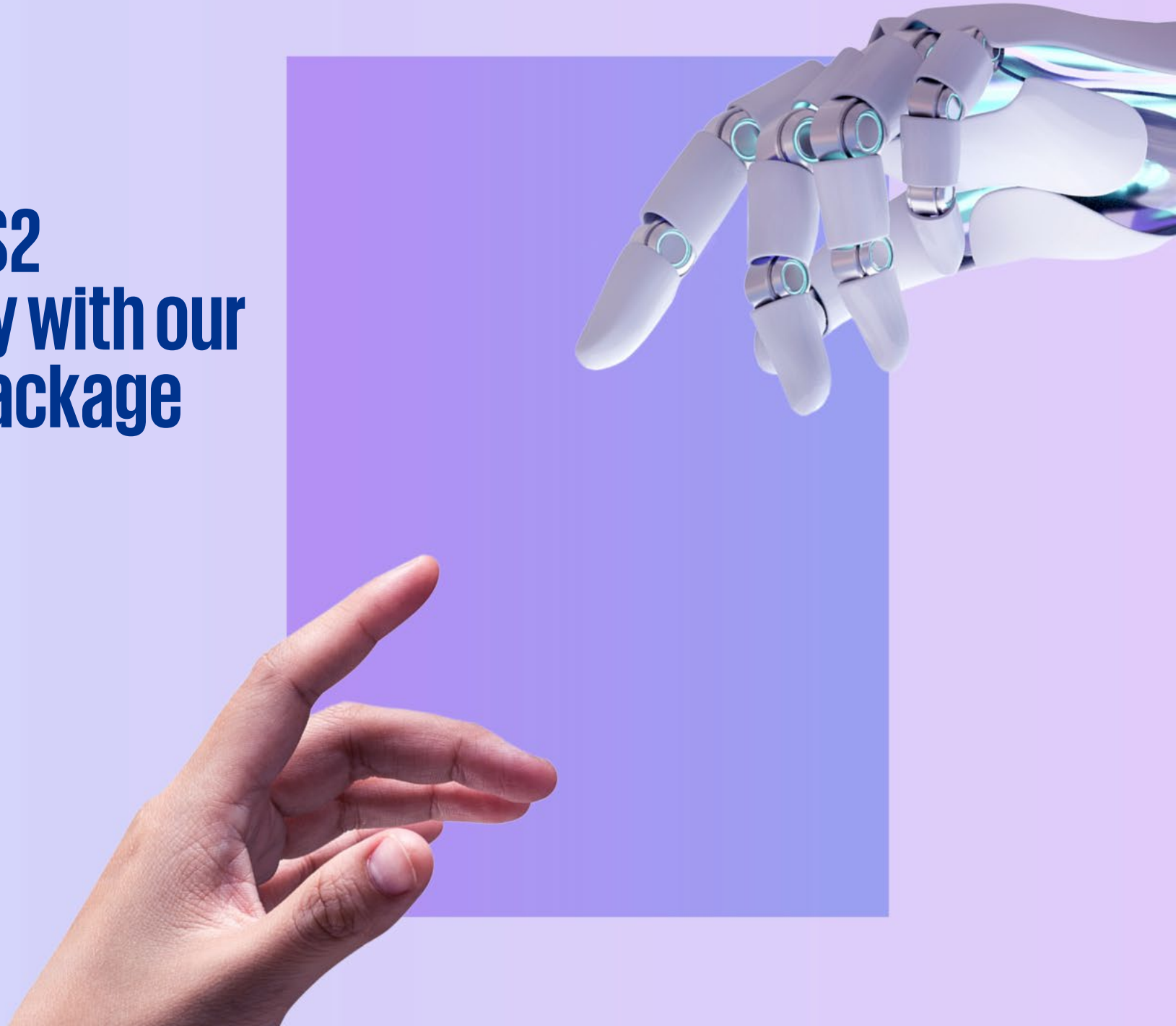




Accelerate your NIS2 compliance journey with our ServiceNow core package

KPMG Webinar

11th May 2026



Content

01 NIS2 Introduction

02 Challenges & Common Pitfalls

03 Proportionality

04 How can ServiceNow IRM support your NIS2 compliance journey

05 DEMO

01

NIS2 Introduction

NIS2 today is not a future obligation

Belgian Transposition of NIS2 Directive constitutes EU-wide cybersecurity legislation, providing legal measures aimed at elevating the collective cybersecurity standard within the EU.

