aftra.io

aftra

The NIS2 Directive

Stepping up cybersecurity resilience

Contents

03 **Key takeaways:** Your NIS2 essentials
04 **Introduction:** Building resilience in the NIS2 era
05 **Decoding NIS2:** What's new?
06 **DORA:** The sister law for financial institutions
07 **Gearing up for NIS2:** Your action plan
08 **The price of non-compliance**
09 **Aftra:** Your partner in NIS2 readiness
11 **Conclusion:** Embarking on your NIS2 journey

Key takeaways:
Your NIS2 essentials

1. NIS2 is casting a wider net, bringing more sectors and businesses into the fold.
2. Non-compliance comes with a hefty price tag - think security exposure, reputation damage and large fines.
3. NIS2 mandates prompt incident reporting within strict timeframes, ensuring quick response and mitigation.
4. NIS2 places individual accountability on executives and board members for implementing cybersecurity measures and ensuring compliance.

Introduction: Build resilience in the NIS2 era

The cybersecurity landscape is rapidly evolving, with imminent regulations designed to protect businesses and citizens from escalating digital threats. The European Union has been at the forefront of this effort, introducing the Network and Information Security (NIS) Directive in 2016. This groundbreaking legislation aimed to establish a common framework for cybersecurity across the EU, ensuring that member states and organizations were better equipped to defend against cyber attacks.

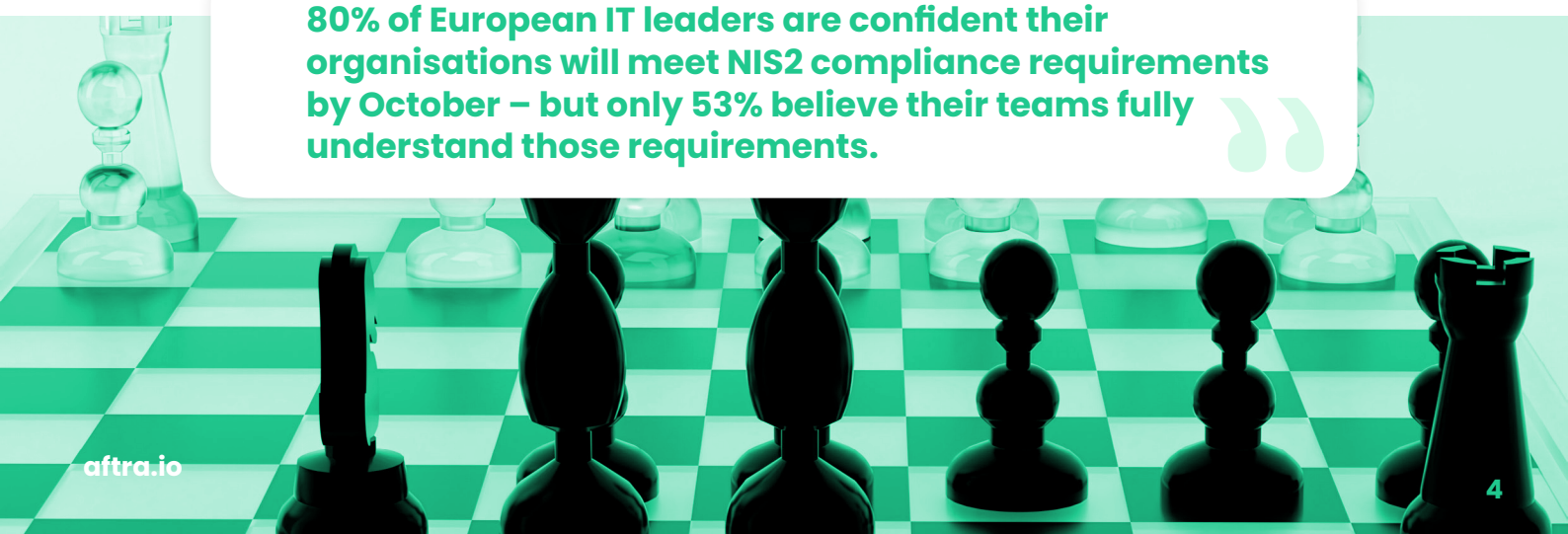
However, as the nature and sophistication of cyber threats continue to advance, the need for a more robust and comprehensive approach has become increasingly apparent. Enter NIS2, the updated directive set to replace the original NIS, bringing with it a host of new requirements and a broader scope of affected entities. The time to act is now to ensure that organizations are prepared for the implementation of NIS2 and can maintain a resilient cybersecurity posture in the face of ever-evolving threats.

