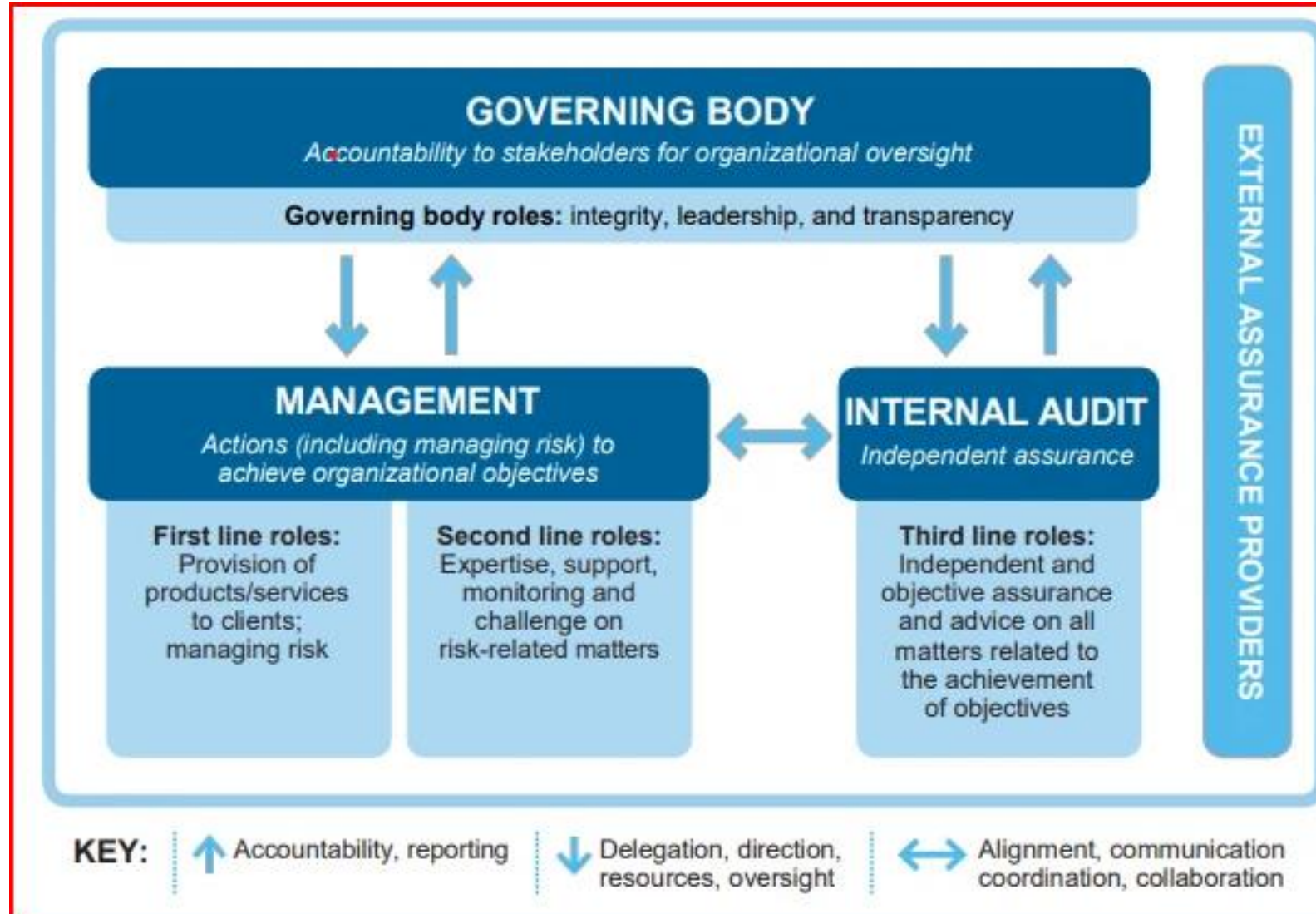
**WHO
ARE
WE?**

AUDIT UNIVERSE

**19 large federal public services & 27 associated
smaller entities with accounting autonomy**
84.594 FTE – budget of 5,8 billion EUR

