

# NIS2 is here – are you prepared?

NIS2 is becoming a **major priority for industrial companies** – Dräger included. Across the sector, many are asking the same questions: What's in scope, what needs to change, and where do we start?

We've broken the topic down in a clear infographic to **support the industry with orientation and spark meaningful exchange**. Because leading the way in digital security also means moving forward together.



## What is NIS2? And who is affected?

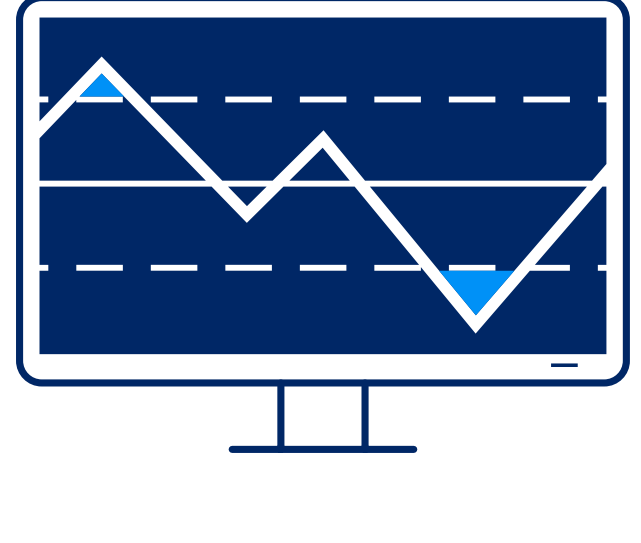
NIS2 is the **EU wide cybersecurity directive** that raises cyber resilience requirements for critical and important sectors. The directive applies to **organisations that are categorized as either “essential” or “important”**, spanning various sectors and are of medium size or larger, with at least 50 employees or an annual turnover exceeding €10 million.



Source: European Union

## What do companies need to do?

Companies in scope must **implement cybersecurity risk management** and be able to prevent, detect, respond to, and report significant incidents, with management accountable for oversight.



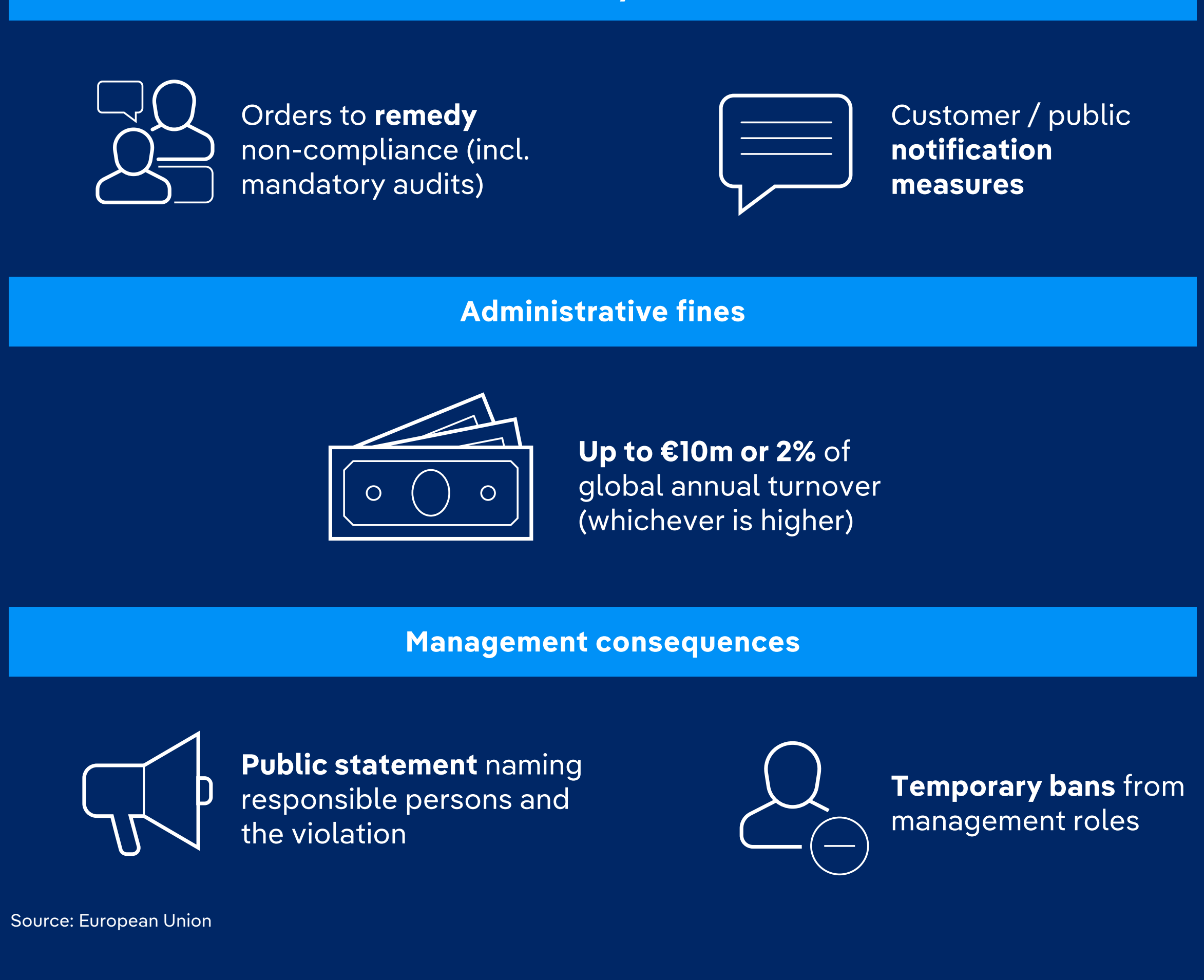
<b>Prevent</b>		Risk management measures, secure operations, access control, supplier security
<b>Detect</b>		Monitoring, vulnerability handling, testing
<b>Respond</b>		Incident handling processes, communication, escalation
<b>Recover</b>		Business continuity, backups, crisis management
<b>Report</b>		Regulatory incident reporting and post-incident documentation



