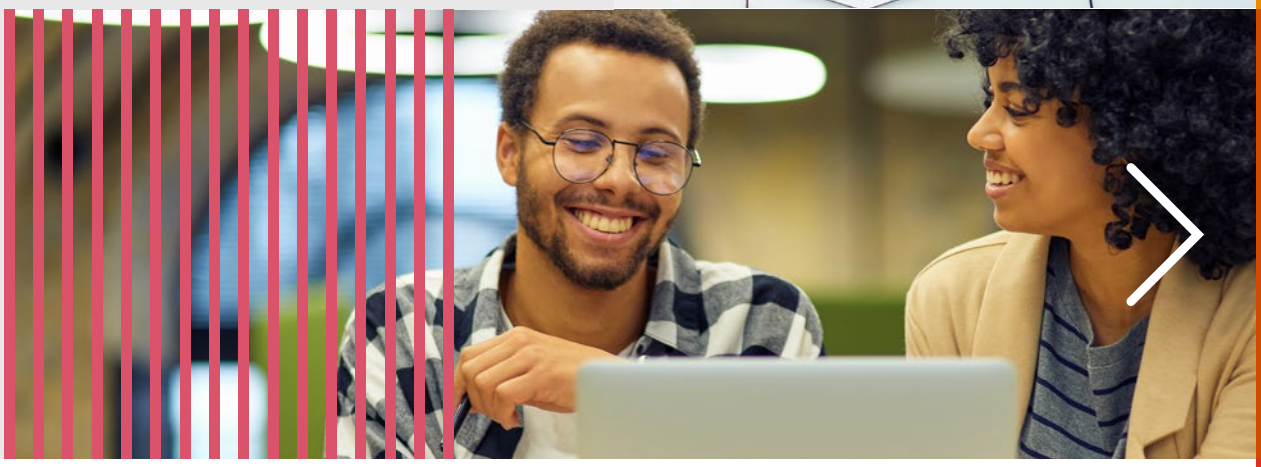
# Zero Trust and Compliance in Europe:



## Fostering cyber resilience in the Age of NIS2 and DORA

pwc

www.pwc.nl

# 1. Summary

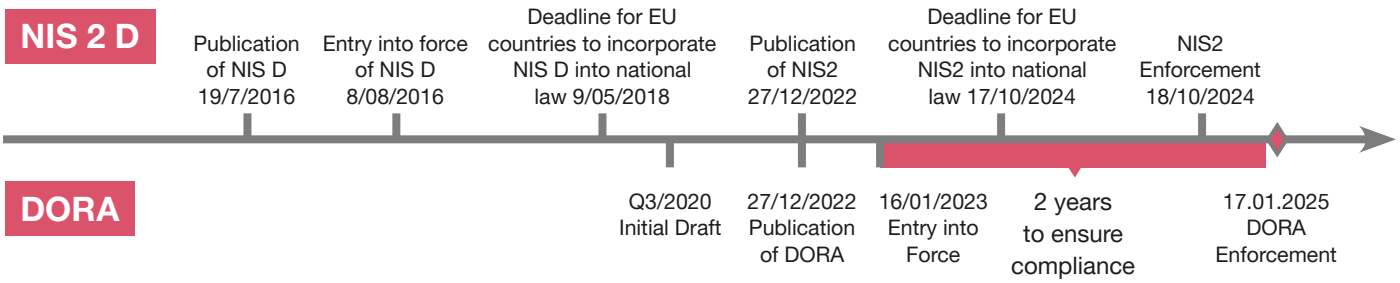
In an era of rapid digital transformation, Europe faces significant cybersecurity challenges, necessitating robust regulatory frameworks such as the Network and Information Systems Directive 2 (NIS2) and the Digital Operational Resilience Act (DORA). These regulations aim to enhance the resilience and security of critical infrastructure and financial institutions against an evolving threat landscape.