NIS2 compliance deadline: October 17, 2024

The importance of NIS2 compliance cannot be overstated. As the directive comes into force, organizations across a wider range of sectors will be required to adhere to stringent cybersecurity standards. Compliance with NIS2 should be a top priority for organizations, not just to avoid severe financial penalties, but because it represents the minimum best practices necessary to protect their assets, reputation and continuity of operations. By embracing NIS2 compliance, organizations can significantly enhance their resilience against cyber threats, safeguarding their future in an increasingly digital world.

It is therefore essential for organizations to gain a deep understanding of NIS2 and take proactive steps to ensure compliance. The time to act is now – delaying compliance efforts could leave organizations vulnerable to cyber attacks and struggling to catch up with the regulatory requirements. By prioritizing NIS2 compliance and embedding cybersecurity best practices into their operations, organizations can build a strong foundation for resilience and success in the digital age.

> **80% of European IT leaders are confident their organisations will meet NIS2 compliance requirements by October – but only 53% believe their teams fully understand those requirements.**



Decoding NIS2: What's new?

One of the most significant changes introduced by NIS2 is the expanded scope of the directive. While the original NIS primarily focused on operators of essential services and digital service providers, NIS2 casts a much wider net, encompassing a broader range of sectors and entity types.

Along with the expanded scope, NIS2 introduces strengthened security requirements for organizations. The directive places a strong emphasis on:

- **Risk management and incident reporting**
- **Supply chain security**
- **Encryption and vulnerability disclosure**
- **Resilient security measures with regular testing and auditing**

Incident reporting obligations have been streamlined and harmonized under NIS2. Organizations must now:

1. Report significant incidents within 24 hours of becoming aware of them.
2. Provide initial incident reports within 72 hours.
3. Submit final incident reports within one month.

This standardized approach ensures that relevant authorities are promptly informed of cyber incidents, enabling quick response and mitigation efforts. One of the most notable aspects of NIS2 is the increased emphasis on management responsibility and accountability.

Executives and board members are now directly responsible for implementing cybersecurity measures, ensuring NIS2 compliance, and providing resources and training for staff.

Managers may now be held personally liable for infringements. This shift in accountability underscores the critical role that leadership plays in driving cybersecurity excellence within organizations.

Most IT leaders (56%) feel their teams are not getting the leadership team support they need to meet the compliance deadline.

DORA: The sister law for financial institutions

While NIS2 covers a broad range of sectors, the Digital Operational Resilience Act (DORA) specifically targets financial institutions in the EU. DORA aims to harmonize and strengthen the cybersecurity requirements for the financial sector, ensuring that these organizations can withstand, respond to, and recover from cyber incidents.

Similar to NIS2, DORA places a strong emphasis on risk management, incident reporting and testing of ICT systems. Financial institutions will be required to implement robust cybersecurity measures, regularly assess their ICT risks and report significant cyber incidents to the relevant authorities.

DORA also introduces the concept of third-party risk management, requiring financial institutions to ensure that their ICT service providers adhere to strict cybersecurity standards. This highlights the importance of supply chain security and the need for organizations to consider the cybersecurity posture of their partners and vendors.

While DORA specifically targets the financial sector, its requirements are closely aligned with those of NIS2. Organizations that fall under the scope of both directives will need to ensure compliance with both sets of requirements, leveraging the synergies between the two to create a comprehensive cybersecurity framework.

Gearing up for NIS2: Your action plan

To effectively prepare for NIS2 compliance, organizations must take a proactive and comprehensive approach. The first step in this process is developing a clear action plan. This plan should outline the necessary steps, resources, and timelines for achieving compliance, ensuring that all stakeholders are aligned and working towards a common goal.

