Projective GROUP

DORA
Are you ready?

ACTUALITÉ EVOLUTION RÉGLEMENTATION

01 février 2024

Imprimer Télécharger

Cybersécurité et risques informatiques : l'AMF appelle les acteurs à se préparer à l'entrée en application du règlement européen DORA

Le règlement européen sur la résilience opérationnelle numérique du secteur financier (*Digital Operational Resilience Act* ou DORA) établit des règles en matière de cybersécurité et de gestion des risques informatiques pour un grand nombre d'entités financières. Il entrera en application le 17 janvier 2025. Afin d'accompagner les professionnels dans l'application de ce texte, l'AMF en rappelle les principales dispositions, à un an de leur entrée en application.

Oversight of cyber risk

The European DORA regulation (the financial sector Digital Operational Resilience Act) adopted at the end of 2022 and effective from January 2025, aims to ensure that nearly all financial sector entities (including banks and insurers, administrators of critical benchmarks, service providers and crypto-asset issuers) put in place the necessary safeguards to mitigate risks linked to cyberattacks. DORA will also require all firms to:

1. implement measures to protect against all types of threat and disruption linked to information and communication technologies (ICT)
2. put in place a system for managing, classifying and reporting ICT-related incidents
3. in the case of systemic entities, regularly conduct advanced tests on ICT tools, systems and processes using threat-led penetration testing (or red teaming)

In addition, DORA will introduce a framework for the direct oversight by financial supervisors of critical service providers, including cloud service providers.

Projective GROUP

A few questions for you:

Do you have:

sufficient knowledge in
the field of cybersecurity?

Do you have:

an emergency procedure ready for the event of a ransomware attack?

Do you have

this procedure
available when all
systems are unavailable
due to the attack?

Are you:

Dependent on an IT provider or third-party system?

Do you have:

Clearly recorded agreements about availability with this party?

Do you have:

Monitoring set up to detect an incident in time?

Do you have:

Monitoring set up to detect an incident in time?

Have you:

Drawn up and executed a test plan on ICT in the past year, based on potential threats?