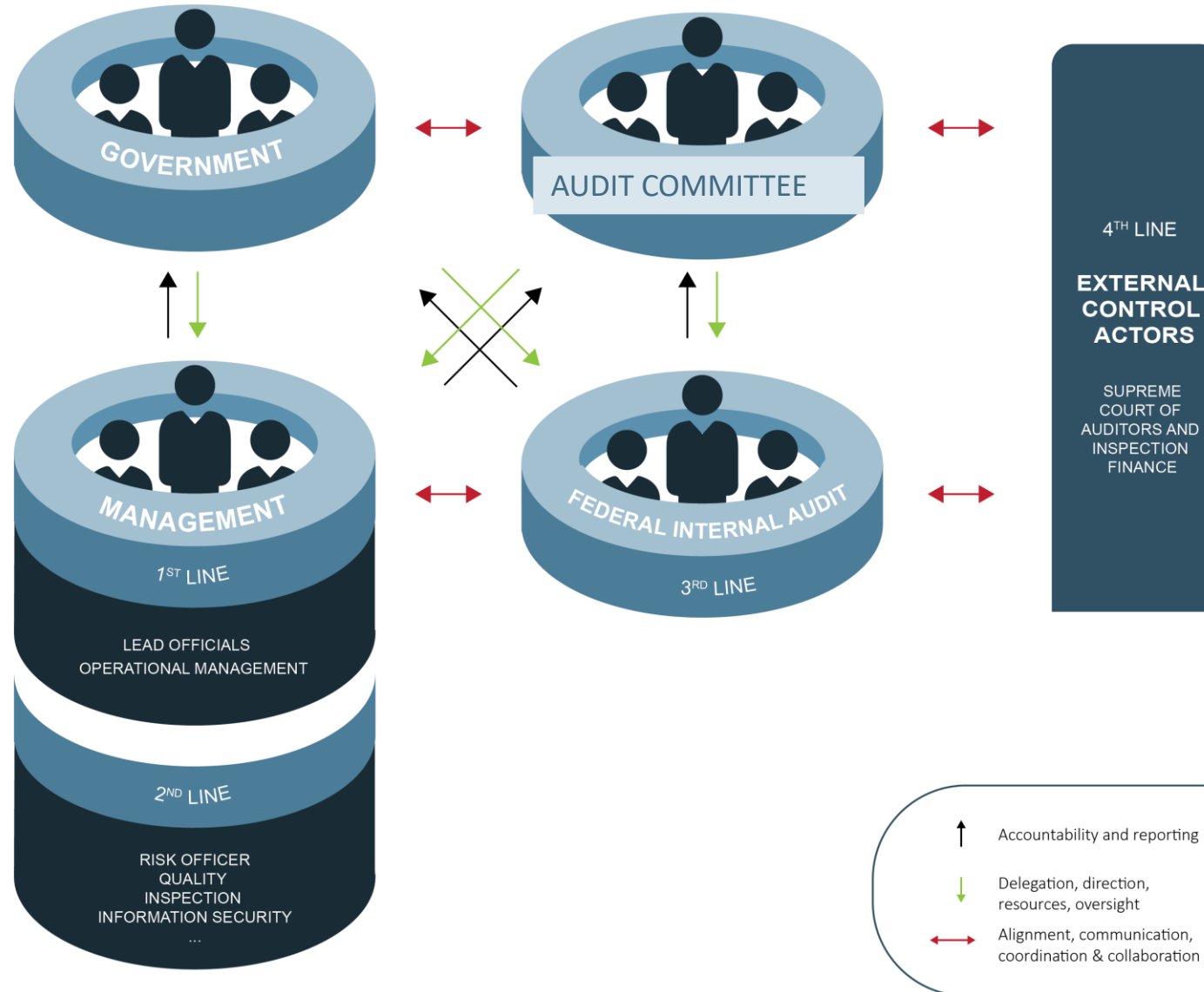


3 LINES MODEL



3 LINES MODEL

FIA
3 lines
model



2025

RISK IN FOCUS

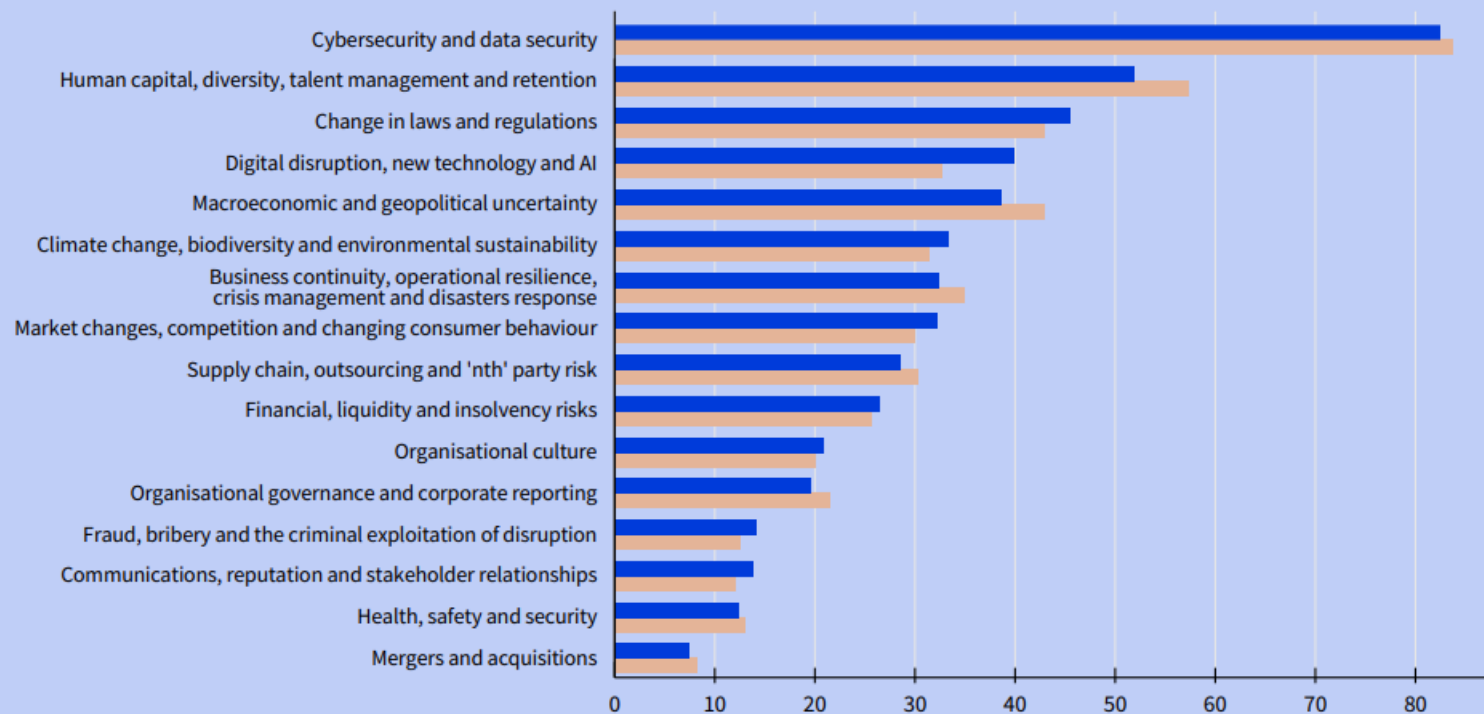
Hot topics for
internal auditors

BOARD BRIEFING



What are the top five risks your organisation currently faces?

Digital disruption, new technologies and AI was the fastest rising category. Organisations are under intense pressure to ramp up efforts to meet growing market demands and keep up with competitors.



Cybersecurity and data security remained the top risk for businesses with the volume and velocity of attacks rising rapidly because of new artificial intelligence (AI) hacking techniques.

