

THE ULTIMATE CYBER SURVIVAL GUIDE

V2

OR HOW TO NAVIGATE THROUGH NIS 2 (AND BEYOND)

WITH COMPLETE PEACE OF MIND

Powered by

SPAC ALLIANCE

STid

SPAC
>ALLIANCE<

We are a **European professional alliance** bringing together numerous experts in both physical and logical security, as well as national agencies such as **ANSSI** (the French National Cybersecurity Agency). Since our creation, we have been committed to helping define **European digital sovereignty** and to contributing to the establishment of **standards built on open and interoperable technological solutions**.

Our approach aligns with the ambitions of the European Union's **Digital Decade Policy Program 2030**, which positions cybersecurity as a prerequisite for the EU's digital independence — a key theme addressed in several recent directives, including the well-known **NIS 2** (Network and Information Security 2) Directive, which you will easily grasp as you explore this guide.

INDEED, SEVERAL QUESTIONS ARE PROBABLY ON THE TIP OF YOUR TONGUE:

- Am I affected by this regulation?

- How has NIS 2 been transposed in my country?

- What will my obligations be?

- When should I be ready, if applicable?

- Who can support me in implementing this regulation?

Beyond the general recommendations issued by **ENISA**, it will be necessary to apply the laws and decrees adopted by each Member State to achieve compliance by 2027. The guidance and tools provided in this guide are here to make that task much easier for you!

SSPAC Alliance is committed to keeping this document up to date by conducting proactive monitoring of the latest available information..

Want to stay informed? Subscribe to receive the latest updates!

CLICK HERE TO SUBSCRIBE

Understanding European regulation means recognizing that all of us — citizens, businesses, unions, associations, institutions, administrations, and the Member States of the European Union — are stakeholders with a shared responsibility and an active role to play in shaping this sovereignty.

Our collective success will depend on the relevance and impact of our individual actions.

TABLE OF CONTENTS

1. **WHEN WILL YOU BE ATTACKED?** 4

2. **REGULATIONS TO PROTECT US** 5
   - A. NIS 1, the fondation of European cybersecurity, focused on raison awareness 5
   - B. NIS 2 : the end-to-end concept 5

3. **ARE YOU AFFECTED BY THE REGULATION?** 6
   - A. Wich entity are you ? 6
     - 1. Important and Essential Entities (NIS 2) 6
     - 2. Critical Entities (CER) 7
   - B. The ULTIME table to understand it all 7

4. **SURVIVING IN A HOSTILE ENVIRONMENT** 8
   - A. Risks analysis 8
   - B. CE / EE / IE : what are your obligations? 9
     - 1. Responding to physical threats 9
     - 2. Communication protocol: a link between physical and logical realms 10
     - 3. Responding to logical threats 11

5. **PROTECTING TOGETHER AGAINST A BORDERLESS THREAT** 12
   - 1. A cross-border network 13
   - 2. Mandatory incident reporting 14
   - 3. Deterrent fines 14

6. **TRANSPOSITION INTO NATIONAL LAW** 15

7. **CONCLUSION : INVESTING TO PREPARE OUR FUTURE** 15

8. **APPENDICES :** 16
   - A. NIS 2 : sectors and sub-sectors concerned 16
   - B. REC : quelles sont les entités et secteurs concernés 17
   - C. NIS 2 / CER agenda 18
   - D. Practical info: what to do if i'm cyber-attacked? 18
   - E. Useful lnks 19
   - F. Listing of national cyber agencies 20

1

WHEN WILL YOU BE ATTACKED?

OH YES - YOU READ THAT RIGHT!

THE QUESTION IS NOT IF YOU WILL BE ATTACKED, BUT WHEN.

The proportion of organizations hit by cyberattacks is following a relentless upward trend. It exceeded **50% in 2021** and, according to a Dell Technologies study (Global Data Protection Index), reached nearly 9 out of 10 companies in 2022.

These attacks make no distinction between size or sector — everyone is a potential target in this growing wave of cybercrime, including individuals

DEVASTATING CONSEQUENCES

The majority of companies that lose access to their IT systems or control of their data for more than a week go bankrupt in the short term. A few figures provide a clear picture of the financial stakes involved.

Since 2015, the global cost of cybercrime has been rising steadily - **from 3 trillion dollars to 10.2 trillion dollars in 2025** - and **forecasts for 2031 exceed 12.2 trillion dollars** according to Cybersecurity Ventures. That represents more than 10% of global GDP, equivalent to the world's third-largest economy.



12.2 TRILLION IN 2031

90% of organizations affected

direct and indirect impact

THE IMPACT MUST BE ASSESSED ON SEVERAL LEVELS — AND IT GOES FAR BEYOND FINANCIAL CONSIDERATIONS:

- Cost of a potential ransom (which it is strongly recommended never to pay)
- Cost of business interruption, depending on the severity and duration of the attack
- Legal costs in case your liability is involved (for example, data theft due to insufficient protection)
- Increase in insurance premiums following a cyber incident
- Direct and long-term impact on your reputation and credibility within your ecosystem — users, business partners, banks, investors, and even employees
- Loss of competitive advantage: theft of research results or unpatented technologies, disclosure of strategic plans, product copying, etc.
- Possible infection of all interconnected information systems, including those of your suppliers and clients

Take a few minutes to estimate — even roughly — what these direct and indirect costs could mean for your organization.
Now that we have your full attention, let's take a closer look at this regulation.