NIS2 Compliance in Belgium

Cyber Fundamentals (CyFun)
Conformity Assessment by an accredited CAB



OR

ISO27001
ISO 27001 Certification by an accredited CAB

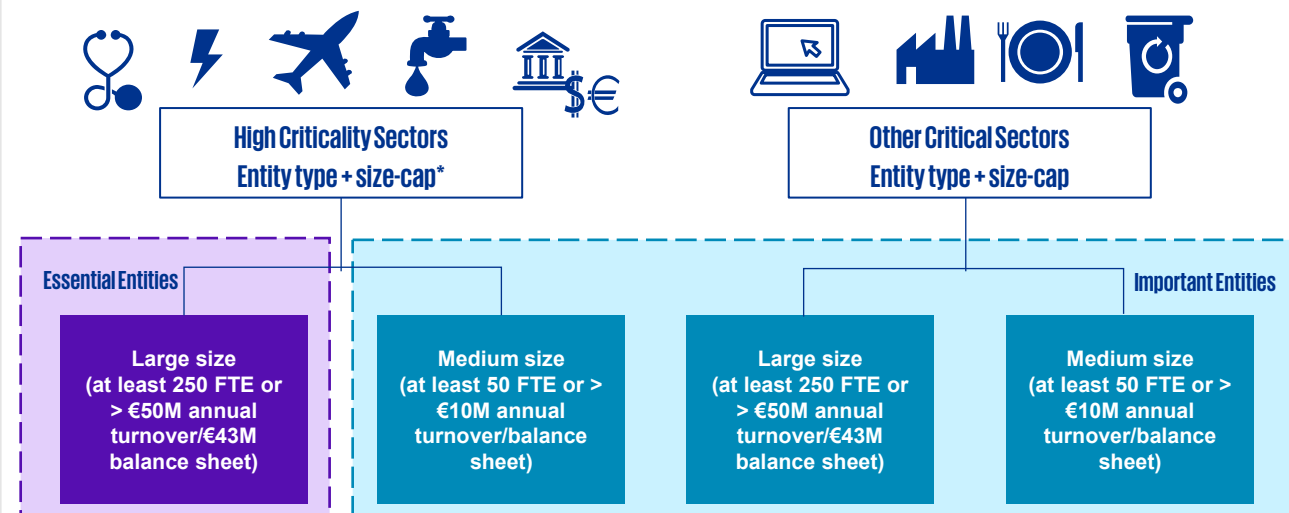


OR

Only for Essential entities: Inspection by CCB and/or equivalent by sectoral competent authority(ies). This is to be done using CCB's Cyber Fundamentals mainly.



Who is impacted?



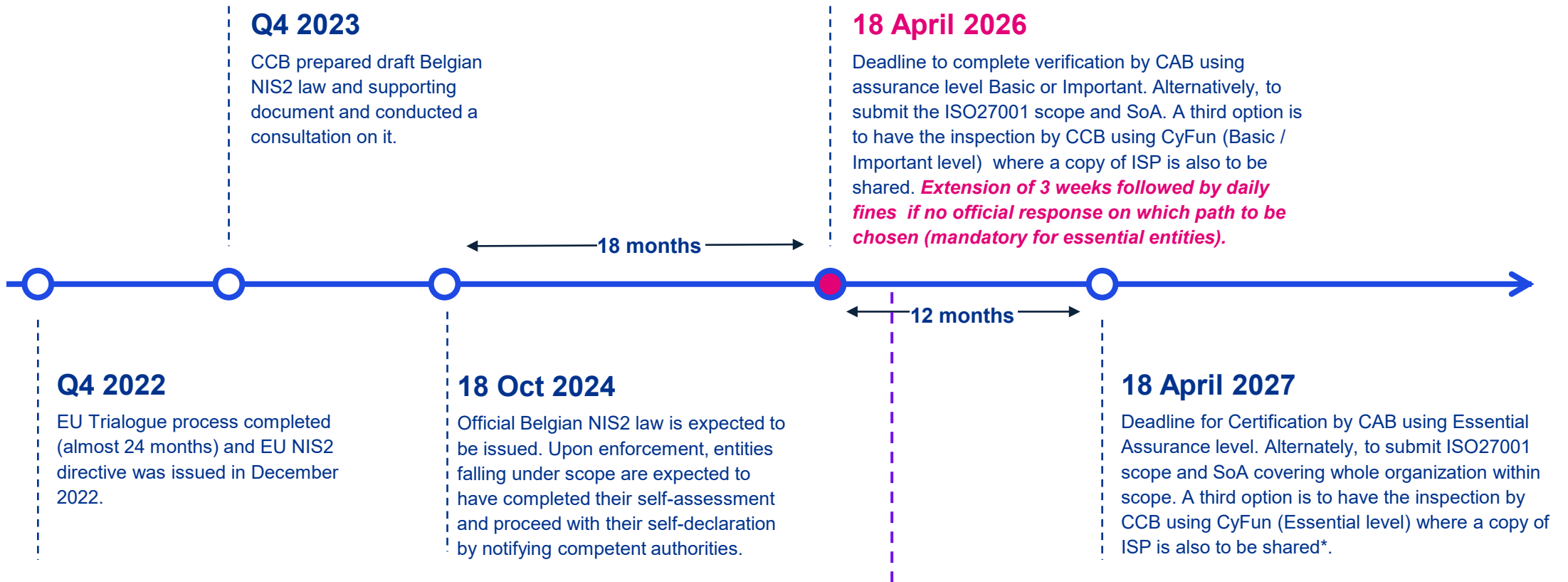
Compliance today means defensible readiness, not perfection

How to demonstrate compliance with NIS2 in Belgium?

