NIS 2: Tutti parlano della direttiva, ma l'hai letta?

NOI L'ABBIAMO LETTA!

Alessandro ROSSI
CEO Advens Italy

Advens
Security for the greater good

Agenda

About Advens

NIS 2 in a nutshell

What can you expect from NIS 2?

What will NIS 2 require from you?

And now?

About Advens

Let’s get to know each other

©Pierre Bouras / TR Racing

Advens
Security for the greater good

About us

- ✓ European **pure-player cybersecurity** leader
- ✓ Born in France, **24 years ago, now in Italy, Spain, Germany**
- ✓ **500+** experts
- ✓ **360° expertise** from strategy to secops, from compliance to ethical hacking, from architecture to CERT
- ✓ mySOC : best-in-class **SOC-as-a-service**

Advens is more than cybersecurity

Our mission to protect is what drives us, every single day. But it goes beyond that.

Up against urgent social and environmental issues, making our performance accessible to those who need it has always been our goal.

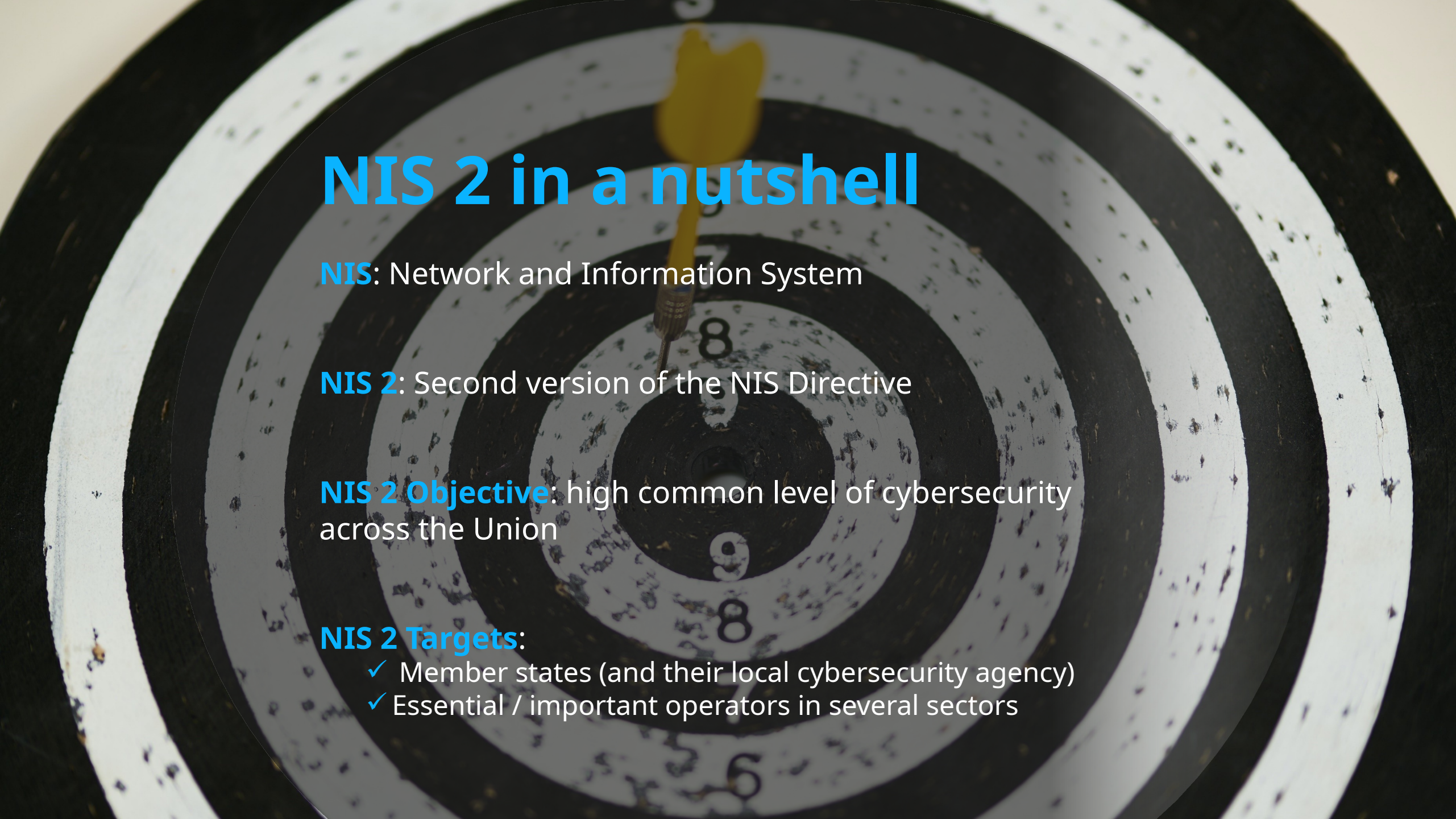
And to finance it all, we redistribute up to 50% of our financial value to **Advens for People & Planet**.