THE TAKEAWAY: **In a hyperconnected economy facing an ever-present cyber threat, all the ingredients are there for entire sectors — not just individual organizations — to be exposed to a devastating domino effect.**
This mission, since it must be accepted, is now more collaborative than ever.

2

REGULATIONS TO PROTECT US

A. NIS 1, THE FOUNDATIONS OF EUROPEAN CYBERSECURITY,FOCUSED ON AWARENESS

Since its creation, the European Union has faced a series of technological evolutions that have profoundly transformed our way of life, our communication, and the way we work — from the digitalization of the economy and the rise of mobile technology to high-speed internet and the spread of remote work.

This fast-paced digitalization has also opened countless new entry points for malicious hackers.

These advancements have always been accompanied by regulations designed to protect users, businesses, and infrastructures. Their goal?

To ensure European sovereignty — particularly in the realms of digital technology and cybersecurity.

On this front, the EU first relied on **NIS 1** (Network and Information Security 1), a regulation limited to the most critical stakeholders. It was a beneficial strategy, yet it failed to achieve a sufficient level of resilience. Several explanations have been put forward: too few actors were covered, a lack of coordination between Member States, and — as we've already seen — a significant evolution in both the nature and volume of cyberattacks.

B. NIS 2 : THE END-TO-END CONCEPT

From this observation, the new European directive introduces the concept of end-to-end security, detailed in **NIS 2**. It is built around three key pillars designed to ensure full commitment from all stakeholders — from awareness to action and cooperation at the European level.

The era of acting alone is over!The EU now delivers a comprehensive response to cyber threats through :

- A **major expansion in the number** of sectors covered by the directive, involving far more stakeholders — even extending to their supply chains, which multiplies the scope of these regulations. Depending on the country, the number of entities affected by the directives is expected to increase to **more than 160,000**.
- A **coordinated and mandatory approach** spanning from prevention to cross-border actions, engaging all stakeholders. Member States must establish prevention policies accessible to all citizens.
- A holistic **consideration of both logical and physical threats** to information systems — where access control and video surveillance now complement traditional cybersecurity measures.

Thus, cybersecurity must be approached in a way that is:

GLOBAL :
It concerns everyone — from individual users to European institutions, encompassing the entire economic, industrial, and social fabric.

COORDINATED :
Cross-border cooperation is essential
to confront a threat that recognizes no borders.

MANDATORY :
Beware of those who fail to comply with the directive!
Companies and their executives risk fines of up to 2% of their global annual turnover.

ACTIVE :
It's not enough to be aware of the problem — you must also be trained to take action in the event of an attack. This requires a clear and coordinated set of action rules to maximize effectiveness..

COMPLETE :
The cyber world doesn't stop at the digital realm.
An access reader, a USB stick found on the ground, or a physicalintrusion can all create vulnerabilities in your system — despite every digital safeguard in place.

BOTTOM LINE:

The EU has learned from its earlier regulations and now offers more than just an update to the framework.

The new vision is comprehensive: more stakeholders involved, all types of threats addressed, everyone trained, and cross-border cooperation strengthened.

3 ARE YOU AFFECTED BY THE REGULATIONS ?

TWO MAJOR TEXTS DEFINE THE RULES THAT HAVE BEEN APPLICABLE SINCE OCTOBER 17, 2024.

NIS 2 and **CER** (Critical Entities Resilience, Directive EU 2022/2557) define which organizations are considered more or less critical to Europe's overall security. Each level of criticality comes with proportionate obligations, based on principles we'll explore later in this guide..

It's easy to see the difference: a data center hosting 20% of France's data is far more critical — in cyber terms — than your local bakery or even a major French chip manufacturer (the latter, of course, falls under other European directives on food safety — we'll spare you those details for now!)..



WITHOUT FURTHER ADO, LET'S EXPLORE THE THREE LEVELS OF CRITICALITY INTRO-DUCEDBY THESE DIRECTIVES :

Critical Entities (CE), as defined by the CER Directive, are organisations that provide essential services necessary to maintain vital societal functions, economic activity, healthcare, or public safety.

This includes, for example, entities previously classified as **Operators of Vital Importance** (OVI), as well as the largest companies operating within the sectors covered by the regulation.

Essential Entities (EE) and **Important Entities** (IE), as defined by NIS 2, encompass the majority of organisations, with obligations that are scaled and proportionate to their resources and level of criticality.

Former **OES** (Operators of Essential Services under NIS 1) are automatically classified as EE. For other organisations, classification depends on the entity's sector and size.

To determine whether you fall under one of these regulations, you must verify that your organization operates withinone of the designated sectors and meets specific criteria related to size, turnover, or revenue.