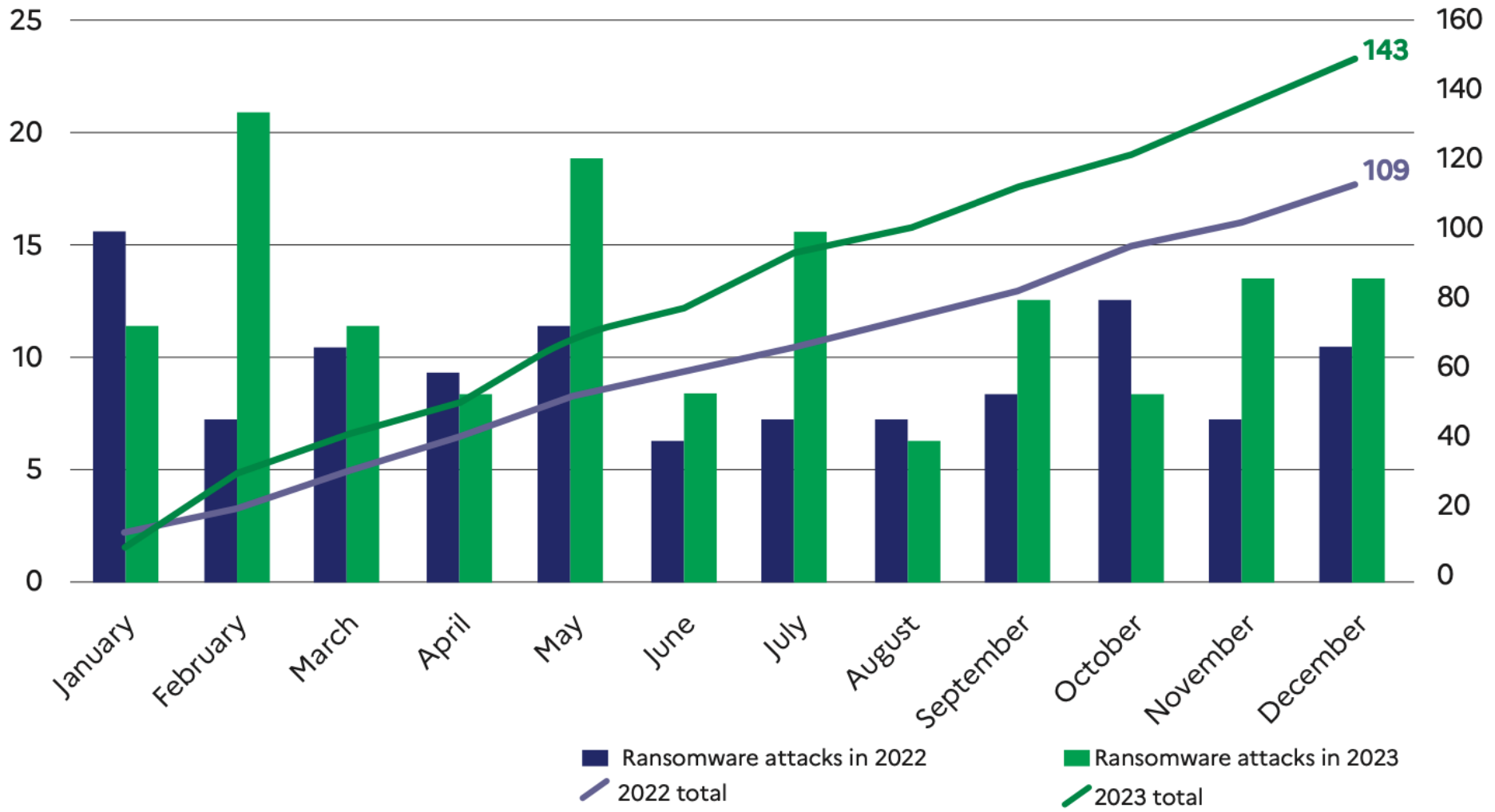
French state serv cyberattacks

Many ministerial services were ta adding the attacks 'are not curre

Le Monde with AFP
Published on March 11, 2024, at 11:43 pm (Pa

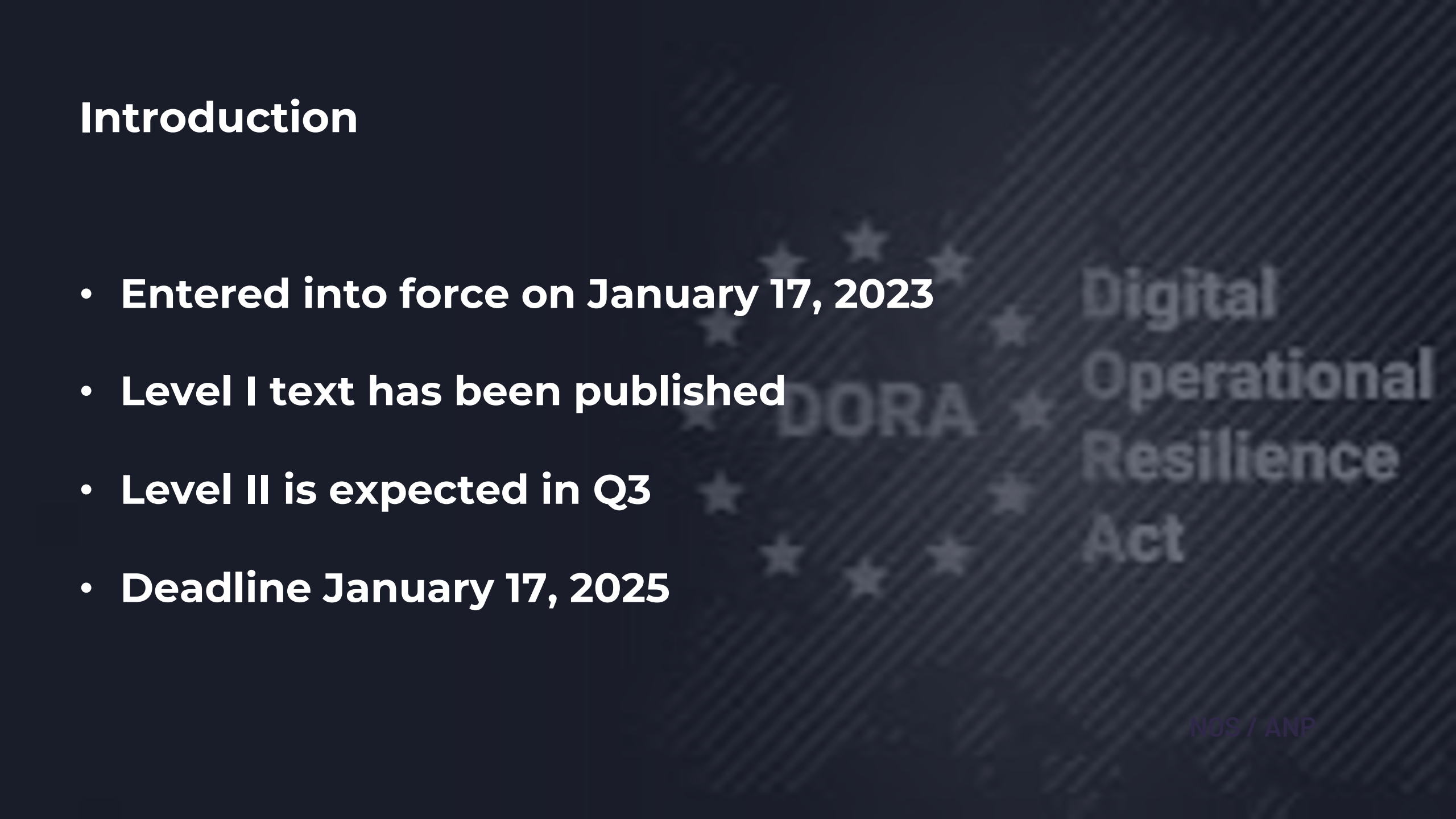
French Prime Minister Gabriel Attal at the M March 6, 2024. REMKO DE WAAL / AFP