This paper explores the necessity of shifting from reactive compliance to a proactive and integrated approach. By embracing Zero Trust principles, organizations can effectively secure their IT assets, business processes, and people, ensuring continuous verification and alignment of security measures with business objectives. Zero Trust advocates for securing assets based on risk profiles, implementing least privilege access, and maintaining dynamic verification processes.

The adoption of Zero Trust principles facilitates proactive compliance, enabling organizations to stay ahead of regulatory mandates while fostering a culture of continuous improvement and resilience. This approach aligns with the requirements of not only NIS2 and DORA but also other emerging regulations such as the Critical Entities Resilience Directive (CER), the AI Act, the Data Act, and GDPR.

By integrating these principles, organizations can future-proof their cybersecurity strategies, ensuring they remain adaptable and resilient in the face of new and complex regulatory landscapes. This integrated compliance strategy not only meets current regulatory demands but also prepares organizations for future challenges, protecting digital assets and maintaining stakeholder trust in an increasingly interconnected digital environment.

## Regulation timelines




We know that several countries, including the Netherlands, will not meet the deadline for implementing the required regulation.

# 2. Decoding DORA and NIS2

When it comes to governance and guidance over cybersecurity, two significant legislations stand out for their impact on organizational resilience and risk management DORA and NIS2. These legislations, crafted with the evolving cyber threat landscape in mind, aim to reinforce the digital infrastructure and operational resilience of organizations across Europe. Let us delve into the essence of each directive before exploring their commonalities and differences.

**Introduction to DORA:**
DORA is a crucial initiative by the European Commission in relation to the resilience of financial markets and the real (EU) economy against cyber threats. Identifying a comprehensive framework as its basis, DORA is designed to harmonize cybersecurity regulations across EU Member States while ensuring operational continuity in the face of potential impactful disruptions. DORA sets a robust structure for enhancing the cybersecurity posture of financial institutions with its inclusion of pillars such as digital operational resilience governance, ICT and cyber risk management, incident management, resilience testing, third-party risk management, and information sharing. Furthermore, while DORA plays a pivotal role in enhancing the resilience of financial institutions, it also provides the European Financial Authorities (ESA) with valuable insights into critical elements, such as third-party ICT service providers, within the broader European financial system. This information is of utmost importance in comprehending the potential vulnerabilities and weaknesses that could lead to vast disruptions in the financial system.

**Introduction to NIS2:**
Parallel to DORA, the NIS2 addresses the broader landscape of cybersecurity, extending its reach beyond the financial sector. Rooted in the European Union's commitment to enhancing cybersecurity and resilience, NIS2 mandates essential and important organizations to adhere to stringent cybersecurity measures. From policies governing supply chain security to assessing the effectiveness of cybersecurity measures, NIS2 encompasses a wide array of directives aimed at fortifying the digital infrastructure and safeguarding critical assets against cyber threats.

**Commonalities:**
Although separated by their defined scopes and directed at distinct sectors, DORA and NIS2 share common objectives and principles that underpin their legislative frameworks. Both highlight the importance of establishing robust policies and governance programs over cybersecurity practices within organizations. They place effective incident handling mechanisms to detect, respond to, and recover from cyber incidents at the forefront of requirements. They both target individual entities but also include the disruption of the larger system as a whole, namely society. Moreover, DORA and NIS2 view business continuity management (BCM) programs as the foundation for resilience and advocate for the development and ongoing maintenance of BCM, ensuring that critical functions, processes and services remain operational amidst cyber disruptions.

**Differences:**
While DORA and NIS2 align on the overarching objective towards resilience, there are clear differences in their scope, emphasis, and being a lex specialis in general DORA is more stringent than NIS2. DORA, designed and tailored for the financial sector, focuses on specific aspects such as digital operational resilience governance and end-to-end risk management. In comparison, NIS2 takes a broader approach, addressing cybersecurity considerations across various domains, including supply chain security and systems development. In addition, NIS2 includes specific technical requirements such as encryption and multi-factor authentication. When we look at DORA and NIS2 both follow a risk-based approach, where entities are required to assess their risk profile, identify potential risks and monitor the threat landscape. In accordance with these risks, DORA mandates the implementation of technical requirements, such as an encryption policy that includes details on cryptographic key management and techniques.