Don't worry — we've compiled all of this into the ultimate table at the end of this chapter!!

To find out whether you're affected, get in touch with your national cybersecurity agency.
Most countries provide an online tool to help you determine whether your organization falls within the NIS 2 / CER scope.

You'll find the full list of national agencies in the Annex of this guide!!

A. WICH ENTITY ARE YOU?

1. NIS2 : ESSENTIAL ENTITIES (EE) AND IMPORTANT ENTITIES (EI)

The NIS 2 directive expands the number of affected sectors from 7 (under NIS 1) to 18.
You will be classified as an Essential Entity (EE) if:

- You were already an Operator of Essential Services (OES) under NIS 1 as of January 16, 2023.
- You belong to one of the 11 highly critical sectors and are a large enterprise (annual turnover > €50M, balance sheet total > €43M, or more than 250 employees).

You may be classified as an Important Entity (IE) if:

- You operate in one of the covered sectors (11 highly critical or 7 critical sectors)
- and your company has an annual turnover or balance sheet total above €10M, or employs more than 50 people.

According to the chain of responsibility principle, regardless of your size, you may be designated as an EE or IE if:

- You are the sole provider of an essential service.
- You are part of the supply chain of a specific entity that could be compromised through your systems.

2. CER : CRITICAL ENTITIES (CE)

As its name suggests, the **CER Directive** specifically targets the most strategic actors across 12 defined sectors. If you fall within its scope, you may be designated as a **Critical Entity (CE)** - regardless of your organisation's size.

Once again, in line with the chain-of-responsibility principle, you may also be affected by the CER if you are **part of the supply chain of a Critical Entity** whose operations could be compromised through your systems.

Finally, keep in mind that the obligations imposed by the CER Directive **come in addition to those required under NIS 2**

And finally (we promise, this is the last one!), if you provide essential services in six or more EU Member States, you will be designated as a Critical Entity of Particular European Importance.
This status entails continuous monitoring by national security agencies to ensure full compliance with the directives.

B. THE ULTIMATE TABLE TO UNDERSTAND EVERYTHING

List of highly critical sectors (NIS 2 + CER)	Type of entity			List of critical sectors (NIS2)	Type of entity
	High Criticity	TURNOVER >€50M	TURNOVER < €50M		
Energy	CE	EE	IE	Postal and courier services	IE
Transport	CE	EE	IE	Waste management	IE
Banking	CE	EE	IE	Manufacturing, production, and distribution of chemicals	IE
Financial market infrastructures	CE	EE	IE	Production, processing and distribution of food	IE
Health	CE	EE	IE	Manufacturing	IE
Drinking water	CE	EE	IE	Digital provider	IE
Wastewater	CE	EE	IE	Research	IE
Digital infrastructure	CE	EE	IE		
Information and communication technologies service management	CE	EE	IE		
Public administration	CE	EE	EE		
Space	CE	EE	IE		
Production, processing and distribution of food	CE				

CE = CRITICAL ENTITIES (CER)

EE = ESSENTIAL ENTITIES (NIS 2)

IE = IMPORTANT ENTITIES (NIS 2)

CLICK HERE TO DISCOVER SUB-SECTORS

FINAL KEY POINTS:

- Each Member State can designate your organization as a specific entity regardless of its size (including small andmicro-enterprises)..
- And don't forget: entities covered by the CER Directive must also comply with NIS 2.

4

SURVIVING IN A HOSTILE ENVIRONMENT

IF YOU'VE JUST BEEN DESIGNATED AS AN EE, IE, OR CE, OR IF YOU SIMPLY WANT TO STRENGTHEN YOUR RESILIENCE, YOU MUST START TAKING SEVERAL KEY STEPS RIGHT NOW

- Conduct a risk assessment
- Map your information system and all related equipment
- Evaluate the impact of an incident across your supply chain
- Define a prevention strategy
- Establish a business continuity and recovery plan

European regulations aim to secure our shared digital space — and complying with them is always beneficial, even when not strictly mandatory.

Remember the figures mentioned earlier: the question isn't if you'll be attacked,but when.

Whether for financial gain (ransom, data resale), ideological motives (cyberterrorism), geopolitical reasons (such as the Russia–Ukraine conflict), or economic rivalry (trade wars), cybercriminals won't wait for you to be ready.

A. ASSESS YOUR RISKS

Risk assessment is the first step to take.
If this topic is new to you, we encourage you to explore the range of support services offered by our members and to conduct our online security mini-audit.

National cybersecurity agencies, along with many European organizations (including SPAC Alliance), can serve as trusted partners to support and guide you through publications, practical guides, and training programs such as MOOCs and webinars.

HERE'S THE TYPICAL PROCESS FOR CONDUCTING AND IMPLEMENTING A SECURITY AUDIT:

The assessment of needs is based on the NIS 2 / CER **compliance framework** defined by each Member State.

By adopting a **cyclical audit** approach, you will gain a clearer understanding of your security posture, identify weaknesses, and improve responsiveness in the event of a threat.