→ Comparison of ransomware attacks reported in 2022 and 2023

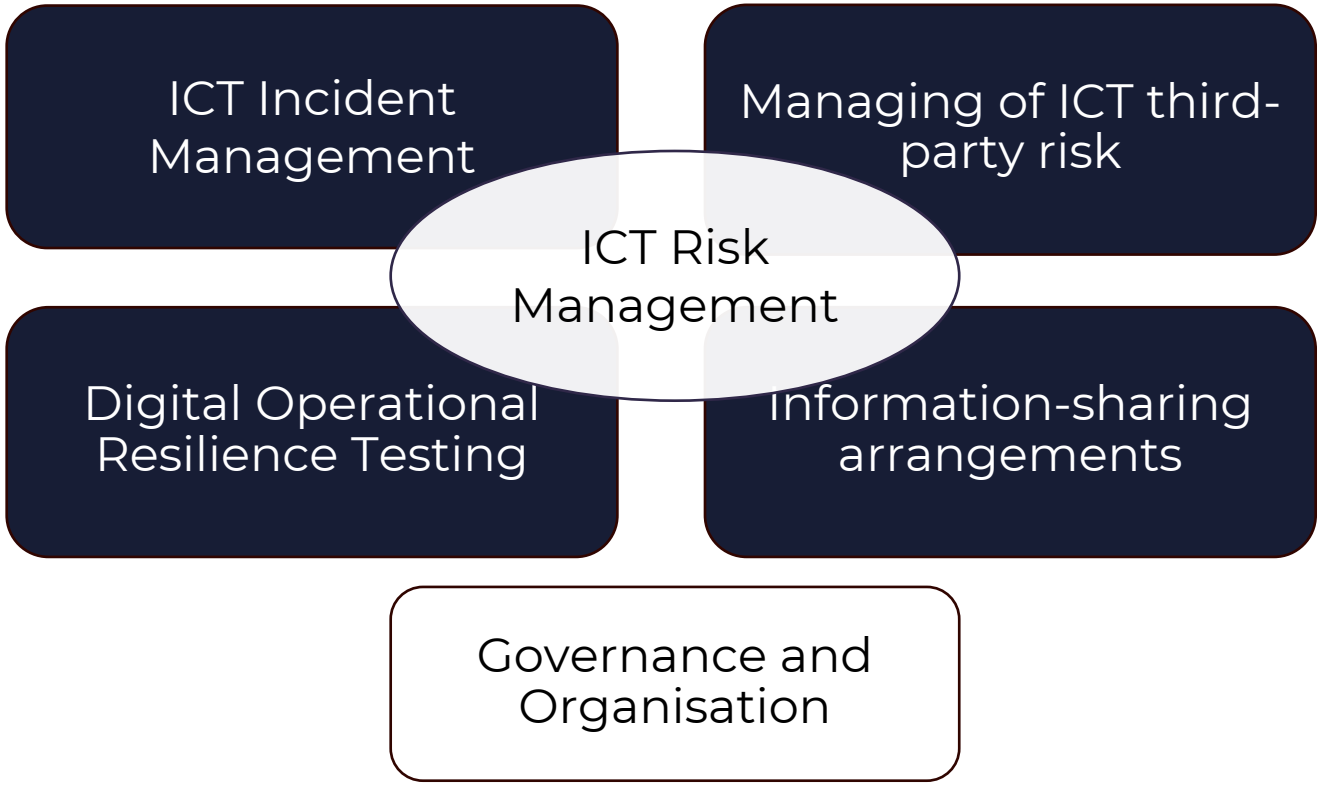


Introduction

- Entered into force on January 17, 2023
- Level I text has been published
- Level II is expected in Q3
- Deadline January 17, 2025



DORA - Overview



DORA

Managing of ICT third-party risk

DORA

ICT outsourced and dependent from partners

Unclear agreements, poor reporting

This is how DORA solves it

- Manage third-party risk
- Distinction between critical and important partners
- Mandatory contractual provisions

DORA

ICT Incident Management

This is how DORA solves it:

- Classify and record incidents
- Expansion of existing obligations
- Decision tree
- Report to supervisor and customers

Projective GROUP

DORA
Are you ready?

Action plan

- Gap analysis
- Project organisation
- Implementation
- Record and monitor

Projective GROUP

Time for action!

267 days to go

Projective GROUP

Questions?
Visit us at le Salon

www.projectivegroup.com