HORISEN®

MEETING NIS 2 AND DORA REQUIREMENTS IN THE CPaaS INDUSTRY

Building Compliant Messaging Technology Solutions:

Meeting NIS 2 and DORA Requirements

The amount of customer data captured online nowadays is growing at an exponential rate. Whether it's opening a bank account, buying a train ticket, or communicating with local government authorities, users are required to share basic personal information, including payment details, email addresses, and home addresses. The more data exchanged online, the greater the risk of data breaches.

In 2023 alone, over 2,800 reported data theft incidents compromised more than 8 billion records. Such breaches have a profound impact on consumer trust, which is the cornerstone of customer loyalty. According to PCI Pal, 83% of consumers would stop spending with a business for months following a security breach, and 21% might never return.

For messaging technology providers like HORISEN, adhering to and even exceeding security standards is essential for maintaining the trust and ensuring the highest level of data protection for our customers' businesses. Although we, as technology providers, are not directly obligated to comply with these standards, the impact of non-compliance can be significant for our customers. Therefore, as a trusted provider to telecom, governmental, and banking sectors, HORISEN's security experts rigorously monitor the latest updates and standards and prioritize aligning with the latest security frameworks such as the **NIS 2 Directive for cybersecurity** and the **Digital Operational Resilience Act (DORA)** to protect our clients' interests and ensure robust, compliant operations.

NIS 2
Directive

What is NIS 2 Directive?

The Network and Information Security Directive 2 (NIS-2) establishes a comprehensive framework for cybersecurity across the EU, developed in response to escalating threats in recent years. These evolving challenges have highlighted the urgent need to improve cybersecurity across the EU, especially to safeguard critical sectors.

In light of this, the EU Commission proposed a revision of the original NIS Directive in late 2020. The new NIS-2 Directive, published in December 2022, replaced the former regulations, setting higher standards for the security of network and information systems in EU member states. Under NIS-2, essential and significant entities are required to implement effective measures to manage and mitigate risks to their network and information systems, promoting a more resilient and secure EU digital landscape.

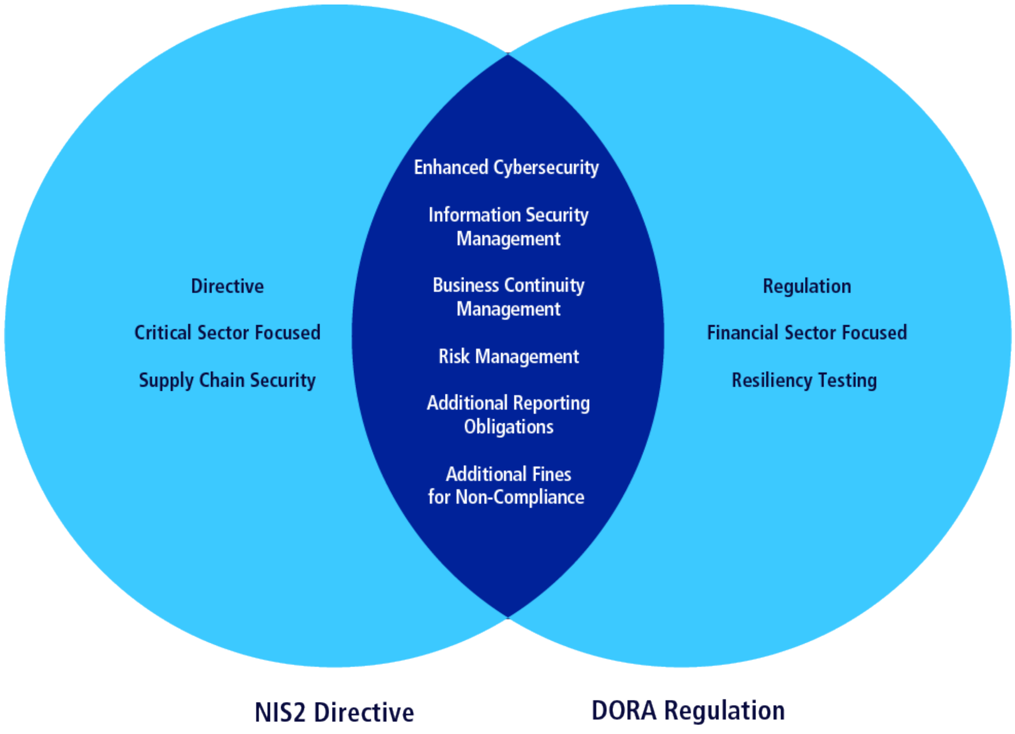
DORA

What is DORA?