For **Critical Entities**, a continuous dual-audit strategy - both internal and external - will be mandatory.

In general, maintaining **proportionate oversight** aligned with your level of criticality is strongly recommended



BOTTOM LINE:
At the risk of repeating ourselves — cybersecurity concerns everyone, even outside a legal framework. Preparing as early as possible and maintaining continuous assessment ensures a solid level of protection and enables smart planning for necessary investments.

B. CE / EE / IE : WHAT ARE YOUR OBLIGATIONS?

SPAC Alliance brings together many leading security players and works continuously alongside legislators. Drawing on the collective experience of our members and active participation in numerous European committees, we offer you an overview of the tools and solutions needed to build an effective and tailored line of defense.

1. RESPONDING TO PHYSICAL THREATS

Article 21 of NIS 2 is crystal clear: organizations must adopt an "all-hazards approach" to protect both their networks and information systems, as well as their physical environment.
Here are some key points that deserve your attention:

- Securing the perimeter of your facilities
- Securing access control
- Managing critical areas (data centers, clean rooms, machinery, etc.)
- Managing visitors

ENISA recommends that all organizations draw inspiration from or integrate ISO 27001 or NIST CSF 2.0, both of which include physical security and access control requirements.
However, since NIS 2 and CER are directives, each Member State defines its own laws, decrees, and compliance frameworks, which may add further obligations beyond those imposed by ISO or CSF standards.

ENISA RECOMMANDATION (NO AUTOMATIC COMPLIANCE)	LAW, DECREE, AND COMPLIANCE FRAMEWORK	CERTIFICATIONS SPÉCIFIQUES (SELON CRITICITÉ)
ISO 27001 / NIST CSF 2.0	SPECIFIC TO EACH COUNTRY	CRITICAL ENTITIES and certain ESSENTIAL ENTITIES

Each country may have its own **regulatory framework**, and certain differences can be observed from one Member State to another. For instance, one country may consider ISO 27001 certification as evidence of compliance, while its neighbour may not.

A commission bringing together the 27 national cybersecurity agencies is continuously working to **harmonise these frameworks** in order to simplify compliance for entities operating across multiple countries.

At the discretion of each authority, **specific certifications may be required**. For example, France and Germany may require **CSPN- or BSZ-certified solutions**, depending on the entity's level of criticality.

CLICK TO VIEW THE LIST OF COMPLIANCE FRAMEWORKS

REMINDER: WHEN IT COMES TO PHYSICAL SECURITY, PROTECTION MEANS

Deter: fencing, warning signs, automatic lighting
Detect: surveillance cameras, motion sensors, security patrols
Delay: locks, multiple barriers, reinforced doors
Deny: access control adapted to the level of criticality (high-security badges and readers, PIN codes, bio, etc.)

2. THE COMMUNICATION PROTOCOL : A LINK BETWEEN PHYSICAL AND CYBER REALMS

As you've likely noticed while reviewing the many potential threats, access control is one of the key pillars of cybersecurity. It also serves as the last line of defense between the outside world and your information system. More specifically, the wired system connecting your badge reader to your security system forms a true link between the physical and cyber realms.

At the heart of any access control system lies the communication protocol, which must be robust enough to meet today's security challenges. Four main standards are commonly used ::



While the first two protocols are now completely obsolete, they still account for over 70% of the global market and should be avoided at all costs.

Only **OSDP™** and **SSCP®** currently provide a high level of security. Although they share some common features, significant differences clearly tip the balance in favour of the European solution.

Both **OSDP™** and **SSCP®** are bidirectional protocols, enabling intelligent and efficient management of an entire security ecosystem. However, **they differ in their design and underlying philosophy**.

OSDP™ was designed to be open but is not secure by default. An organisation using **OSDP™** has no inherent security guarantee and must ensure that the Secure Channel option is properly enabled during deployment.

Equally open, **SSCP®** was built to deliver the highest possible level of security. With **SSCP®**, all **communications are systematically authenticated, signed, and encrypted,** meeting the most stringent certification requirements - such as the **CSPN certification issued by ANSSI**, required for the most critical entities.

In fact, SSCP® even outperforms the secure configuration of OSDP™.

If you have to choose, **we strongly recommend SSCP®** - an open and sovereign protocol, fully integrated into certified solutions available on the market, including those holding French **CSPN certification**.



Moreover, **choosing SSCP® means actively contributing to the creation of a true European cyber fortress** by prioritizing sovereign solutions that support the very objectives at the heart of NIS 2 and CER — a vision we wholeheartedly share, as you've probably guessed!