This **endowment fund** supports high-impact initiatives promoting social inclusion, education for the younger generations and environmental protection.

NIS 2 in a nutshell

But we're pretty sure you already know all of it!

Gdvens
Security for the greater good



NIS 2 in a nutshell

NIS: Network and Information System

NIS 2: Second version of the NIS Directive

NIS 2 Objective: high common level of cybersecurity across the Union

NIS 2 Targets:

- ✓ Member states (and their local cybersecurity agency)
- ✓ Essential / important operators in several sectors

A brief history of NIS2 Directive

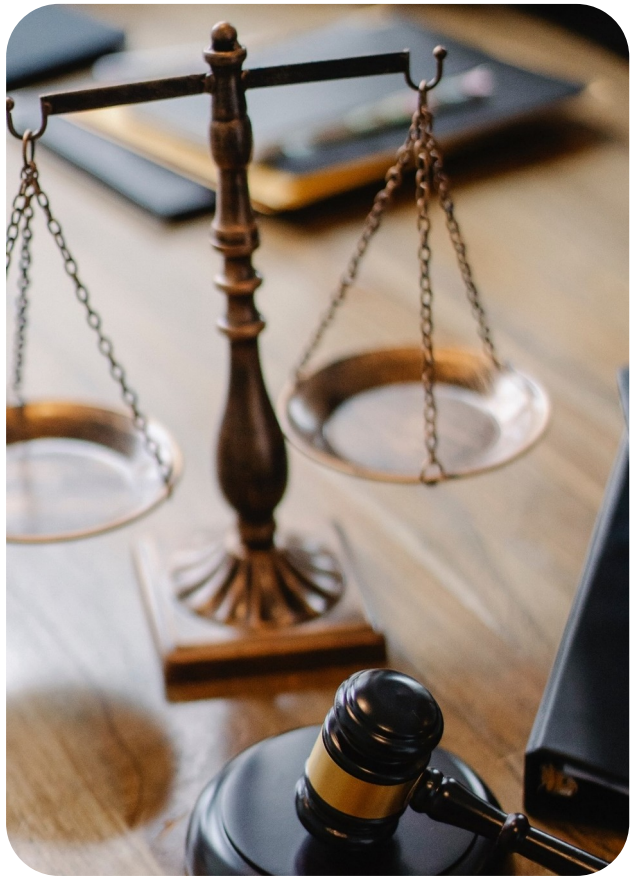
A strengthening of NIS 1

- Abrogation of Directive NIS 1 in favor of Directive NIS 2, which covers more areas
- Objective of this text: to ensure a high common level of security of networks and information systems in the European Union

Deadlines

- December 14, 2022: adoption of the Directive
- **October 17, 2024** at the latest: transposition of the Directive in all Member States

What is a directive?



A "directive" is a legislative act that sets out a goal that **EU countries must achieve** (UE Dir. 2022/2555)

However, it is up to the individual countries to **devise their own laws** on how to reach these goals.

It is not as “powerful” as a Regulation (GDPR) and it only applies to member states.

https://european-union.europa.eu/institutions-law-budget/law/types-legislation_en#:~:text=Directives,how%20to%20reach%20these%20goals

.

From Europe to my country

Each member state must work on a **local transposition** of a directive. It will create / update local law to ensure the country reach goals defined in the directive.