NIS2 stays more on the general side of things and has less descriptive requirements. In general critical entities should adopt these practices based on industry standards and their own risk profile, and regularly update them to address emerging threats.

In conclusion, DORA and NIS2 are key milestones in the European Union's efforts to uplift and shine a light on cybersecurity and resilience across critical sectors. While they have been shaped towards the common goals of enhancing operational resilience and mitigating cyber risks, they have distinct differences that highlight the bandwidth of considerations for risk and resilience across sectors. Not only by putting policies and controls in place but also to train and test in advance. By understanding the commonalities and nuances of each legislation, organizations can navigate the legislative landscape effectively and enhance their cybersecurity posture in alignment not only with regulatory expectations, but also with evolving threats.

# 3. Proactive and integrated compliance: beyond ticking the box

In the preceding chapters, we explored the regulatory landscapes outlined by legislations such as NIS2 and DORA, which mandate organizations to secure their digital resilience through compliance with a set of requirements and obligations. While these legislations are well-intentioned and essential for mitigating cyber risks, they often pose significant challenges for organizations since they entail a substantial investment of resources, time, and money. From conducting comprehensive risk assessments to implementing robust cybersecurity measures and establishing governance frameworks, the compliance journey can be arduous and resource-intensive. Moreover, the dynamic nature of cyber threats and regulatory landscapes exacerbates the challenge, requiring regulations to continuously adapt and evolve their requirements.

The consequences of non-compliance with such regulations can be severe and far-reaching. Organizations may face legal penalties, reputational damage, and loss of customer trust in the event of non-compliance. Moreover, non-compliance undermines organizational resilience and exposes organizations to heightened cyber risks, potentially leading to data breaches, financial losses, and regulatory scrutiny.

Rather than viewing compliance as a box-ticking exercise, organizations should adopt a proactive approach that goes beyond mere regulatory adherence. Proactive compliance involves anticipating regulatory requirements and proactively implementing measures to strengthen cyber resilience and mitigate risks. By aligning cybersecurity initiatives with business objectives and leveraging advanced technologies and frameworks, organizations can stay ahead of regulatory mandates while fostering a culture of continuous improvement and innovation.

With technological advancement and evolving regulatory landscapes, organizations must future-proof their cyber security strategies to anticipate and adapt to emerging regulations effectively. You can do this by applying Zero Trust principles, which enable you to navigate regulatory complexities with agility and resilience.

In conclusion, proactive compliance offers a strategic imperative for organizations seeking to navigate the intricate web of regulatory requirements while promoting cyber resilience and future-proofing against emerging threats. By embracing proactive compliance as a strategic enabler of cyber resilience, organizations can not only ensure regulatory adherence but also fortify their defenses against evolving cyber threats, thereby safeguarding their digital assets and maintaining stakeholder trust in an increasingly interconnected and dynamic digital landscape.

# 4. Understanding Zero Trust as a Strategy

In the world of cybersecurity, strategies act like carefully made plans aiming for certain goals. These plans guide organizations through the complex relationship between business needs and security concerns. Like in building projects, the success of these strategies depends on how well they can adjust to the changing landscape of cyber threats. Old-fashioned perimeter-based security methods, once thought strong, now struggle against the constant and varied challenges of cybersecurity. Zero Trust (ZT) emerges as a strategic paradigm shift, advocating for a fundamental reassessment of trust assumptions within organizational networks. At its core, Zero Trust embodies a set of guiding principles that redefine how security is conceptualized, implemented, and maintained. In this chapter, we delve into the essence of Zero Trust, emphasizing its foundational principles and their significance in fostering cyber resilience.

**1. Security to Business Objectives Alignment**
Central to the Zero Trust philosophy is the alignment of security measures with overarching business objectives. Rather than viewing security as an isolated function, organizations must integrate it seamlessly into their operational fabric. This entails a holistic approach to risk management, where the protection of business processes and personnel takes precedence. By prioritizing controls based on asset sensitivity levels, organizations can tailor their security posture to mitigate risks effectively. Moreover, extending the culture of security across the supply chain ensures that cybersecurity practices are enforced consistently, bolstering resilience against external threats.