IT SECURITY AUDITS (2019-now)

Goals	Combination of 2 components	Methodology used:
<ul style="list-style-type: none">• Provide assurance on operational, compliance and reputational risk to the organisations cyber resiliency• Minimise the organisations exposure to the risk of misconfigurations and weaknesses in the institution's environment	<ul style="list-style-type: none">• security capabilities audit : interviews, evidence-based• vulnerability assessment/security testing: external and internal infrastructure testing, web application testing, ...	<ul style="list-style-type: none">• CCB's Baseline Security Guidelines• ISO 27001 /NIST• Support by subcontractors: for example : Deloitte's cyber strategy framework• Evaluation maturity of several cyber capabilities



IT SECURITY AUDITS (2019-2022) – lessons learned workshop 19/04/2023

Key improvements areas

The tests performed have highlighted 6 main domains that require attention and where organisations could benefit to improve and bolster their overall cyber resiliency

7. Cyber Security Governance

Formally define and agree upon a cyber security strategy. Derive cyber security policies and standards. Define sufficient cyber security roles and assign sufficient personnel to manage cyber security risks within the organisation. Collaborate at Federal level on cyber security.

6. Security event monitoring

Organisations could use the services of CERT.be to help them setup better incident monitoring and establish a common base line for incident management.

5. Web application security

Secure application development lifecycle should be incentivised.

1. Patch and vulnerability management

Guidelines and defined procedures for updates and lifecycle management could help prevent the usage of outdated and vulnerable software.

2. Network security

A better design of the network and the usage of a secure encryption standard for the wireless network could help enforce the boundaries of the security zones.

3. System configuration security

The system security used across organisations could be improved by following industry approved recommendations such as the one provided by the CIS.

4. Identity and Access Management (IAM)

The management of Identities and accesses is a complex and challenging project that would benefit from a holistic approach.