For cybersecurity related regulation, **European and national agencies** are involved.

enisa
EUROPEAN UNION AGENCY FOR CYBERSECURITY

Bundesamt für Sicherheit in der Informationstechnik

AGENCE NATIONALE DE LA SÉCURITÉ DES SYSTÈMES D'INFORMATION
ANSSI

AGENZIA PER LA CYBERSICUREZZA NAZIONALE
ACN
SAPIENTIA ADIUVAT

CCN
centro criptológico nacional

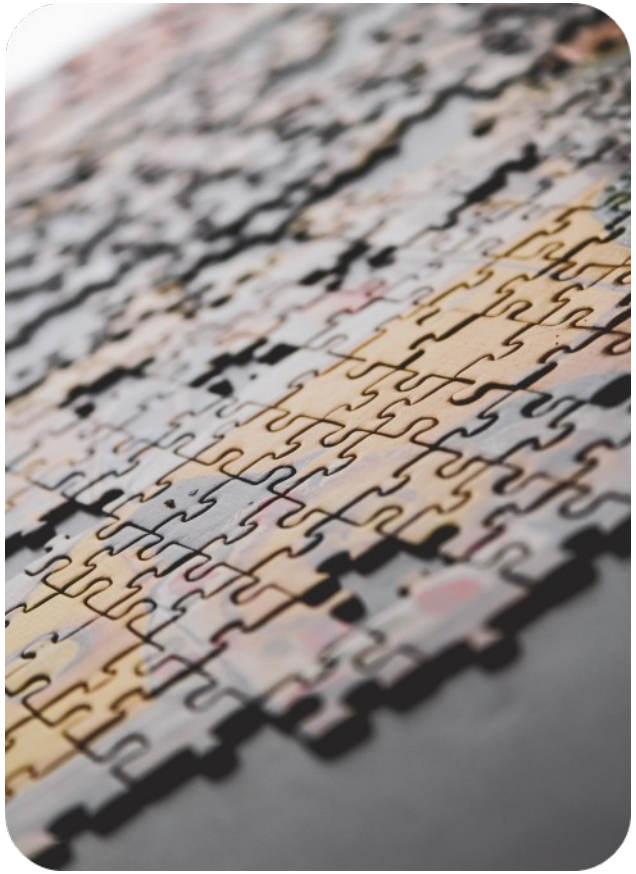
https://digital-strategy.ec.europa.eu/en/policies/nis-transposition

What can you expect from NIS 2?

It's not only about you having to work... It's about improving cybersecurity in Europe !

Security for the greater good

Consistent pan-European cybersecurity strategy



Goal : Require each Member State to maintain a high level of cybersecurity on its territory

— Adopt a national cybersecurity strategy

— Designate or establish one or more competent authorities responsible for cybersecurity (ACN in Italy)