Sources: European Commission, ENISA, European Union

## What are the consequences of non-compliance?

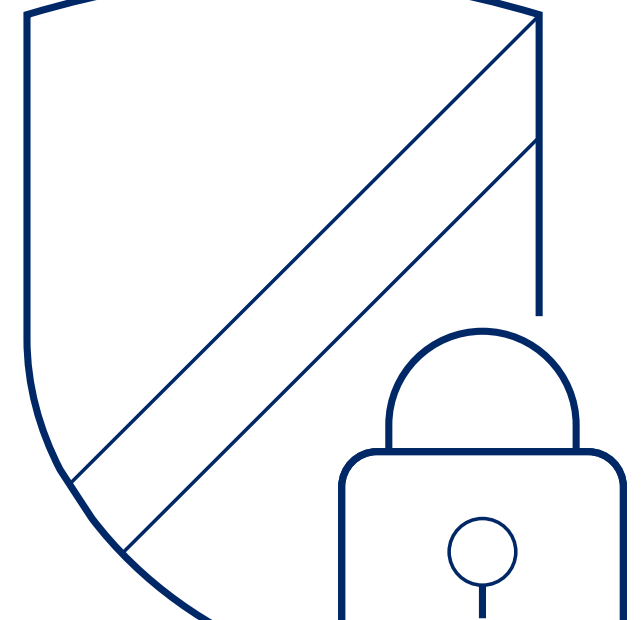
Non-compliance can **trigger regulatory orders and significant fines**, plus management-level measures.