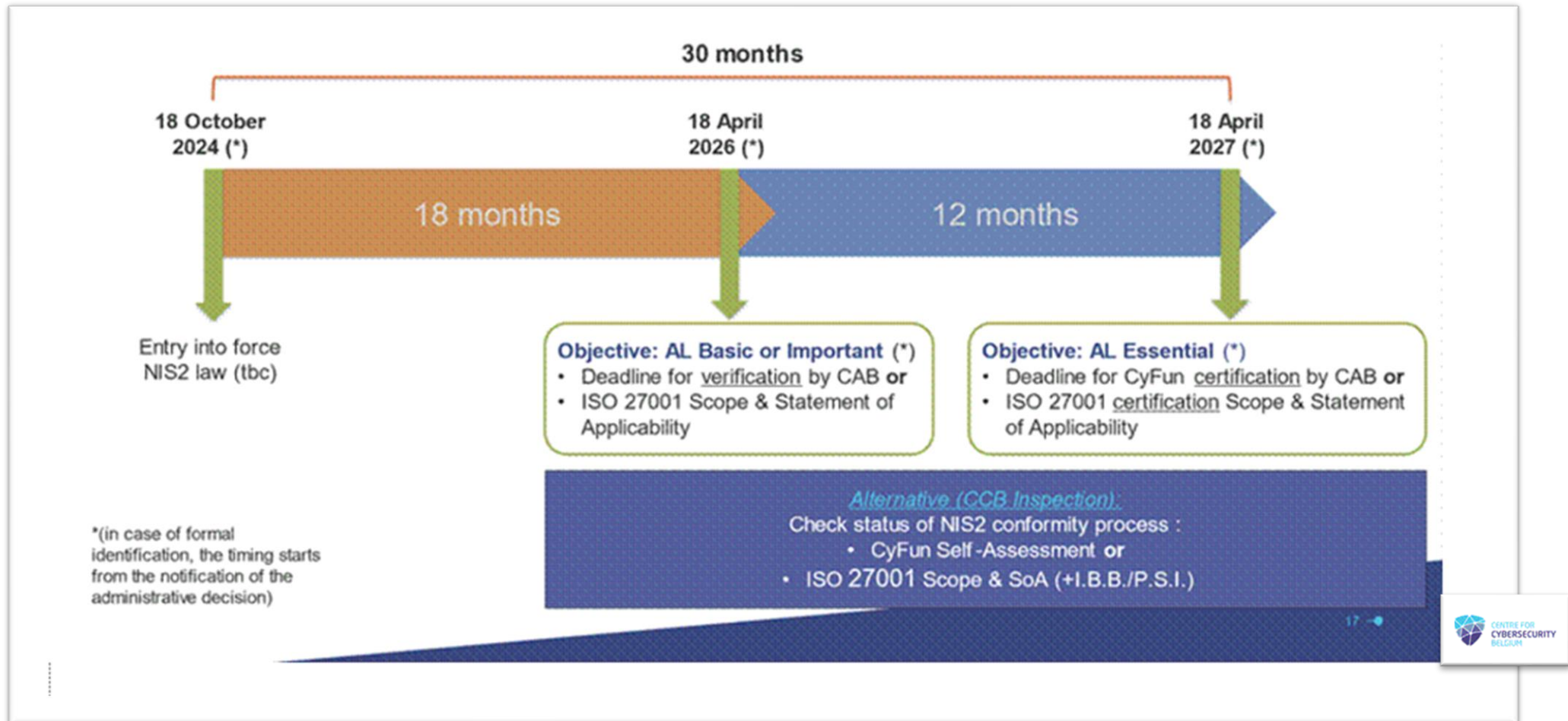


NIS2 IS COMING

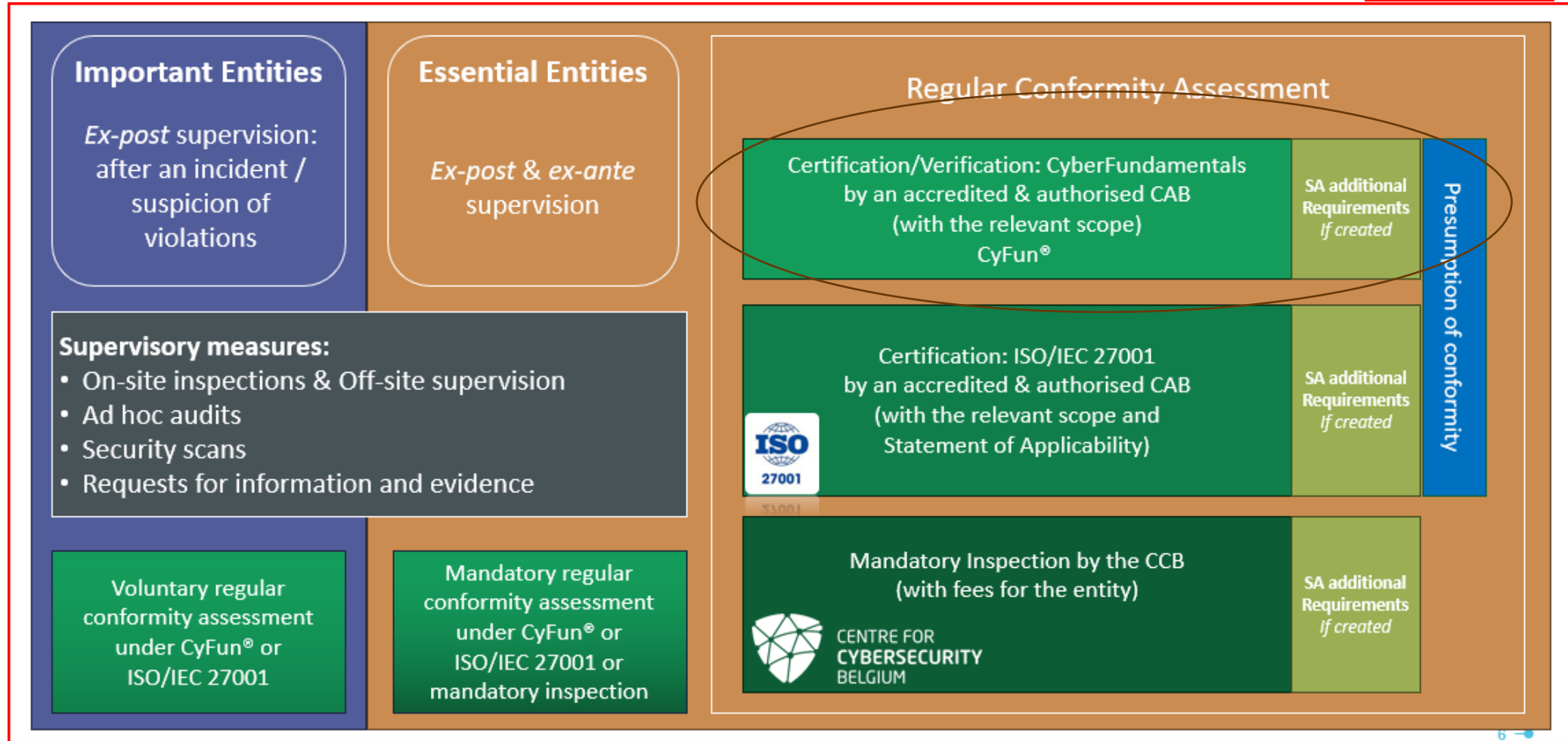
- NIS2 regulation will have a major impact on cybersecurity in EU and raises new challenge for the federal entities and for the audit function.
- FIA has been designated by the Royal Decree of 09 June 2024 as Conformity Assessment Body (CAB)
- An authorisation by CCB is required to perform the conformity assessments / verification audits of the federal entities.