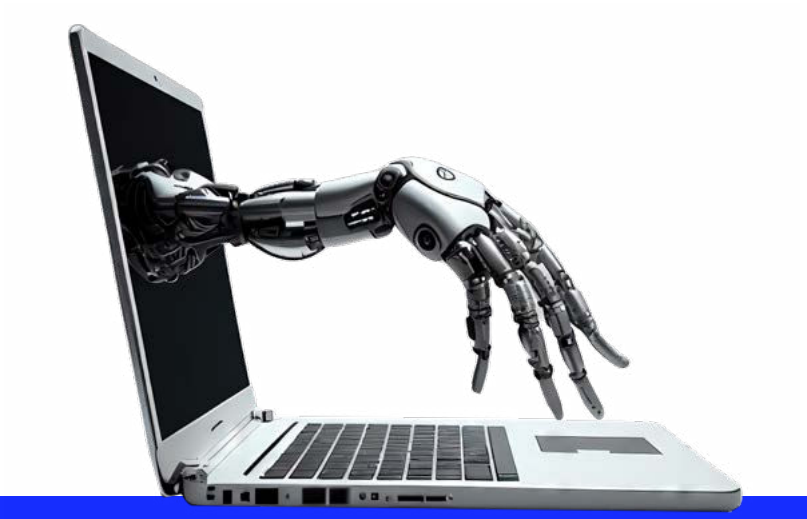
***BOTTOM LINE*:**
The connection between your reader and the control panel is the natural link between physical security (attempts to gain access) and cybersecurity (attempts to corrupt).
The reliability of any access control solution depends directly on the strength of the communication protocol that drives it.
SSCP®, supported by SPAC Alliance, stands as the security benchmark.

3. THE ANSWER TO LOGICAL THREATS

Human error remains the **leading cause of cyber intrusions** — a reality that highlights just how critical **training** and **prevention** are when it comes to effectively protecting an information system, which itself must be well-designed and properly maintained..

As stated in the directives, obligations are proportionate to each entity's size and level of criticality. However, some essential countermeasures apply to everyone (and are strongly recommended even for microenterprises, small businesses, and individuals outside the regulation's scope):

- Training in digital hygiene and cybersecurity best practices
- Installation of a complete security suite (anti-virus, anti-spam, anti-phishing)
- Use and regular renewal of strong passwords
- Password management vaults for secure storage
- Automatic updates for workstations and software
- Remote data backups
- Firewall protection for each workstation to guard against internet-based attacks
- SSL certificates for all websites



DID YOU KNOW?

SILENT ATTACK !

Cyber attacks can be particularly insidious — some are designed to remain invisible, with no intention of stealing data or spying.Many digital devices are silently infected, such as the smartphone in your pocket or your home computer (often less protected). These devices can become relay machines, remotely controlled by hackers, whose computing power and memory are then used to launch largescale attacks — including the infamous DDoS (Distributed Denial of Service), which floods a network or website with massive simultaneous connections until it crashes

Entities covered by NIS 2 (EE and IE) must implement an additional layer of security tailored to their status. Here are a few examples:

- Appointment of an Information Security Officer (ISO) or Chief Information Security Officer (CISO)
- Traceability of all IT assets.
- Access rights limited to actual needs (Administrator, User, Visitor)
- Policy for remote and mobile work
- Deployment of a local firewall to protect the internal network
- Data encryption and use of a VPN for secure communications.
- Monitoring and management tools for the information system
- Physical access control for critical areas (authentication required to enter data centers)
- Attack simulations to test response and recovery procedures



DID YOU KNOW?

THE HIDDEN CONNECTION ATTACK !

Whether working remotely or traveling, mobile work comes with its own set of risks that must be anticipated.
For instance, using public Wi-Fi networks should be strictly avoided, and you should always use a privacy filter to prevent others from viewing your screen. Even public USB charging stations pose a threat — while it may seem convenient to charge your phone at an airport, it's essentially like plugging in a potentially infected USB device

And finally, we come to the Critical Entities (CE) under the CER Directive, which — as you might expect — must aim for excellence in cybersecurity::

- **Zero-trust strategy**: systematic authentication of every user on a device, and every device on a network
- **Ban on connecting external hardware** (USB drives, external hard disks, personal phones)..
- **Network and backup segmentation** to contain any potential spread.
- **Penetration testing** conducted by independent organizations
- **Regular audits** performed by the relevant national cybersecurity agency or certified consultants

DID YOU KNOW?

ATTACKS STRAIGHT OUT OF THE MOVIES!

Successful hybrid attacks are on the rise. Their modus operandi is simple: gain direct access to a machine—often via a single USB key—that installs malware straight into the heart of the system. That's enough to bypass most conventional cyber defenses and inflict extensive damage. Cyber-attackers know how to put into practice what we see in the movies!



As you've likely noticed, regardless of an entity's level of criticality, most vulnerabilities stem from human error. Across Europe, this means that companies play a central
role in spreading best practices and strengthening both digital resilience and sovereignty..

While ISO 27001 certification is generally considered sufficient to presume compliance with NIS 2, it's still essential to review the specific regulations of each Member State. Good news: you'll find everything here!