Essential entities shall be mandated to submit conformity assessments to CCB whereas Important entities may submit it on voluntary basis:



Evolution of EU NIS2 Directive in Belgium



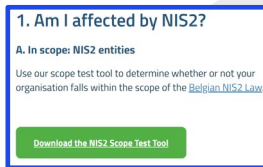
We are here!

NIS2 Journey of Compliance (for more organisations)

Implementation Challenge:
What is the span for each control in scope?

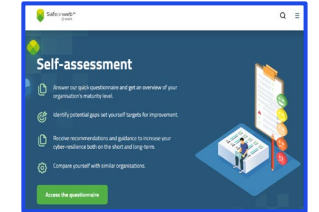
1. Am I impacted by NIS2 ?

- **CCB NIS2 Scope test tool:** determines if your organisation is in scope, based on answering set of questions.



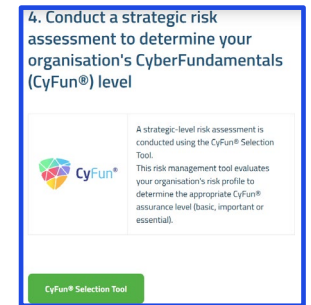
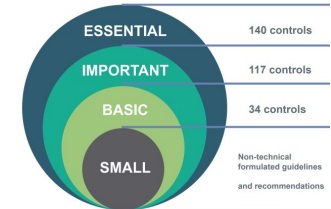
3. What is my current cyber maturity?

- **CyFun self assessment tool:** can be used to conduct a (self) gap assessment determining how far your entity is from compliance.



2. What is my designation level ?

- **CCB CyFun selection tool:** Based on perceived level of risk, this tool provides you with the answer to the right level of assurance to be targeted (e.g. Essential entities can comply with Important or Basic level controls). Needs rationale documentation and supporting evidence.



02

Challenges & Common Pitfalls

Where do organizations struggle today?



Unclear NIS2 scope definition and application



Fragmented ownership and unclear accountability model



Scattered compliance evidence across teams and tools



Securing resources from management



Lack of centralized visibility over NIS2 compliance status



Excel-based tracking is reaching its limits (manual Compliance work is done ad-hoc instead of regular)