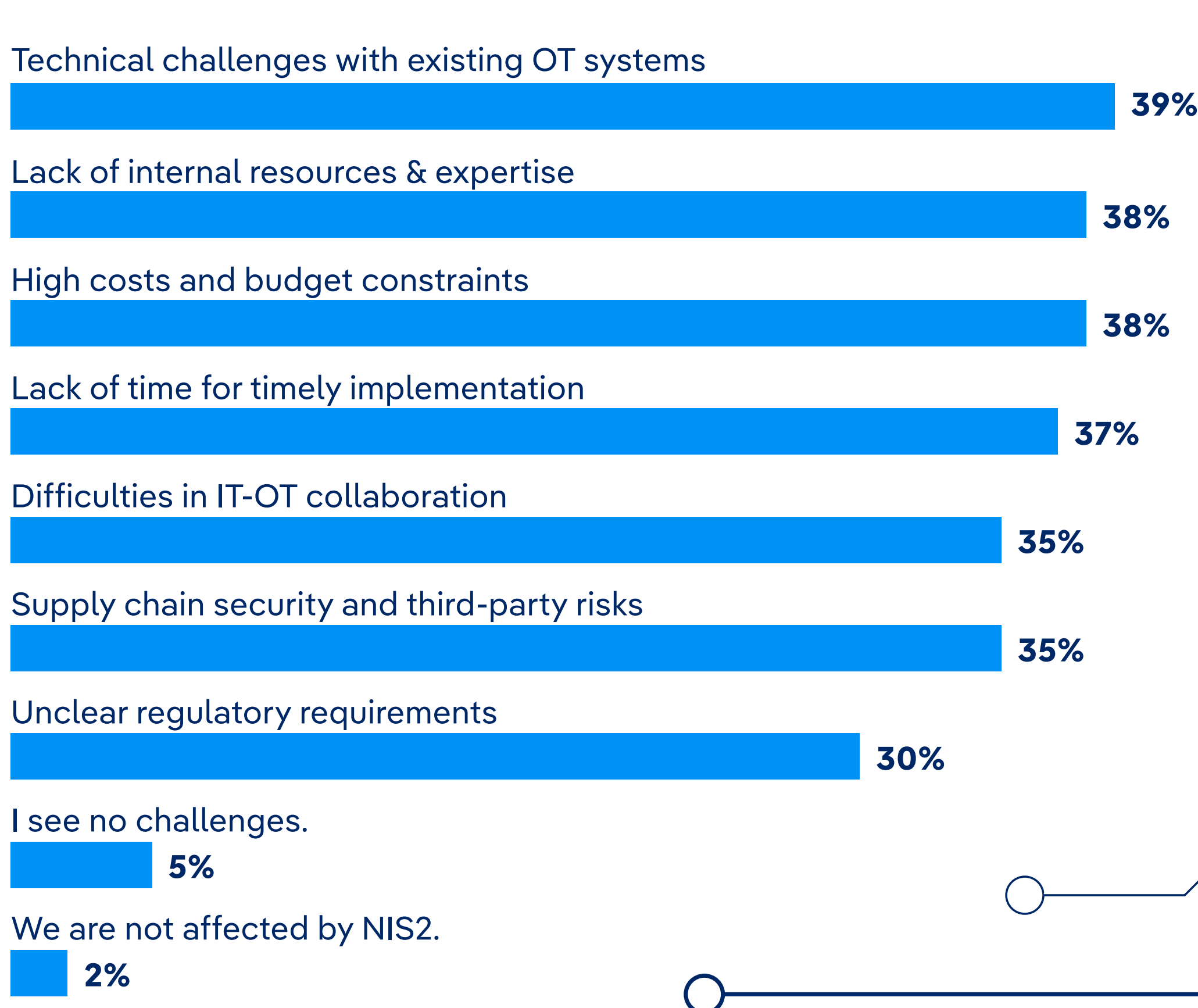
Source: European Union

## What hinders implementation?

According to our own Dräger survey conducted by Statista among decision-makers and employees in the OT-cybersecurity environment of industrial facilities, **only 5% of respondents see no challenges in the implementation of the directive**.