— Adopt a national large-scale cybersecurity incident and crisis response plan

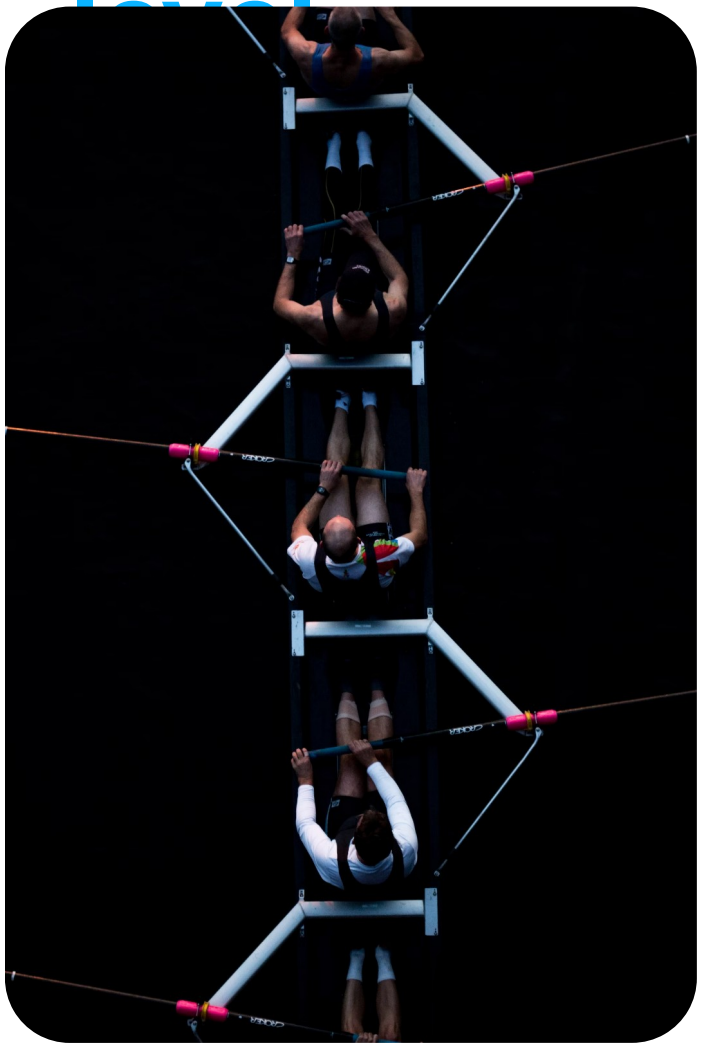
Focus on CSIRT

Designate or establish one or more CSIRTs

- Monitor cyber threats
- Alert on potential vulnerabilities
- Assist entities affected (ex: to carry out a proactive scan of their network if they request it)
- Coordinate vulnerability disclosure (one can signal a vulnerability to a CSIRT and the CSIRT will be in charge of contact the vulnerable entity)

Ask ENISA to develop and maintain a **European vulnerability database**

Cooperation at union and international level



Create a Cooperation Group composed of representatives of Member States, the Commission and ENISA

- Provide guidance to the competent authorities
- Exchange best practices
- Carry out coordinated security risk assessments of critical supply chain

Establish a network of CSIRT

- Focus on assistance in addressing cross-border incident

Establish the **European cyber crisis liaison organisation network** (EU-CyCLONe)

- Increase the level of preparedness of the management of large-scale cybersecurity incidents and crises
- Assess impact of such crises
- Coordinate the management of large-scale cybersecurity incidents and crises

What will NIS 2 require from you?

It's time to get prepared for a long To do list...

Security for the greater good

Know who you are!

Everyone is presumed to know the law… and It is your responsibility to find out if NIS 2 applies to your organization ….

- *Following the establishment of the Agency for National Cybersecurity (ACN) by d.l. 2021/82 in June 2021 and the subsequent handover of competencies in June 2022, the "Competent Authority" for all NIS sectors (NIS-1, and NIS-2 upon transposition of the new Directive) and the single point of contact is ACN, The role is thus one of identification, regulation and inspection*

- The "sector table" will be extended to all new entities falling under NIS-2 in which ACN also participates in the exercise of its functions

- **ACN participates in the NIS cooperation group (NISCG) at the European level**

- **Italian criteria (L. n. 15, 21/02/24):** government delegation to:

  - → Select and exclude companies and institutions in scope
  - → Establish and develop a national CERT and CERT network
  - → Register essential and important national players
  - → Select and verify the adoption of necessary technologies and solution
  - → Refine and better define the area of responsibility of ACN
  - → Define a system of penalties and fines

….. so stay tuned to know if our activity in the list of critical sectors defined in annex I and II of the directive !

Point of contact

Our local competent authority or the national CERT may contact you about a vulnerability on of your systems…