BOTTOM LINE: **When it comes to cybersecurity, the human factor is both the greatest threat and the best defense. Training, proper implementation of EU directives, and sustained investment are the keys to achieving effective and lasting protection..**

5

PROTECTING OURSELVES TOGETHER AGAINST A BORDERLESS THREAT

BETTER SAFE THAN SORRY: SUPPORT LIES AT THE HEART OF THE NEW EUROPEAN FRAMEWORK, WITH AN END-TO-END STRATEGY DESIGNED TO ACHIEVE SEVERAL KEY OBJECTIVES

- Education and awareness in digital hygiene and best practices
- Network monitoring and surveillance
- Mandatory incident reporting
- Development and dissemination of solutions to address threats or attacks

A strategy notably supported by SPAC Alliance, which brings together numerous experts in the field and actively contributes to the development of robust security standards.

PREVENTION AND DETECTION

For EE, IE, and CE — as well as for organizations outside the regulatory scope — strong preventive measures must be implemented. While the level of obligation may vary depending on each entity's criticality, every country provides tools and training resources, such as the digital best practices **MOOC** developed by ANSSI in France.

In addition, the European Union is investing in several Security Operations Centers (SOCs) equipped with supercomputers capable of detecting large-scale malicious activity early on. It has also launched a **European Cyber Skills Academy** to address growing training needs — further strengthening and reinforcing our collective cyber shield.

1. A CROSS-BORDER NETWORK

A mandate has been given to **ENISA** (the European Union Agency for Cybersecurity) to establish the Joint Cyber Unit, whose mission is to strengthen European coordination and provide the best possible support to all designated entities (IE, EE, and CE).

This network begins within each individual organization and then extends across the entire European Union:

Chief Information Security Officer (CISO) within each entity

CERT (Computer Emergency Response Team) for each country, and CERT-EU at the European level.

A single point of contact is designated in each country — the first organization to contact in case of an incident.
This may be a CSIRT (Computer Security Incident Response Team), either regional or national.
We advocate a territorial approach to cybersecurity, emphasizing that public authorities must support businesses within each region.



ENISA, CyCLONe (Cyber Crises Liaison Organisation Network).

EUROPOL: European police cooperation agency, which includes the European Cybercrime Centre (EC3)

Constant, two-way communication is essential to ensure high efficiency in threat identification, countermeasure development, and knowledge sharing.

2. MANDATORY INCIDENT REPORTING

In the event of an incident, you are required to contact your **Single Point of Contact (SPoC)**, which triggers a standardized procedure common to all entities:

- **Within 24 hours:** notification to the Single Point of Contact and the CSIRT network.
- **Interim report:** provided upon request by an authority or the CSIRT network
- **Within 30 days:** submission of a final report detailing the severity and impact, the type and cause of the threat, and the mitigation measures implemented

Note that this **Single Point of Contact** can be reached by any company in the event of an attack.
Developing the reflex to file a formal complaint systematically is essential — it ensures you receive full support, including investigation, compensation, and follow-up from the relevant authorities and agencies mentioned above.



3. DETERRENT FINES

In cases of non-compliance with the NIS 2 Directive, Essential Entities (EE) and Important Entities (IE) are subject to administrative fines.

For **Essential Entities**, the maximum fine is at least **€10 million or 2% of global annual turnover**, whichever amount is higher.

For **Important Entities**, the maximum fine is at least **€7 million or 1.4% of global annual turnover**, whichever amount is higher.

These amounts were modeled after the typical ransoms demanded by hackers when they successfully encrypt a company's data.

Sanctions applicable to Critical Entities (CE) will be determined by each Member State and must be effective, proportionate, and dissuasive..

BOTTOM LINE: **You are no longer alone when facing a cyber incident — but you MUST take proactive measures to strengthen your cybersecurity posture. Failure to comply with the regulations could come at a high price, adding to the already significant direct and indirect costs of a successful attack.**

6

IMPLEMENTATION INTO NATIONAL LAW

NIS 2 AND CER CAME INTO FORCE IN JANUARY 2023, INITIATING THE PROCESS OF TRANSPOSITION BY EACH EU MEMBER STATE.

Initially scheduled for October 17, 2024, the transposition of these directives into national laws has often faced delays. The same applies to the decrees detailing obligations for each type of entity and the compliance frameworks.

In general, the recommendations align with the objectives set out in **ISO 27001** and **NIST CSF 2.0**, two frameworks endorsed by **ENISA**. The next major milestone is 2027, when penalties will begin to apply.

SPAC ALLIANCE

SPAC Alliance actively contributes to numerous regulatory working groups, standardization committees, and policy-design commissions — bringing together the expertise and knowledge of its members.

CLICK HERE TO CONSULT

- ***STATE-BY-STATE TRANSPOSITIONS***
- ***COMPLIANCE FRAMEWORKS LIST ACROSS EUROPE***

7

CONCLUSION: INVESTING TO PREPARE OUR FUTURE

"MORE CONSTRAINTS, YOU SAY?"

Yes — NIS 2 and CER are two major new regulations. And, as always, they come with certain constraints that must be implemented within relatively short timelines..

However, it's important to look on the bright side..

Citizens, employees, local authorities, and businesses alike often underestimated cyber threats or overestimated their defenses. With these directives, we now have an objective view of the risks and the ability to deploy the tools and practices needed to mitigate them.