Once the action plan is in place, the next crucial step is conducting a thorough risk assessment. This involves identifying critical assets, processes and data that are essential to the organization's operations and evaluating the potential impact of cyber incidents on these elements. By assessing the organization's current cybersecurity posture against NIS2 requirements, gaps and areas for improvement can be identified, forming the basis for a robust compliance strategy.

Only 31% of IT leaders would label their current cyber hygiene as 'excellent'

Based on the findings of the risk assessment, businesses should develop and implement a comprehensive cybersecurity strategy aligned with NIS2 requirements. This strategy should encompass various elements, including:

- The establishment of an information security management framework
- The implementation of technical and organizational security measures
- The definition of incident response and business continuity plans
- The regular testing and auditing of security controls

By adopting a holistic approach to cybersecurity, organizations can ensure that they are well-prepared to meet the challenges posed by NIS2 and the evolving threat landscape.

For the successful implementation of NIS2, empowering leadership is crucial, ensuring that management understands the value of compliance and possesses the necessary competence to oversee and guide the organization's efforts effectively.

Establishing clear communication channels between leadership and IT/security teams is also essential, for facilitating informed decision-making. Regular updates on NIS2 compliance progress and risk mitigation efforts should be provided to leadership, ensuring they remain engaged and accountable throughout the compliance journey.

The price of non-compliance

Failing to comply with NIS2 can have severe consequences for organizations, both financially and reputationally. The directive introduces hefty fines for non-compliance, with penalties reaching up to:

- **€10 million,** *or*
- **2% of an organization's total worldwide annual turnover,** whichever is higher.

These substantial financial repercussions underscore the importance of taking NIS2 compliance seriously and investing in robust cybersecurity measures.

Beyond the financial impact, non-compliance (if an incident occurs) can also result in significant reputational damage:

- Erosion of trust and confidence from customers, partners and stakeholders
- Loss of business and negative publicity
- Long-term damage to brand reputation

Ultimately, non-compliance leaves businesses vulnerable to cyber incidents, which can cause severe operational disruptions and financial losses. A successful cyber attack can result in the theft or destruction of sensitive data, the interruption of critical services and the need for costly remediation efforts. The fallout from such incidents can be devastating, impacting an organization's bottom line, customer relationships and overall viability.

The legal and regulatory consequences of non-compliance are also significant. Organizations that fail to meet NIS2 requirements may face legal action, including lawsuits from affected parties and regulatory investigations. The time, resources and legal costs associated with defending against such actions can be substantial, further compounding the impact of non-compliance.

In light of these potential consequences, it is clear that the price of non-compliance with NIS2 is simply too high. Organizations must prioritize cybersecurity and take proactive steps to ensure compliance, safeguarding their assets, reputation and long-term success in an increasingly digital world.

82% of European chief risk officers (CROs) believe cybersecurity is the biggest business risk.

Aftra: Your partner in NIS2 readiness

Aftra is a leading provider of SaaS that empowers organizations to fortify their cybersecurity posture and work towards compliance with regulations like NIS2.

Attack surface management & vulnerability scanning: Armed with cutting-edge technology and seasoned expertise, Aftra's flagship offering revolves around vigilant monitoring of your external attack surface. By swiftly identifying and prioritizing vulnerabilities and misconfigurations, Aftra empowers organizations to preemptively thwart cyber threats, minimizing the risk of successful attacks.

Revealing hidden risks: Unveiling the clandestine realms of shadow IT and forgotten assets, Aftra identifies potential security blind spots. By shedding light on these overlooked vulnerabilities, organizations can quickly take remedial action, cementing a robust security posture.

Continuous risk assessment & monitoring: Aftra's vigilant eyes never waver, providing businesses with real-time insights into their cybersecurity posture. By continuously evaluating risks and staying abreast of evolving threat landscapes, organizations can maintain compliance with NIS2 mandates and fortify their resilience against emerging cyber threats.

Informed decision-making: Armed with data-driven insights, organizations can make informed decisions and allocate resources judiciously. By showcasing compliance through comprehensive reporting, Aftra helps organizations build trust with both stakeholders and regulators.