TIMELINE OF NIS2

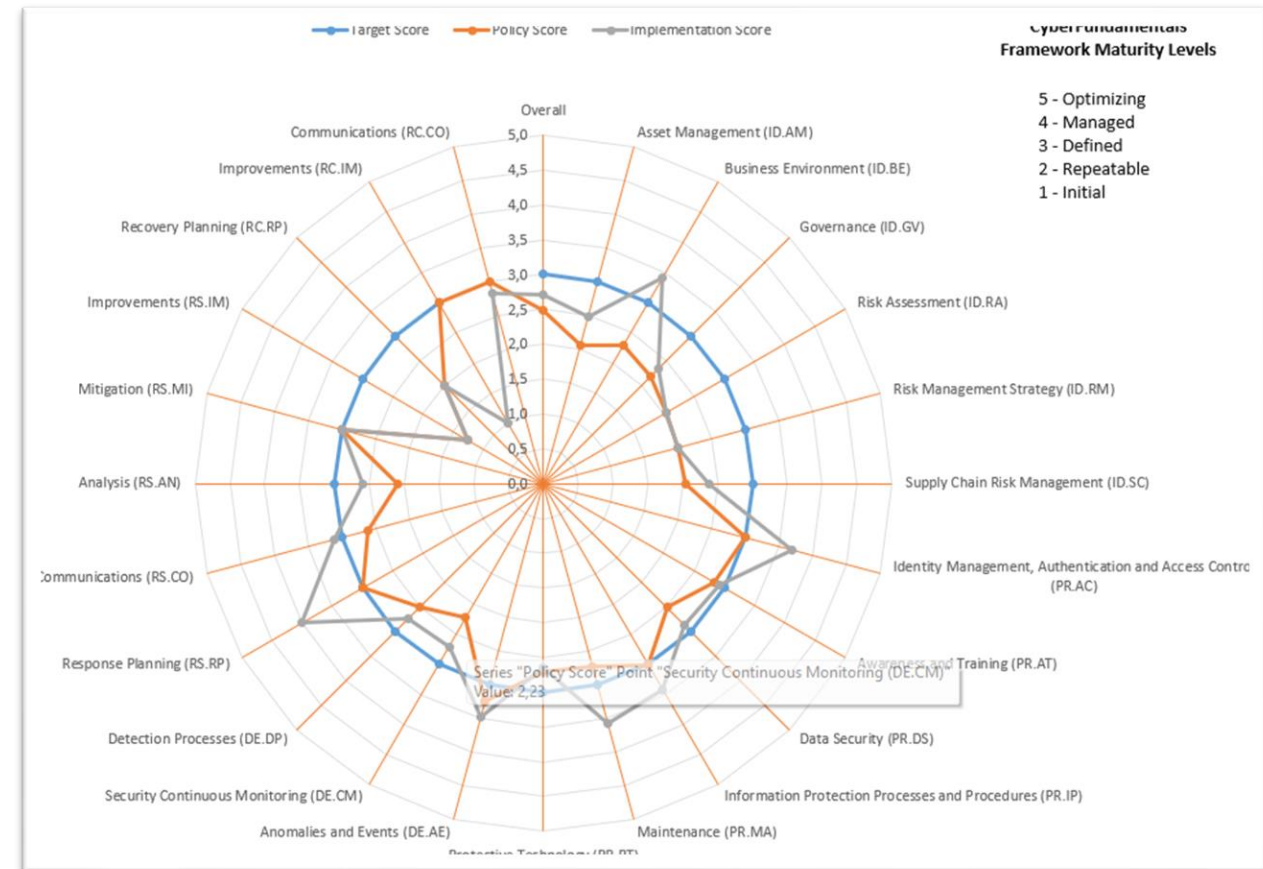
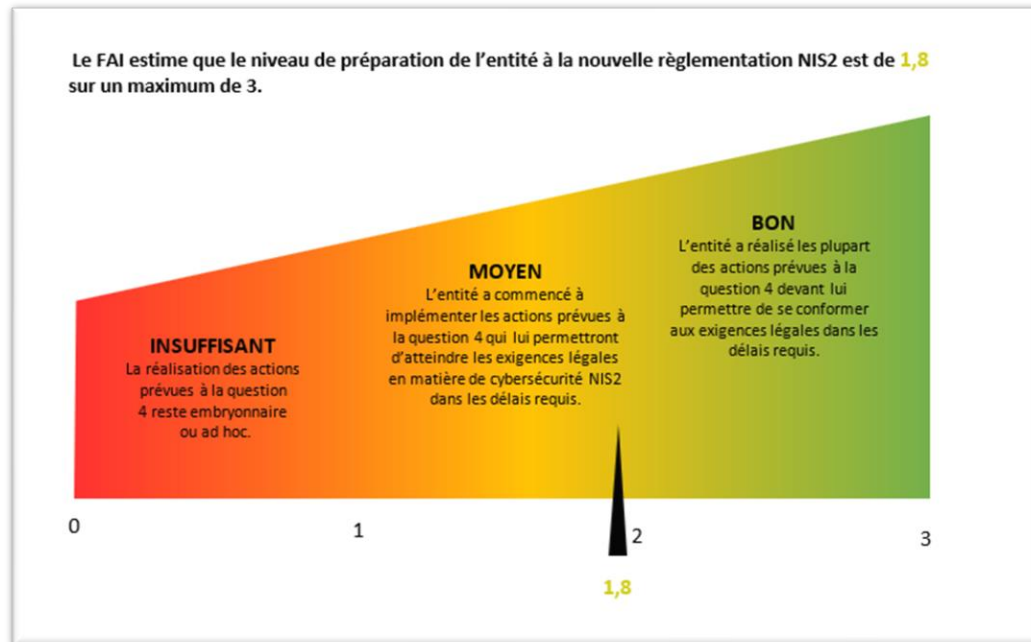


SUPERVISION OF NIS2 ENTITIES

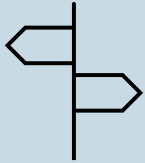


NIS2 IS COMING

FIA performed an audit on readiness of the federal entities in 2024 to evaluate the preparation of the NIS2 implementation.



CHALLENGES FOR THE AUDIT FUNCTION



Reshaping the way to approach the cybersecurity audits by taking over the role of Conformity Assessment Body



Audit function has to propose a governance structure aligned with the norms ISO17029 and 17021-1 based on the following principles:

- Impartiality
- Competence & Training



Need for more resources, training to upskill and reskill auditors, difficulties in recruiting and retaining Cybersecurity profiles



INTERNAL AUDIT METHODOLOGY



The **Cybersecurity Topical Requirements** edited by the International Professional Practices Framework (IPPF) of IIA provide an interesting guideline for the audit function.

Source: <https://www.theiia.org/en/standards/international-professional-practices-framework/>



What are the key elements of the Cybersecurity Topical Requirement?