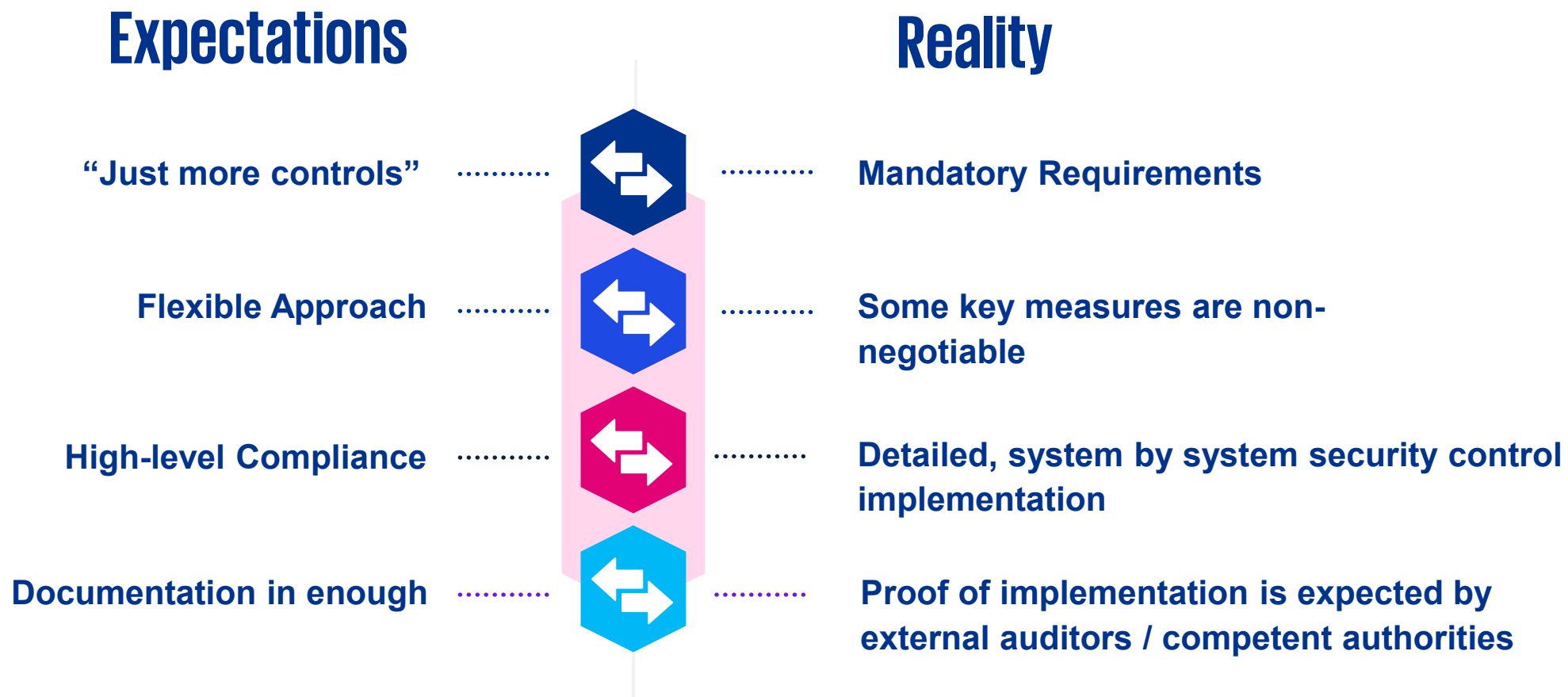


Risk of Paper Compliance (design and Implementation mismatch)



Finding the right balance (adequate risk assessment to weigh costs versus benefits)

Why NIS2 Feels Harder Than Expected



Common NIS2 Pitfalls We See

NIS2 introduces a more structured and demanding approach to cybersecurity and risk management. While many organizations already have security measures in place, the directive raises expectations by requiring consistent control application, system-level risk-based decisions, and demonstrable evidence of compliance.

What are the common NIS2 Pitfalls we see?

1. Using “low risk” to avoid applying controls

2. Treating proportionality to exclude controls

3. Not knowing your Crown Jewels (thus potentially not adequately protecting them)

4. Paper Compliance (generation of documentation without clear design structure nor solid proof of implementation)

5. Not knowing span of controls (i.e., What do they apply to in practice?)

6. Losing traceability between risk, controls and evidence

03

Proportionality

Principle of Proportionality: “Scope ≠ Depth”

NIS2 applies organisation-wide, but controls are not applied with the same depth everywhere

1. What “proportionality” means under NIS2

- Proportionality = risk-based tailoring, not optionality
- Baseline measures apply everywhere; any reduced/differentiated depth must be explicitly justified, documented, and evidenced (in the SoA).
- Requirements are normative: where a requirement applies, it must be implemented in full (as defined).

2. “Scope” (always broad)

- NIS2 scope covers the entire organisation, including IT & OT, business processes/services, data & supporting infrastructure, and critical third-party dependencies.

3. “Depth” (risk-based)

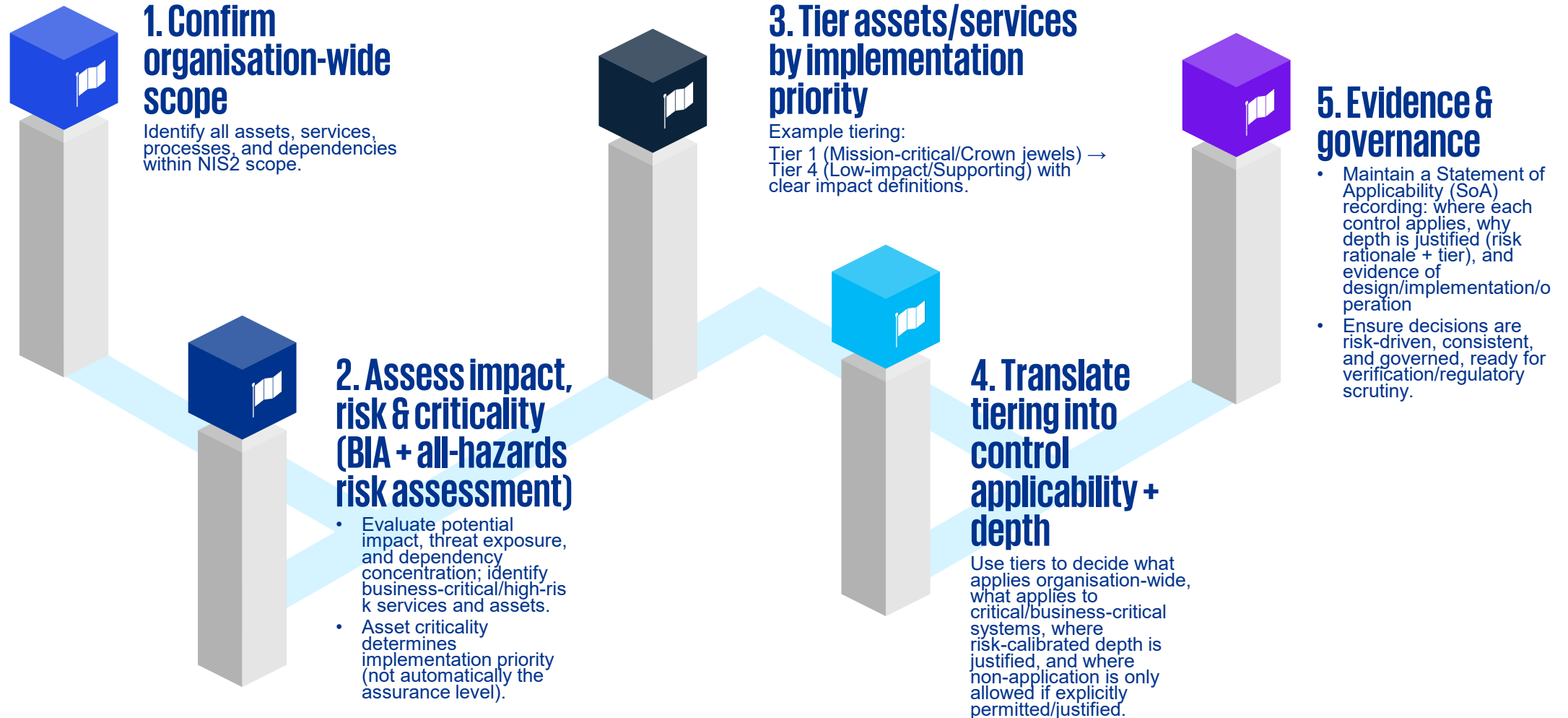
- Control depth must be appropriate to risk exposure and the potential impact of disruption—not “maximum effort everywhere”.