Of course, this level of compliance comes at a cost. But rather than being a simple expense, it should be seen as a measured and worthwhile investment, one that enables sustainable growth and long-term peace of mind.

This milestone, part of the broader **European Digital Decade Policy Program 2030**, lays the foundation for lasting European digital sovereignty.

It also sets the stage for upcoming strategic initiatives in the fields of **digital identity** (eIDAS V2), **artificial intelligence** (AI Act), **European blockchain infrastructure** (EBSI), and the **Cyber Resilience Act**.

But don't worry — we'll provide you with all the insights you need, when the time comes, to understand these concepts and make the most of the opportunities they bring.

SUBSCRIBE

BECOME A MEMBER

JOIN THE CLUB

8

APPENDICES

A. NIS 2: SECTORS AND SUB-SECTORS CONCERNED

LEntities already covered by NIS 1 remain within the scope of NIS 2.
However, the perimeter has been significantly expanded, now distinguishing between two main sectors: :

HIGHLY CRITICAL SECTORS AND SUBSECTORS

- Energy
  - Electricity
  - District heating and cooling
  - Oil
  - Gas
  - Hydrogen
- Transportation
  - Air
  - Rail
  - Water
  - Road
- Banking
- Financial market infrastructure
- Health
- Drinking water
- Wastewater
- Digital infrastructure
- Information and communication technologies service management
- Public administration
- Space



OTHER CRITICAL SECTORS AND SUB-SECTORS

- Postal and shipping services
- Waste management
- Manufacturing, production, and distribution of chemical products
- Food production, processing, and distribution
- Manufacturing
  - Manufacture of medical devices and in vitro diagnostic medical devices
  - Manufacture of computer, electronic and optical products
  - Manufacture of electrical equipment
  - Manufacture of machinery and equipment
  - Manufacture of motor vehicles, trailers and semi-trailers
  - Manufacture of other transport equipment
- Digital Providers (DSPs): online marketplaces, search engines, social networks
- Research

B. CER : WHICH ENTITIES AND SECTORS ARE CONCERNED?

Organizations designated by each country as Critical Entities or Critical Entities of Particular European Importance fall under the scope of the **CER Directive** (Critical Entities Resilience Directive) — regardless of their size, number of employees, or annual turnover.

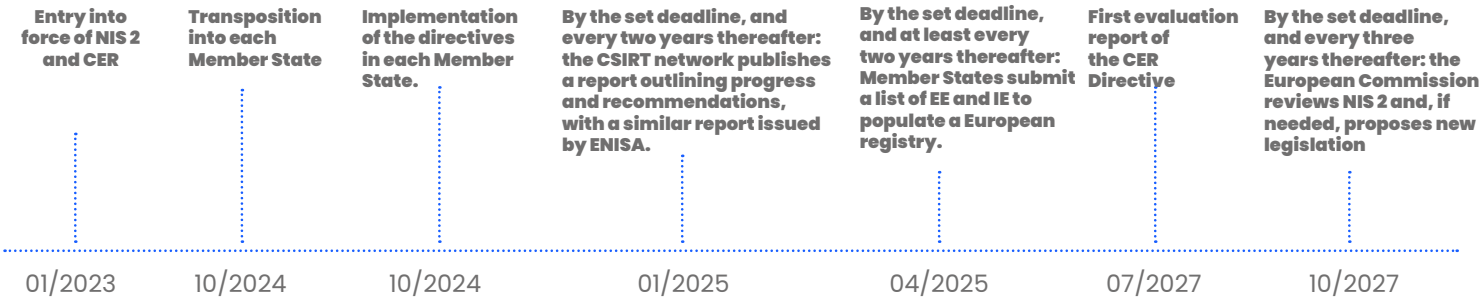
SECTORS COVERED BY THE CER DIRECTIVE :

- Energy
  - Electricity
  - District heating and cooling networks
  - Oil
  - Gas
  - Hydrogen
- Transport
  - Air transpor
  - Rail transpor
  - Water transpor
  - Road transpor
  - Public transport
- Banking
- Financial Market Infrastructure
- Helathcare
- Drinking water
- Wastewatr
- Digital Infrastructures
- Public administration
- Space
- Production, processing, and distribution of food products



C. NIS 2 / CER TIMELINE

The implementation timelines for NIS 2 and CER are identical across the European Union



D. PRACTICAL GUIDE: WHAT TO DO IF YOU'RE CYBERATTACKED?

In the event of a cyberattack, it's crucial to take immediate action to minimize damage and protect your data. Here are some best practices to follow:

1/Isolate and disconnect:

Identify the source of the attack quickly and isolate infected systems or devices by disconnecting them from the network. This can help contain the spread of the attack.

2/Notify the parties concerned:

Notify the relevant people in your organisation, including IT teams, management, and any security officers, so they can take appropriate action.

3/Gather evidence:

Document all relevant information about the attack, such as system logs, screenshots, and malicious files. This evidence can be useful for subsequent investigations and recovery measures.

4/Contact the relevant authorities:

Report the incident to the relevant cybercrime or law enforcement agencies in your area. They can provide advice and assistance in managing the attack. As we have seen, regulations define different processes depending on your criticality. It is important to lodge a complaint.