### What challenges do you face when implementing the NIS2 directive in your company?



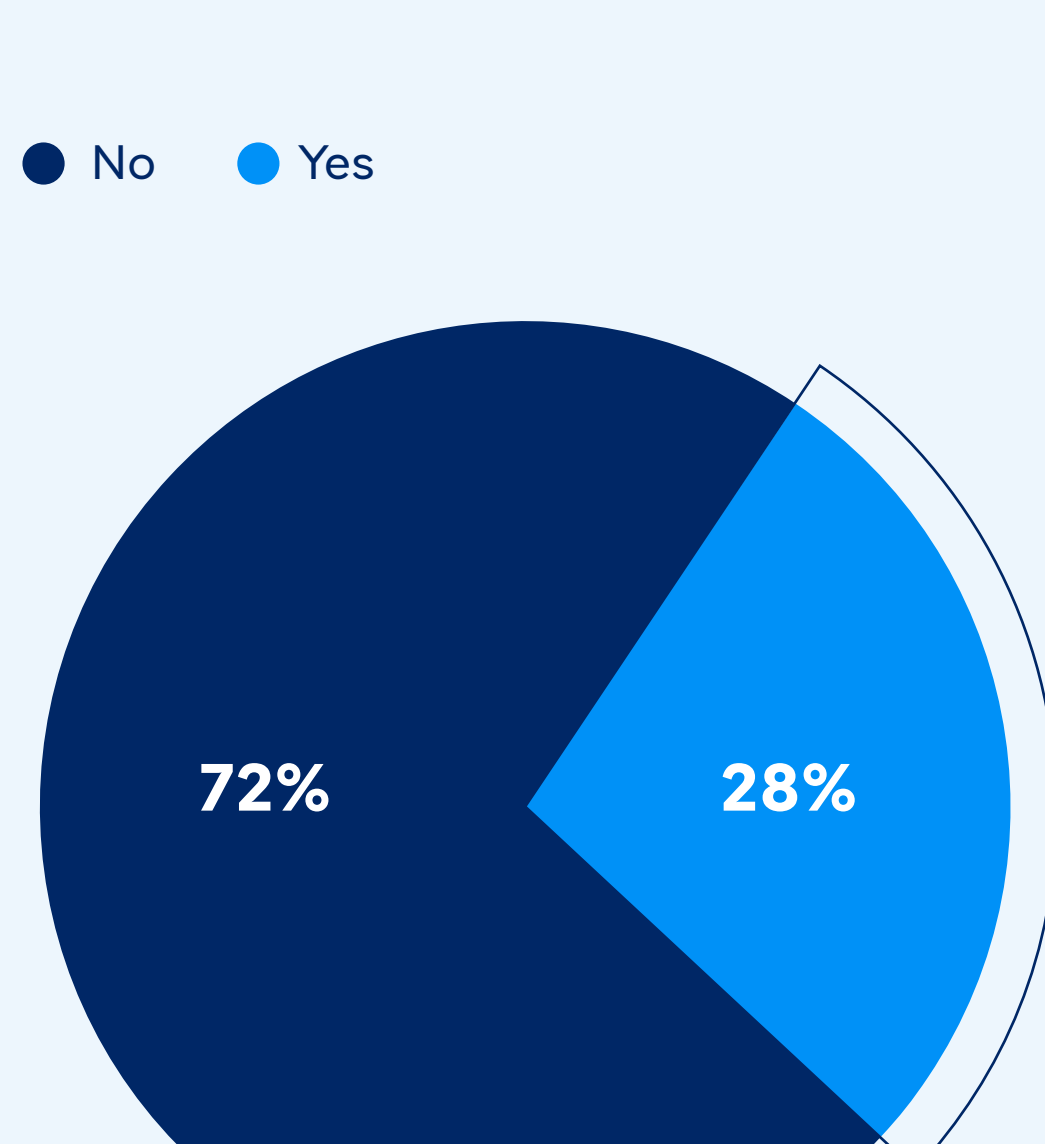
Source: Dräger Report “Securing the Weak Links – The Critical Role of Operational Technology”, 2025

## How has NIS2 affected the budget?

**By 2025, around three quarters of organisations did not have their own NIS2 budget**, while the rest has clearly established NIS2 and typically **reserved 5–15% of their cybersecurity budget** specifically for implementation and operation.