4. Non-negotiables (what you cannot “down-tier”)

- Mandatory baseline measures always apply: CyFun Key Measures apply organisation-wide and cannot be removed or downgraded once applicable.
- CyFun 2025 includes 218 total control requirements and defines Key Measures per assurance level: Basic (13), Important (9), Essential (7).
- CyFun layers are cumulative: Basic → Important → Essential (increasing rigour aligned to criticality/risk).

How to achieve proportionality (in the context of NIS2)

Common Pitfall: Treating proportionality to exclude controls or “use low risk to avoid applying controls”.



04

How can ServiceNow support your NIS2 compliance journey

Solving NIS2 Compliance challenges with GRC tooling

Automation

Reduces manual effort by automating repetitive tasks, enhancing efficiency, and minimizing human errors.

Reporting

Produces detailed, customizable reports with visual aids, allowing stakeholders to quickly grasp compliance outcomes and make informed decisions.

Accuracy and reliability

Improves the precision and consistency of audit results through standardized and algorithm-driven processes.

Collaboration

Supports teamwork through shared platforms and real-time updates, improving coordination and ensuring everyone stays aligned.

Centralized data

Aggregates all compliance-related information in one place, making data management easier and improving data integrity.

Security

Safeguards sensitive information with robust security features, preventing unauthorized access and data breaches.

Monitoring

Enables continuous oversight and real-time anomaly detection, helping to maintain compliance and address issues promptly.

Quality

Enhances the thoroughness and reliability of compliance activities by adhering to best practices, leading to more dependable and actionable insights.

ServiceNow Integrated Risk Management (IRM)

Starting with **ServiceNow's IRM module**, a robust solution for efficient risk and compliance management, centralizing processes, optimizing risk assessment, control implementation and compliance monitoring.