**2. Continuous Verification**
Zero Trust challenges the traditional notion of trust by advocating for continuous verification of entities accessing organizational resources. This principle emphasizes the dynamic nature of security, where trust is not assumed but rigorously verified. Continuous verification entails the use of diverse security controls and telemetry to assess the integrity of connections in real-time. Factors such as identity authentication, data criticality assessment, endpoint posture checks, and network hygiene are scrutinized to ensure that only authorized entities gain access. By monitoring connections persistently, organizations can swiftly detect and respond to any malicious activity, minimizing the impact of cyber incidents.

**3. Secure Assets by Risk**
A cornerstone of Zero Trust is the concept of securing assets based on risk profiles. Rather than applying blanket security measures, organizations deploy stringent controls where necessary, proportionate to the criticality of business operations. This risk-based approach enables resource optimization while maintaining robust protection against potential threats. Additionally, Zero Trust architecture orchestrates various security domains—such as identity, application security, data protection, network security, and endpoint security—through platforms like Policy Information Point (PIP), Policy Decision Point (PDP), and Policy Enforcement Point (PEP). Embracing policy as code facilitates the automation of security policies, ensuring scalability and adaptability in the face of evolving threats.

**4. Utilize Least Privilege**
Zero Trust advocates for the principle of least privilege, wherein entities are granted only the minimum permissions necessary to perform their designated tasks. By limiting access rights and privileges, organizations minimize the risk of unauthorized access and maintain data integrity. This granular approach to access control reduces the attack surface, mitigating the potential impact of security breaches.

In summary, by aligning security with business goals, implementing continuous verification, securing assets based on risk, and adopting least privilege principles, organizations can strengthen their defenses against modern threats while promoting a culture of cyber resilience.

# 5. Applying Zero Trust Principles to Support Compliance Efforts

Zero Trust (ZT) architecture emerges as a pivotal framework, offering a proactive approach to compliance that transcends traditional paradigms. By redefining trust assumptions, ZT enables organizations to fortify their defenses, align security initiatives with business imperatives, and adapt dynamically to emerging threats. Let's explore ow organizations can implement ZT principles to achieve proactive compliance effectively.

By aligning security measures with business objectives and fostering a culture where security is prioritized alongside business goals, organizations ensure that cybersecurity practices are tailored to address specific business needs. This alignment also resonates with regulatory requirements, emphasizing the importance of robust policies and governance frameworks that support business objectives while minimizing the risk of unauthorized access.

Since ZT also advocates for securing assets based on risk, prioritizing protection for critical assets will adopt a risk-based approach to security. In practice, this involves conducting comprehensive risk assessments to identify and prioritize critical assets, systems, and supply chain dependencies. Organizations will implement appropriate security controls and measures to mitigate risks effectively, aligning security investments with the level of business risk posed to each asset. This approach closely mirrors the regulatory focus on securing critical assets and ensuring operational resilience.

Continuous verification is another cornerstone of Zero Trust, emphasizing the need for ongoing assessment of security controls and practices. By continuously monitoring and analyzing network traffic, endpoint activities, and user behavior in real-time, organizations can promptly detect and respond to any malicious activity. This proactive approach to security aligns with regulatory requirements that emphasize the importance of assessing the effectiveness of cybersecurity measures and conducting continuous security training and education.

In summary, applying Zero Trust principles offers organizations a proactive strategy for compliance that goes beyond mere regulatory adherence. By aligning security measures with business objectives, securing assets based on risk, and continuously verifying the integrity of connections, organizations can fortify their defenses against emerging threats and regulatory scrutiny. While the specifics of Zero Trust principles and regulatory requirements may vary, the overarching goal remains the same: to foster a culture of cybersecurity resilience. In today's rapidly evolving cybersecurity landscape, adopting a proactive approach to compliance is not only essential for regulatory compliance but also for safeguarding critical assets and maintaining stakeholder trust.