Cybersecurity **Governance** – Clearly defined cybersecurity objectives and strategies that support organizational goals, policies and procedures, use of widely adopted frameworks (NIST, COBIT, and others), reporting and communication to the board.

Cybersecurity **Risk Management** – Established a risk management process to identify, analyze, manage, and monitor cyber threats, including a process to quickly escalate cyber risks.

Cybersecurity **Controls** – Established control processes that are evaluated periodically to mitigate cyber-related risks.



5 Governance Requirements:

- A. Policies and procedures.
- B. Roles and responsibilities.
- C. Board communication for objectives, strategy, risks, and controls.
- D. Engagement with stakeholders such as leadership, operations, and others.
- E. Resource requirements, including funding, talent, and technology are communicated.



What are the key elements of the Cybersecurity Topical Requirement?



9 Risk Management Requirements:

- A. Risk management process.
- B. Cross-functional risk management team.
- C. Policies and procedures.
- D. Team/individual identified for accountability.
- E. Escalation process.
- F. Coordination between IS, legal, compliance, and management.
- G. Third-party risk management.
- H. Data classification.
- I. Operation risk reporting process.

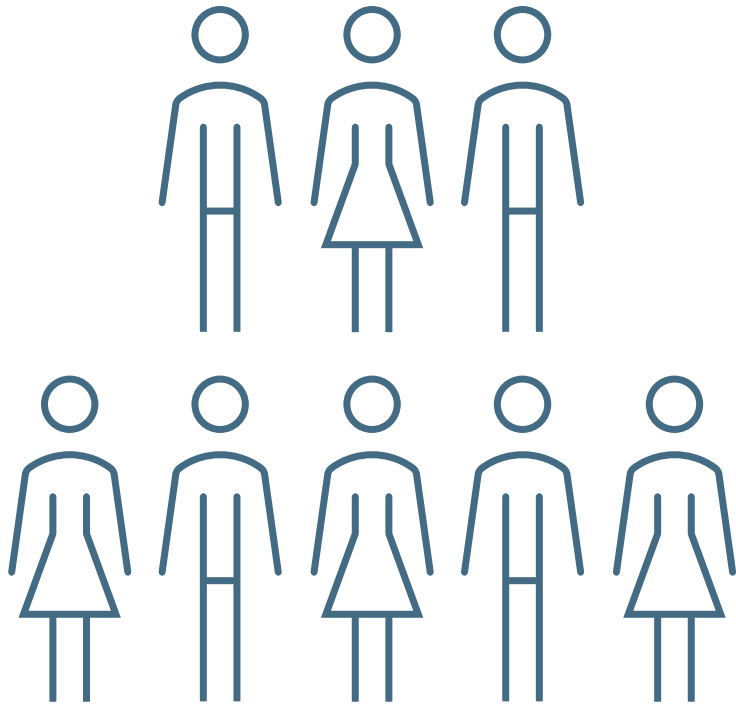
13 Control Process Requirements:



- A. Resource optimization.
- B. Promotion of objectives.
- C. Training.
- D. Policies and procedures.
- E. Emerging issue monitoring.
- F. SDLC.
- G. Hardware management.
- H. Patching and configuration.
- I. Network segmentation.
- J. Communications.
- K. Service delivery.
- L. Physical security.
- M. Incident response and recovery.



Conclusion



Let's work together!

Internal audit can help you to:

- ✓ Give insight in the relationship between cybersecurity and organizational risk.
- ✓ Prioritizing responses and control activities.
- ✓ Auditing for cybersecurity risk mitigation across all relevant facets of the organization
- ✓ Assurance in remediation activities.
- ✓ Raising risk awareness and coordinating with cybersecurity risk management
- ✓ Validating that cybersecurity provisions are included in the organization's business continuity plans and disaster recovery testing efforts.



Questions



Thank you for
your attention!

CONTACT

Kathleen Meganck



kathleen.meganck@audit.fed.be



0496/06.85.10

**Check our
website:
www.audit.fed.be**

ANNUAL
REPORT