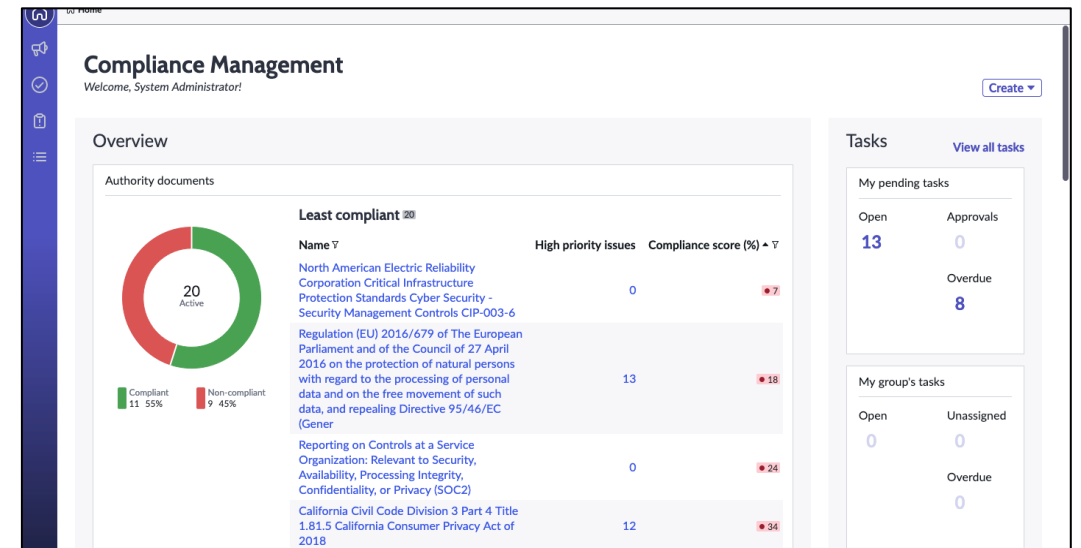
ServiceNow IRM

Risk
Management

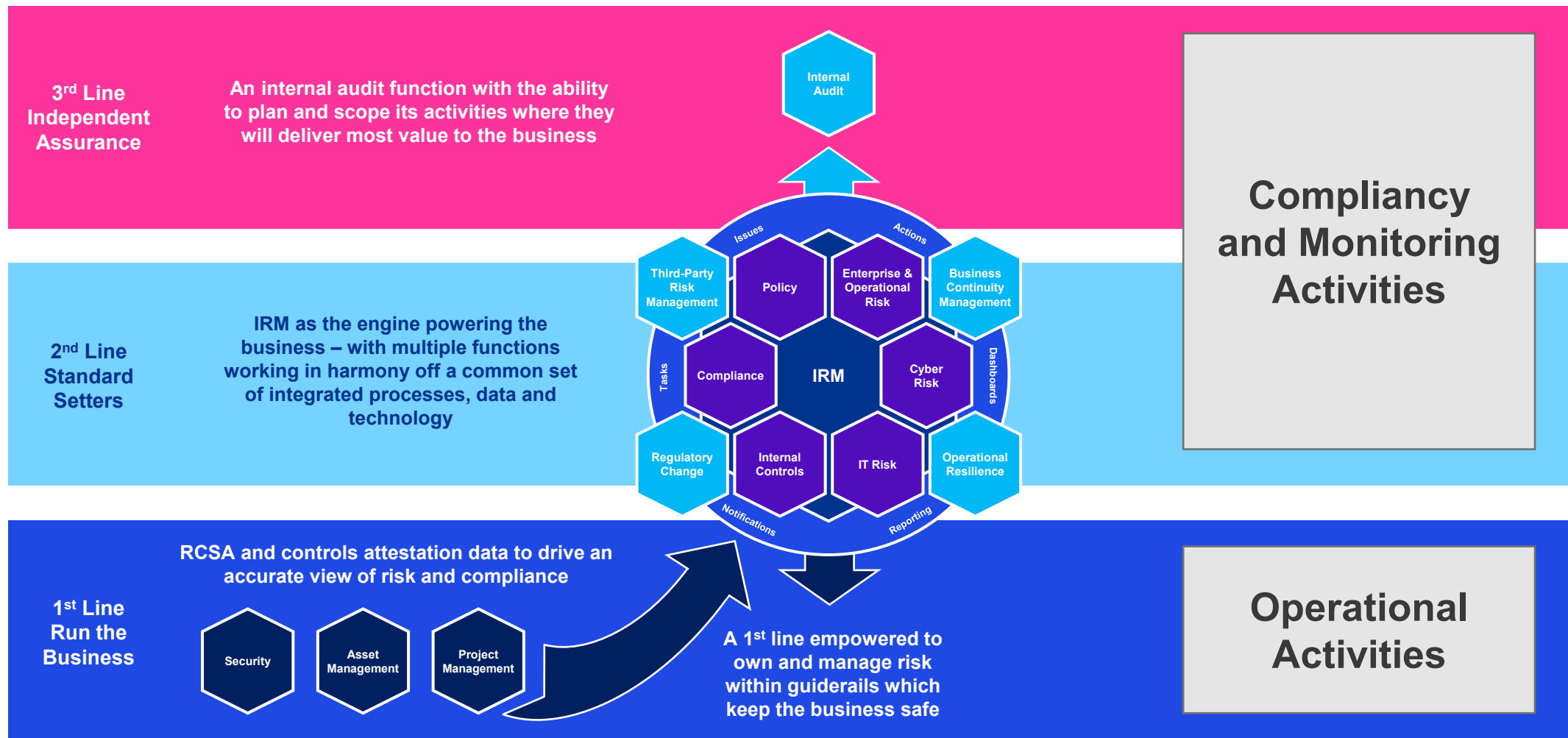
Policy &
Compliance

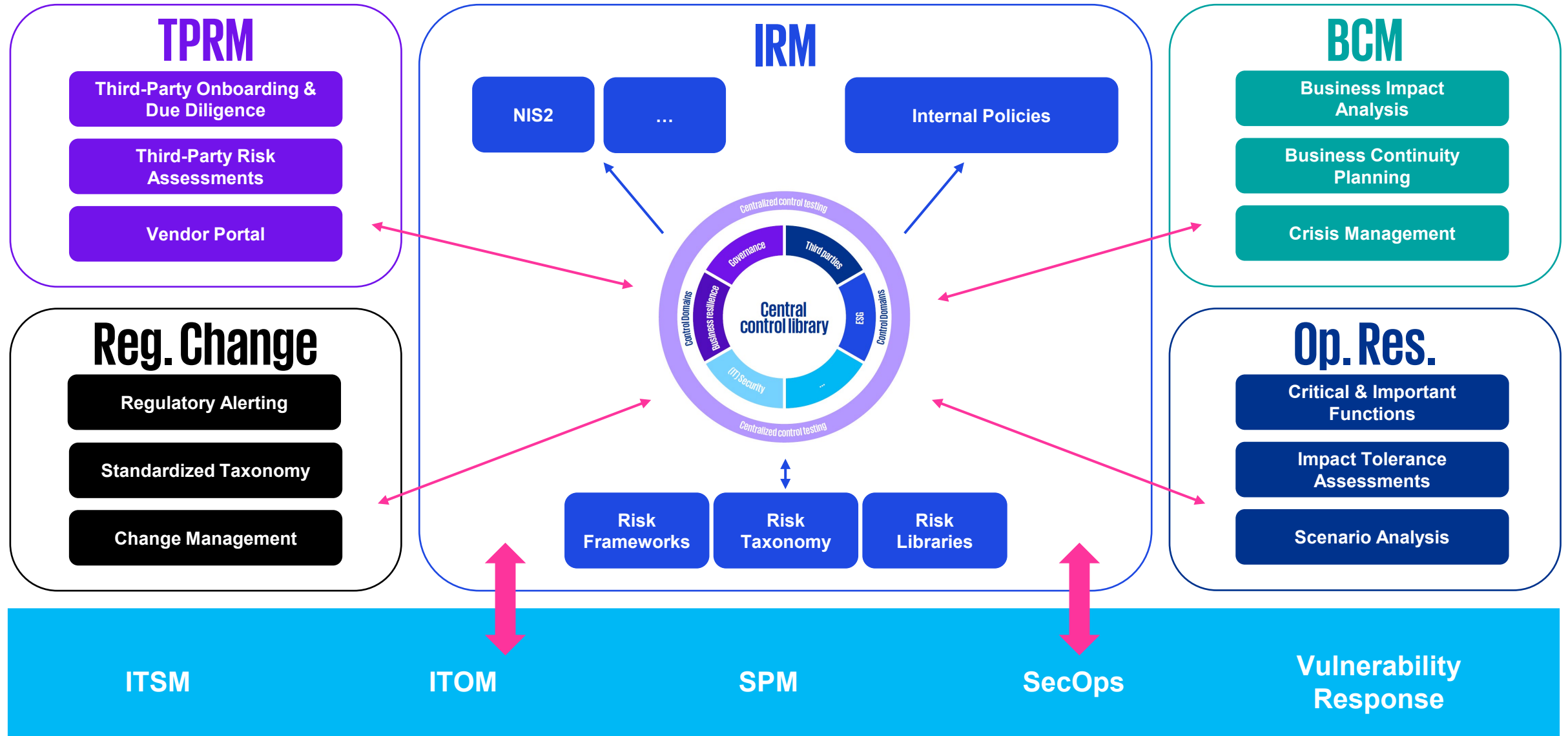
Incident
Management

Audit
Management



Compliance is managed across the 3 lines of defence





How can ServiceNow support your NIS2 Compliance journey?

Starting with **ServiceNow's IRM module**, a robust solution for efficient risk and compliance management, centralizing processes, optimizing risk assessment, control implementation and compliance monitoring.

ServiceNow IRM - Key Capabilities for NIS2



Centralized Compliance Repository supporting NIS2



Clear ownership and accountability for NIS2 controls and compliance activities



Clear identification and management of entities and assets



End-to-end traceability from NIS2 requirement to implemented control and supporting evidence



Structured support for incident management and regulatory reporting obligations



Regulatory reporting and real-time dashboards for NIS2 oversight

05

DEMO

Our Offering: ServiceNow IRM NIS2 Core Package

Our regulatory core packages enable clients with the essential functionalities to begin reporting and monitoring compliance with NIS2.

The NIS2 Core Package



By choosing ServiceNow IRM, compliance becomes simple and structured. The platform enables you to comply with NIS2 by implementing either the CyFun control framework or the ISO-based control framework, providing flexibility to meet Belgian regulatory expectations.

What is included?