The Digital Operational Resilience Act (DORA) is another critical piece of EU legislation that focuses on financial institutions' resilience against cybersecurity threats. It was introduced by the European Parliament and Council, with the aim to strengthen the operational resilience of digital systems across the European financial sector. It addresses regulatory gaps by setting specific rules for managing ICT-related incidents and enhancing resilience.

DORA significantly enhances the previous regulatory framework by expanding requirements for business continuity management, threat-led penetration testing, and third-party risk management, strengthening operational resilience for financial institutions. Unlike earlier regulations, DORA adopts a broader approach by addressing resilience from both institutional and systemic perspectives across Europe. Where DORA and NIS-2 overlap, particularly in relation to financial entities, DORA takes precedence, ensuring comprehensive protection tailored specifically to the financial sector.

NIS2 vs. DORA: Overlaps and Distinctions



Directive

Critical Sector Focused

Supply Chain Security

Enhanced Cybersecurity

Information Security Management

Business Continuity Management

Risk Management

Additional Reporting Obligations

Additional Fines for Non-Compliance

Regulation

Financial Sector Focused

Resiliency Testing

NIS2 Directive

DORA Regulation

HORISEN

HORISEN's Commitment to Industry Standards and Regulatory Compliance

As a pure software product house specializing in messaging technology, HORISEN has been committed to adhering to the highest security and compliance standards over the years to safeguard clients' interests in protecting their customers' data.

Hence at HORISEN, GDPR compliance is not just a legal requirement but a fundamental value. The General Data Protection Regulation (GDPR) is a comprehensive legal framework established by the European Union to protect personal data and privacy for all EU citizens. Therefore, every HORISEN product, service, and process is designed with GDPR in mind, ensuring that personal data is handled with the utmost care. We have a certified Data Protection Officer (DPO) who oversees the implementation of privacy policies and related documentation to guarantee that our platforms are GDPR-compliant. Moreover, continual optimization of our products and services ensures that our customers can confidently offer GDPR-compliant services to their clients.

Moreover, HORISEN's certification under ISO/IEC 27001:2022 underscores our commitment to safeguarding information security. This certification involves implementing processes, technical measures, and organizational practices to manage and mitigate risks. ISO/IEC 27001 is the global standard for information security management. It provides a systematic approach to managing sensitive company and customer information, ensuring that it remains secure.

In addition, ISO/IEC 27002, a supplementary guide to ISO/IEC 27001, offers best practices for implementing security controls within the ISO 27001 framework. Although certification is only available for ISO 27001, ISO 27002 plays a crucial role in enhancing the effectiveness of security measures. Notably, many ISO 27002 controls align with the requirements of other regulatory frameworks like DORA, making it a valuable reference for maintaining robust security practices.

Adapting to Evolving Standards Through Current Best Practices

Aligning with top security standards and practices continuously empowers companies to navigate new regulatory updates by establishing a strong foundation that simplifies compliance. This is precisely the case with **HORISEN**, whose adherence to ISO/IEC 27001:2022, ISO/IEC 27002, and GDPR compliance gives it a significant advantage in meeting the stringent requirements of NIS-2 and DORA. This proactive alignment not only supports regulatory readiness but also enhances resilience and trust.

The first step for HORISEN was to conduct a gap analysis to assess current alignment with new regulatory requirements, identifying areas that meet the standards and those needing further development and provide a clear roadmap for prioritizing efforts ensuring a structured approach to achieving full compliance with frameworks like NIS-2 and DORA.

Identifying Required Enhancements

After a thorough analysis of the standards, we currently adhere to alongside the latest requirements of NIS-2 and DORA, we have identified that HORISEN's existing ISO 27001 compliance provides a strong foundation for meeting these regulatory demands.

While NIS-2 does not explicitly mandate ISO 27001, it does encourage the use of international standards, such as the ISO/IEC 27000 series, for implementing cybersecurity measures. Consequently, HORISEN's ISO 27001 adherence enables us to meet 25 of the 26 cybersecurity requirements outlined in NIS-2, effectively positioning us for near-complete compliance.

DORA, meanwhile, focuses on rigorous ICT risk management, incident reporting, and resilience testing—all of which closely align with ISO 27001 standards. However, DORA requires additional measures in business continuity management, which can be supported by implementing ISO 22301, a complementary standard to ISO 27001 that enhances our resilience efforts.

Through our initial gap analysis, HORISEN has pinpointed key areas needing further enhancement to fully meet NIS-2 and DORA's specific requirements. While ISO 27001 remains a solid foundation, implementing targeted adjustments will ensure complete alignment with these advanced regulatory frameworks, further strengthening HORISEN's cybersecurity and operational resilience.