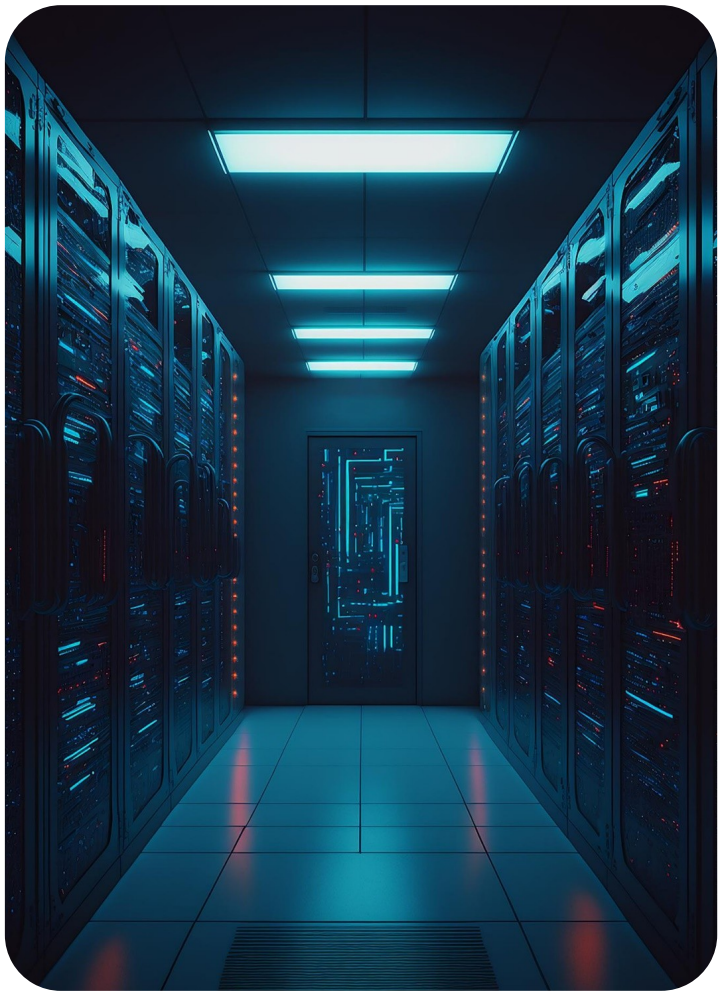
- Who will be **in charge** in your organization?
- Is it the CISO or someone else?
- It the CISO in place **available 24/24 and 7/7**?

Mapping systems

When the authorities will call and share a vulnerability, will you we able to identify the vulnerable asset?

- When was the last time you **update your system mapping**?
- Is it 100% accurate?
- What about deprecated systems or subsidiaries?
- What about **OT systems**?

Secure (all) your IT systems



To avoid such upsetting calls, you will enforce your security policy with all controls required by the directive.

- **All your systems** have to be protected, not only the one supporting sensitive business operations
- Security controls must embrace non-IT security topics like **HR security and awareness or 3rd party / supply-chain security**.

2. Le misure di cui al paragrafo 1 sono basate su un approccio multirischio mirante a proteggere i sistemi informatici e di rete e il loro ambiente fisico da incidenti e comprendono almeno gli elementi seguenti:

a) politiche di analisi dei rischi e di sicurezza dei sistemi informatici;

b) gestione degli incidenti;

c) continuità operativa, come la gestione del backup e il ripristino in caso di disastro, e gestione delle crisi;

d) sicurezza della catena di approvvigionamento, compresi aspetti relativi alla sicurezza riguardanti i rapporti tra ciascun soggetto e i suoi diretti fornitori o fornitori di servizi;

e) sicurezza dell'acquisizione, dello sviluppo e della manutenzione dei sistemi informatici e di rete, compresa la gestione e la divulgazione delle vulnerabilità;

f) strategie e procedure per valutare l'efficacia delle misure di gestione dei rischi di cibersicurezza;

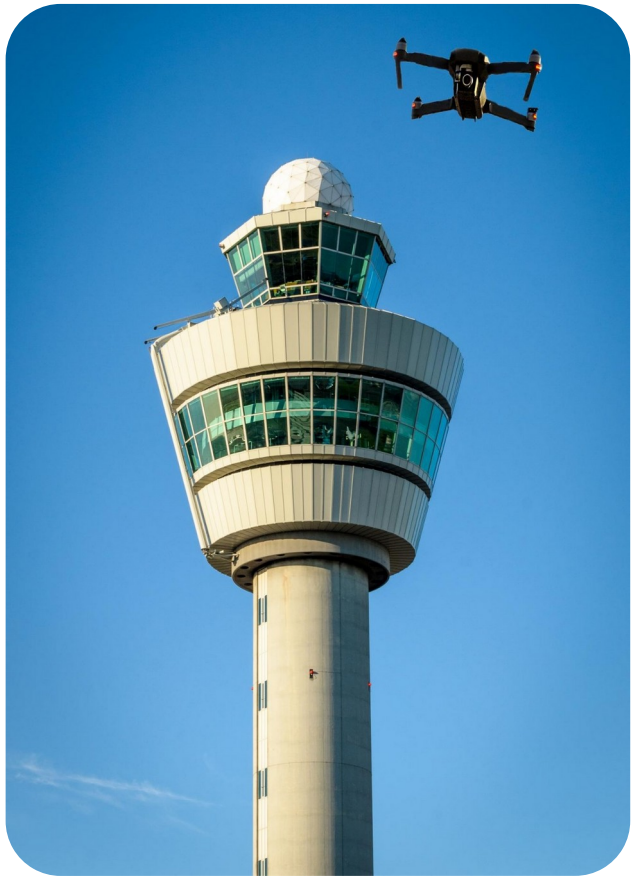
g) pratiche di igiene informatica di base e formazione in materia di cibersicurezza;