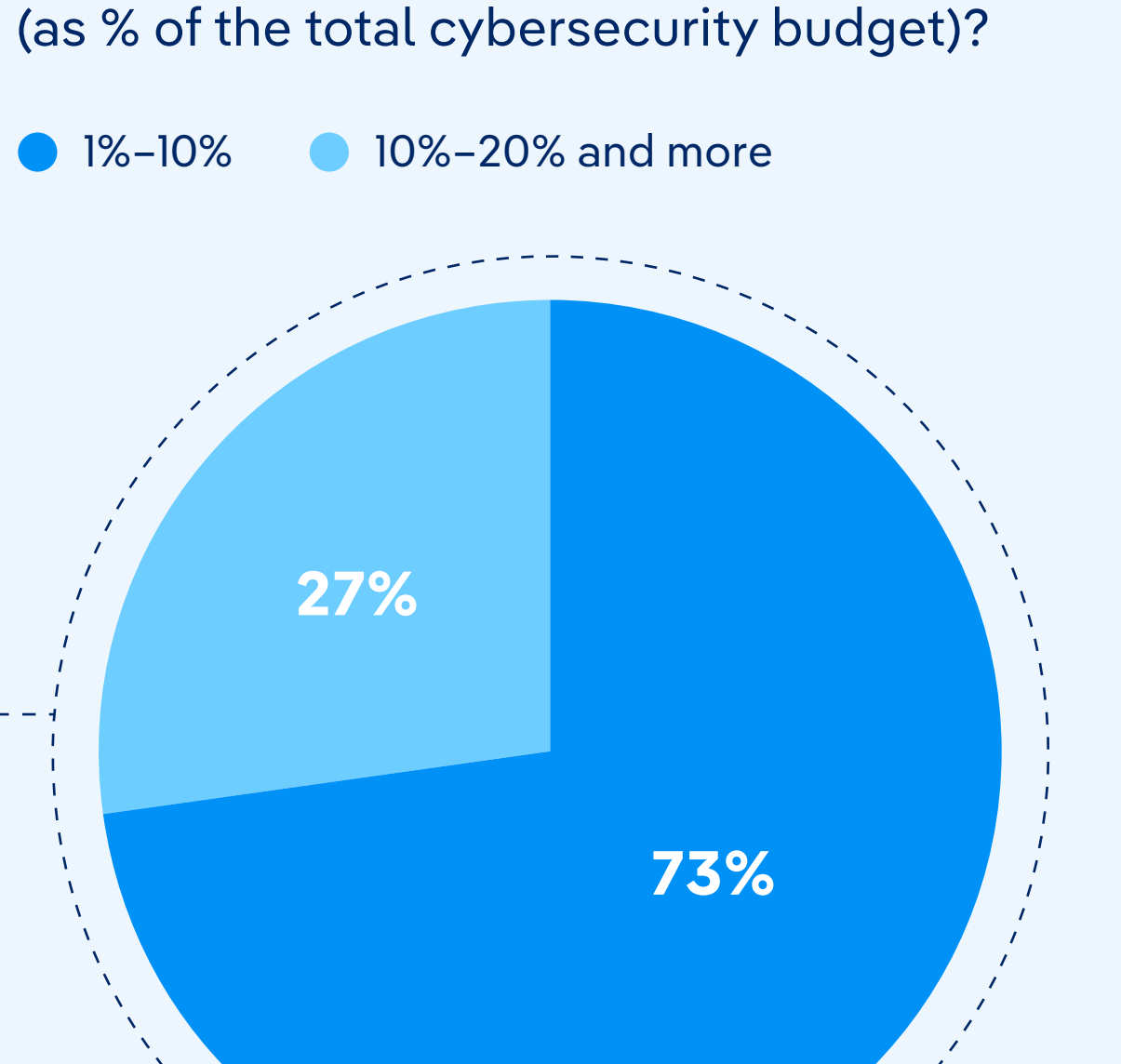
Do you have a dedicated budget for the NIS2 Implementation?

● No ● Yes



If yes, could you please indicate the financial value reserved for the NIS2 (as % of the total cybersecurity budget)?

● 1%–10% ● 10%–20% and more



Source: European Cyber Security Organisation (ECSO), 2025

## NIS2 readiness starts in the plant.

### Are you prepared?

Learn how we work with industrial teams and the community to strengthen digital security in industrial plants:

[draeger.com/industrial-cybersecurity](https://draeger.com/industrial-cybersecurity)