# 6. Conclusion

In today's landscape, the intersection of cybersecurity and regulatory compliance is critical for organizational success. Throughout this paper, we've underscored the importance of adopting proactive and integrated strategies, particularly through Zero Trust (ZT) principles.

Zero Trust offers a pragmatic approach by challenging traditional trust assumptions and emphasizing continuous verification. By aligning security measures with business objectives, prioritizing asset protection based on risk, and enforcing the principle of least privilege, organizations can significantly strengthen their defenses while ensuring regulatory compliance.

Emerging threats like cloud-based attacks and ransomware underscore the urgent need for adaptive cybersecurity strategies. Zero Trust principles help organizations address these challenges by ensuring a consistent and rigorous approach to security across all organizational layers.

To embark on the journey towards proactive and integrated compliance, organizations should take the following first steps:

1. **Conduct a Comprehensive Risk Assessment:** Identify and prioritize critical assets, systems, and processes based on their risk profiles.
2. **Align Security with Business Objectives:** Ensure that cybersecurity measures support and enhance overall business goals and operations.
3. **Implement Continuous Verification:** Establish processes for ongoing monitoring and real-time assessment of network traffic, endpoint activities, and user behavior.
4. **Adopt the Principle of Least Privilege:** Limit access rights and permissions to the minimum necessary for individuals to perform their tasks, reducing potential attack surfaces.
5. **Integrate Security Across the Supply Chain:** Extend Zero Trust principles beyond the organization to include third-party vendors and partners, ensuring consistent security practices throughout.

In conclusion, the journey towards proactive and integrated compliance is ongoing. By embracing Zero Trust principles and a holistic cybersecurity approach, organizations can navigate regulatory complexities and emerging threats with confidence, protecting digital assets and preserving stakeholder trust. This strategic shift not only ensures regulatory adherence but also fosters a resilient and secure environment for sustained growth and innovation.


# 7. What can we do for you

PwC offers comprehensive support to assist your company in aligning with the legislations stipulated by DORA and NIS 2. Our services encompass evaluating your current state of preparedness, guiding the implementation of measures to fulfill statutory requirements, and integrating these measures into your risk management, security management, resilience management, and compliance management systems.

Additionally, our Zero Trust Assess and Design services are tailored to analyze your existing security architecture and formulate a customized Zero Trust strategy aligned with your organizational needs. We further provide Implement and Operate services that facilitate the practical execution of the Zero Trust strategy, ensuring its efficient operation and ongoing effectiveness.


# Contacts

*For further details or to initiate the assessment, design, or implementation process, please refer to the contact information provided below.*

**Bram van Tiel**
Partner Cybersecurity & Dataprivacy
E: bram.van.tiel@pwc.com
T: +31 (0)62 243 29 62

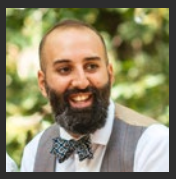
**Renske de Haan**
Senior Manager Advisory
E: renske.de.haan@pwc.com
T: +31 (0)68 136 61 55

**Ivo van Bennekom**
Digital Identity partner
E: ivo.van.bennekom@pwc.com
T: +31 (0)63 911 54 02

**Cate Pratt**
Manager Advisory
E: cate.p.pratt@pwc.com
T: +31 (0)68 136 28 90

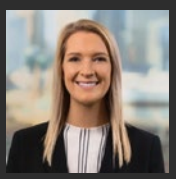
**Fadi Daood**
Senior Security Architect
E: fadi.daood@pwc.com
T: +31 (0)63 875 94 32

## About the Authors:



**Fadi Daood:** Fadi is an experienced Information Security architect leading PwC's Zero Trust community in EMEA.

**Renske de Haan:** Renske is an experienced crisis resilience consultant, guiding organizations to navigate challenges and build resilience through effective crisis management and business continuity



**Cate Pratt:** Cate is an experienced Crisis and Resilience consultant. Her specialised expertise lies in the areas of Business Continuity and Crisis Management