5/Recovery from backups:

If you have regular backups of your data, use them to restore affected systems and files. Make sure that the backups are secure and not compromised by the attack.

6/Incident analysis:

Carry out an in-depth investigation to understand the nature of the attack, the weaknesses exploited and the corrective measures to be taken. This analysis will help you strengthen the security of your IT infrastructure to prevent future attacks.

7/Strengthening security:

Identify the security gaps that enabled the attack and take steps to correct them. This may involve updating software, improving authentication practices, raising employee awareness of IT security, etc.

8/Raising employee awareness:

Regularly educate and inform your staff about cyber security threats, social engineering techniques and good security practices. Well-informed employees can be an effective first line of defence against attacks.

9/Reassess your security policy:

Review your IT security policy and update it if necessary. Make sure it covers all relevant aspects of cyber security and complies with industry best practice.

10/Continuous monitoring:

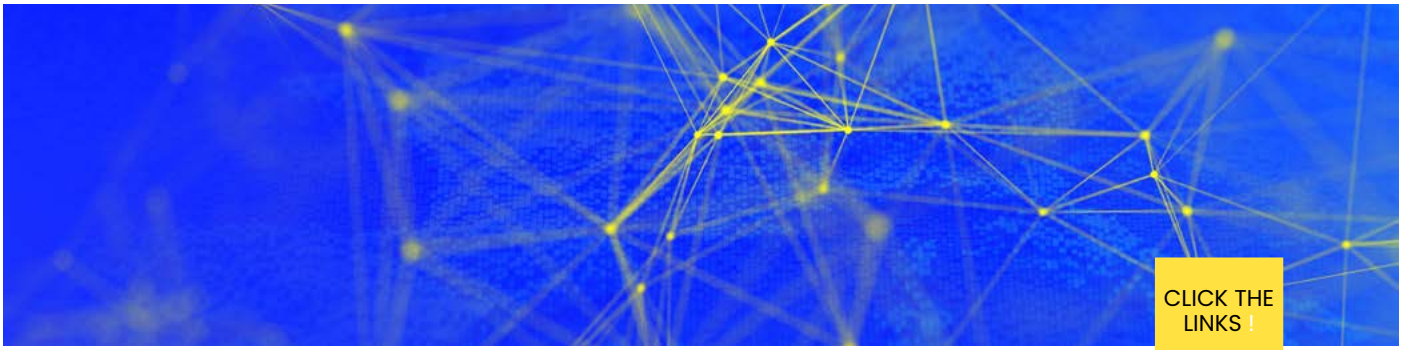
Put in place continuous monitoring mechanisms to quickly detect suspicious activity or intrusion attempts. This can include the use of intrusion detection software, advanced firewalls, and intrusion prevention systems.

It is also recommended to consult cybersecurity professionals and work with experts to effectively manage the consequences of a cyberattack and strengthen your organization's overall resilience

E. USEFUL LINKS

OFFICIAL TEXTS :
- NIS 2
- Critical Entities Resilience Directive

F. NATIONAL CYBER AGENCIES



COUNTRY	NATIONAL COORDINATION CENTRE
Austria	Federal Chancellery of Austria in cooperation with the Austrian Research Promotion Agency
Belgium	Centre for Cybersecurity Belgium (CCB)
Bulgaria	Ministry of Electronic Governance
Cyprus	Digital Security Authority (DSA)
Czech Republic	National Cyber and Information Security Agency
Germany	National Coordination Centre for Cybersecurity - Federal Office for Information Security (BSI)
Denmark	The Danish Business Authority
Estonia	Estonian Information System Authority
Greece	National Cybersecurity Authority of Greece
Ireland	National Cyber Security Centre of Ireland
Spain	National Cybersecurity Institute (INCIBE)
Finland	NCSC-FI
France	Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI)
Italy	Agenzia per la Cybersicurezza Nazionale (ACN)
Lithuania	National Coordination Centre, Ministry of National Defence
Luxembourg	National Cybersecurity Competence Center Luxembourg
Latvia	Ministry of Defence
Malta	Malta Information Technology Agency
Netherlands	The Netherlands Enterprise Agency (RVO)
Poland	National Cybersecurity Coordination Centre Unit in the Chancellery of the Prime Minister
Portugal	Portuguese National Coordination Centre
Romania	Centrul Național de Coordonare
Sweden	Swedish Civil Contingencies AgencyEN
Slovenia	Office of the Government of the Republic of Slovenia for Information Security
Slovakia	Cyber Security Competence and Certification Centre (KCCKB)

EUROPEAN COORDINATION BODIES AND INCIDENT REPORTING

- CSIRT Network
- CERT & CERT EU
- ENISA et List of ENISA Liaison Officers
- Europol

DISCOVER OUR MEMBERS

SPAC ALLIANCE MEMBERS

JOIN THE SPAC ALLIANCE CLUB

SPAC ALLIANCE CLUB

BROWSE OUR NIS 2 / CER SERVICES