h) politiche e procedure relative all'uso della crittografia e, se del caso, della cifratura;

i) sicurezza delle risorse umane, strategie di controllo dell'accesso e gestione degli attivi;

j) uso di soluzioni di autenticazione a più fattori o di autenticazione continua, di comunicazioni vocali, video e testuali protette e di sistemi di comunicazione di emergenza protetti da parte del soggetto al proprio interno, se del caso.

Detect and react (quickly!)



On a daily basis, you need detection and reaction capabilities

- You must be able to **detect** incident on our systems.
- And once detected you must **notify** them to the local national authority.

✓ You must submit an early warning without undue delay and in any event **within 24 hours**.

✓ That early warning should be followed by an incident notification [...] without undue delay and in any event **within 72 hours** of becoming aware of the significant incident.

Brace yourselves: audits are coming

According to the text, here are the main measures that competent authorities can take to ensure compliance with the NIS 2 Directive:

- **On-site inspections and remote control**
- **Regular and targeted security audits**
- **Ad hoc audits**
- **Security scans**
- **Requests for access to data**
- **Requests for evidence of cybersecurity policies**

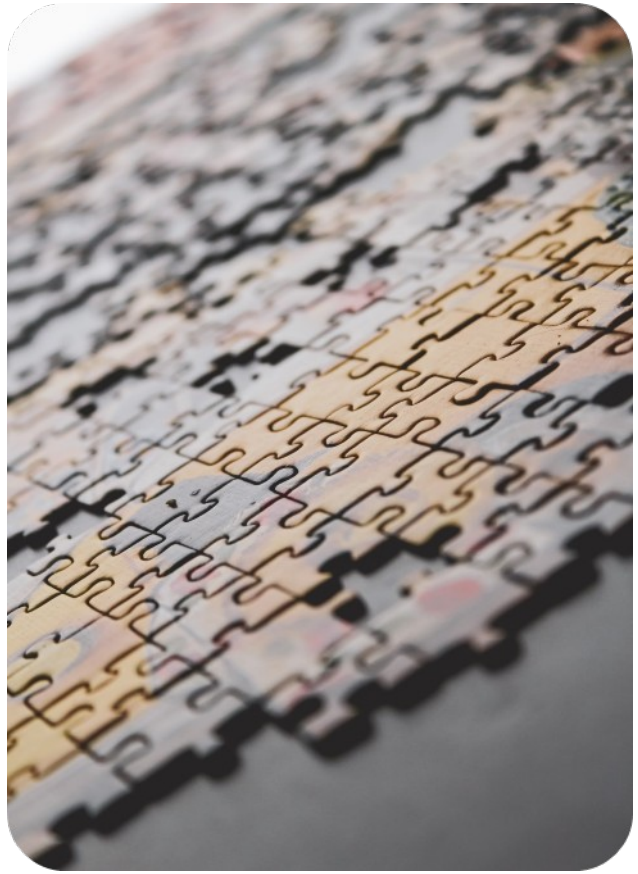
** by an independent body or by the competent authority itself*

And now?

Major takeaways

Gdvens
Security for the greater good

Now is the time



- ✓ Check if your organization is to be concerned
- ✓ Define the person in charge (it might probably be you!)
- ✓ Prepare the top management to a NIS 2 compliance program and a dedicated budget (for 2025 if it’s too late)
- ✓ Don’t wait for basic cyber “hygiene”

Security for the greater good

www.advens.it

Italy France Spain Germany Canada Tahiti