Framework Selection (ISO or CyFun)



ServiceNow IRM Setup (set-up of NIS2 requirements, entities and controls)



ServiceNow IRM Trainings and Documentations

now

All Favorites History Workspaces

Compliance Workspace

Home

Compliance Management

Welcome, System Administrator!

Create

Overview

Authority documents

20

Active

Compliant

11 55%

Non-compliant

9 45%

Least compliant 20

Name	High priority issues	Compliance score (%)
North American Electric Reliability Corporation Critical Infrastructure Protection Standards Cyber Security - Security Management Controls CIP-003-6	0	7
Regulation (EU) 2016/679 of The European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (Gener	13	18
Reporting on Controls at a Service Organization: Relevant to Security, Availability, Processing Integrity, Confidentiality, or Privacy (SOC2)	0	24
California Civil Code Division 3 Part 4 Title 1.81.5 California Consumer Privacy Act of 2018	12	34

Tasks

View all tasks

My pending tasks

Open

13

Approvals

0

Overdue

8

My group's tasks

Open

0

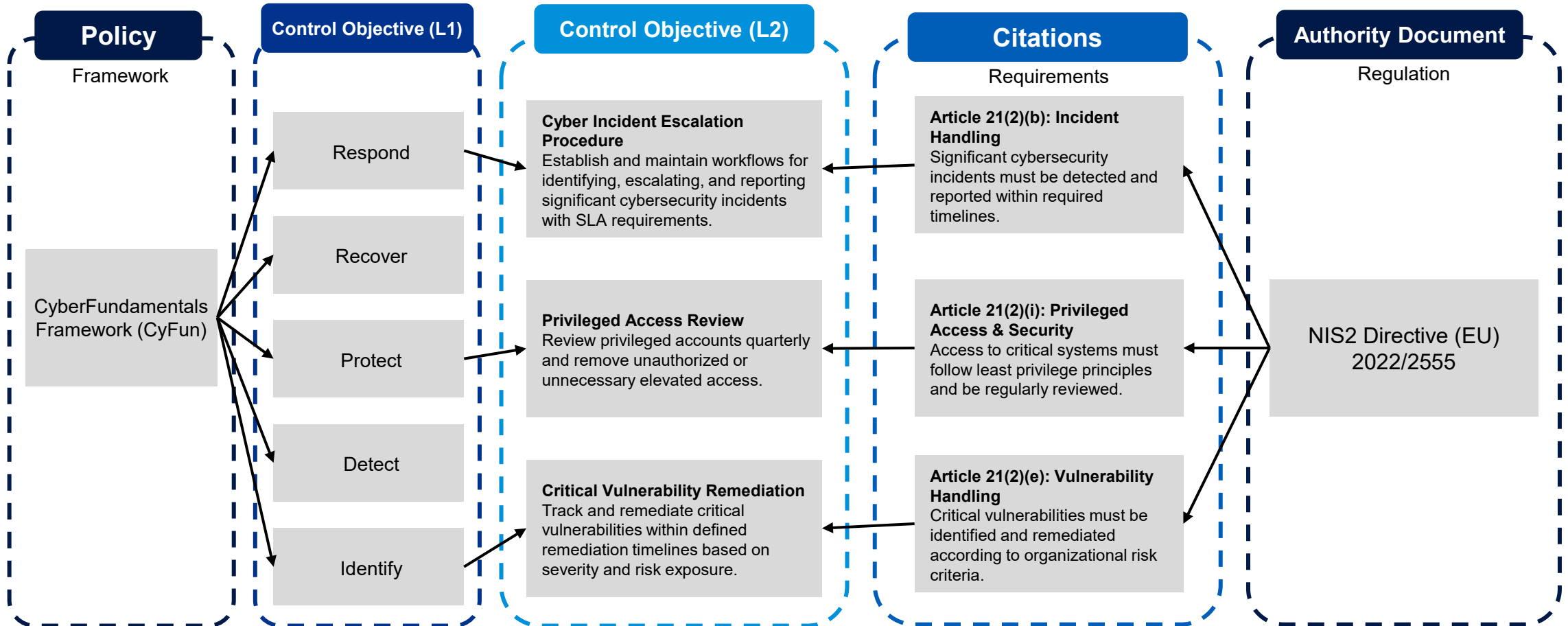
Unassigned

0

Overdue

0

DEMO Example



Our Key Takeaways

1.

Several activities can be carried out to **optimize level of investments** and mapping of applicable security controls to organisational processes and tools in scope of NIS2.

2.

KPMG can support you with your journey of NIS2 Compliance. From design elements to full fledge implementation while benefiting from the principle of **proportionality**.

3.

Great **synergies can be achieved** when working on **the same platform** and when using the same technologies.

4.

Significant efficiencies can be realized by **adopting well-established and harmonized processes across the full organization**.

5.

Control automation can significantly **decrease the organization's cost of control**.

6.

Don't start from scratch, but start from best practices, the out-of-the-box workflows and industry standards.