Proactive leadership support: Recognizing the pivotal role of leadership, Aftra provides the necessary insights and information to help organizations understand their cybersecurity landscape and meet the leadership requirements of NIS2. By empowering executive teams with this knowledge, Aftra enables leaders to foster a culture of cybersecurity awareness and accountability.

> **"At Aftra, we're more than just your NIS2 compliance partner – we're your trusted guide in navigating the ever-evolving cybersecurity landscape. Let us help you secure your organization's digital future."**
> ***– Aftra spokesperson***

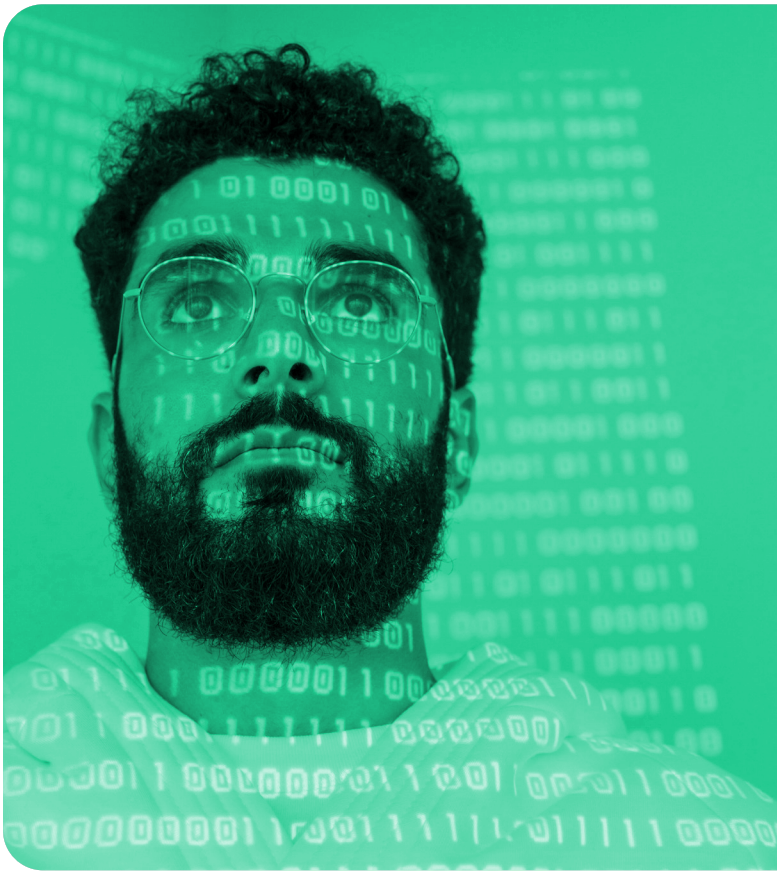
Conclusion: Embarking on your NIS2 journey

The introduction of NIS2 represents a significant milestone in the EU's ongoing efforts to create a more secure and resilient digital environment.

As organizations across a wide range of sectors face the challenge of complying with the new directive, it is essential to recognize the importance of proactive preparation and the value of partnering with trusted cybersecurity providers like Aftra.

By leveraging Aftra's cutting-edge solutions and deep expertise, organizations can navigate the complexities of NIS2 compliance with confidence, strengthening their cybersecurity posture and safeguarding their critical assets and reputation. Through continuous monitoring, risk assessment and expert guidance, Aftra empowers organizations to proactively address the evolving threat landscape and maintain a strong cybersecurity stance in the face of ever-growing digital risks.

Contact Aftra for more information or to schedule a consultation.



Sources:

https://digitalisationworld.com/news/67776/european-businesses-confident-they-will-reach-nis-2-compliance

https://www.i40today.com/action-required-on-new-nis2-regulation-for-two-thirds-of-european-businesses-says-sailpoint-as-12-month-countdown-begins/

https://www.ifcreview.com/news/2024/february/europe-cybersecurity-remains-the-top-risk-for-european-banks-on-a-12-months-horizon/