Defining Steps to Reach Compliance

NIS-2 Compliance:

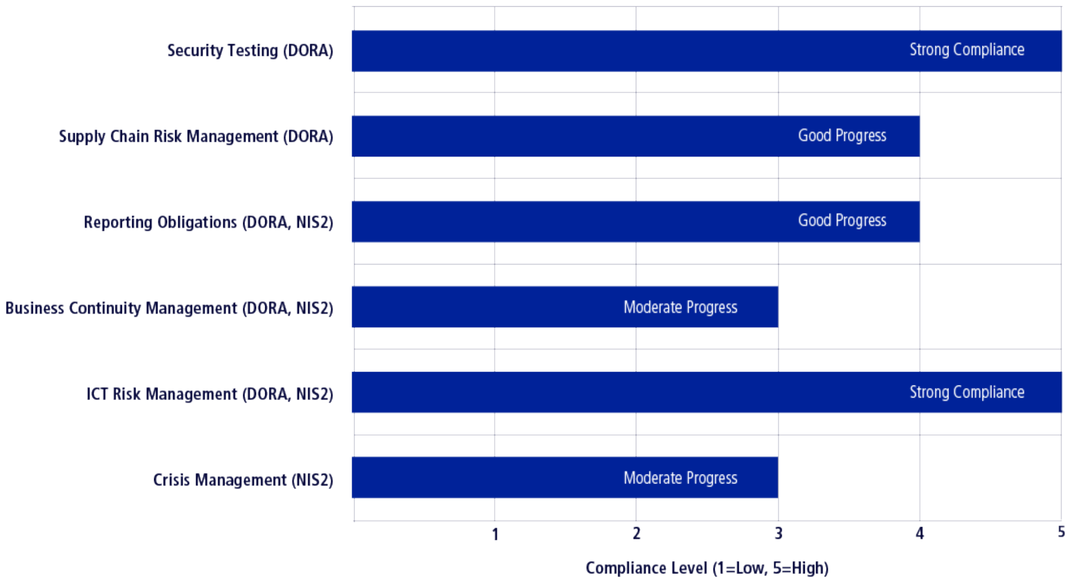
Coverage of Cybersecurity Requirements

While ISO 27001 covers 25 of 26 NIS-2 cybersecurity requirements, the gap lies in Crisis Management (Articles 9 and 16), where additional measures will be needed to comply with this aspect.

Reporting Obligations

NIS-2 Article 23 mandates detailed and specific reporting requirements that ISO 27001 alone cannot satisfy. Compliance with NIS-2 will require implementing a more robust incident reporting framework to meet these exacting standards.

Visual Representation of HORISEN's Compliance Progres



These specific regulatory requirements go beyond the measures already addressed by the ISO 27001 standard, where we achieve the highest compliance level (score 5). There is still room for improvement in crisis management and business continuity management (BCM), which can be enhanced through the adoption of ISO 22301 and recommendations outlined in the regulations.

DORA Compliance:

Alignment with ISO 27002 Controls

Many ISO 27002 controls map well to DORA's requirements, offering a solid base for cybersecurity measures.

However, while ISO 27001 alone may lack some of DORA's more comprehensive specifications for resilience, by including all ISO 27002 controls in our certification scope and Statement of Applicability (SOA), we are one step closer to meeting DORA requirements.

Business Continuity Management (BCM)

Although ISO 27001 includes certain business continuity management aspects, it does not cover all detailed requirements for implementing and maintaining BCM. DORA emphasizes a structured continuity approach, which can be achieved by adopting ISO 22301 as a complementary standard.

Supply Chain Risk Management

DORA imposes stringent requirements on managing risks associated with third-party ICT providers. While ISO 27001 partially addresses these risks, ISO 27036 provides a more detailed framework for supply chain risk management, meeting DORA's demands.

As HORISEN acts also as a cloud provider for our customers, we have a very strict and well-defined supply chain management process with a strong emphasis on vendor risk assessment – particularly for our main and most important vendors like data centres and ISP providers. To further mitigate risk, all key services and processes are performed and managed in-house.

Incident Reporting and Notifications

Articles 16 to 23 of DORA outline specific requirements for incident reporting and notification to customers, stakeholders, company management, and other financial entities. ISO 27001's reporting structure does not fully meet these extensive obligations, requiring enhancements to align with DORA. Accordingly, we have incorporated all additional DORA reporting requirements into our procedures to ensure compliance, including our obligations to report incidents in a specific format to designated institutions.

Enhanced Security Testing

DORA demands a more rigorous approach to security testing, requiring organizations to conduct resilience testing programs at least annually and perform threat-led penetration tests at least once every three years. ISO 27001's testing guidelines fall short of these intensive requirements, necessitating additional testing protocols to fully comply with DORA.

HORISEN already has in place annual third-party penetration tests conducted by specialized security experts, covering both web applications and infrastructure. This proactive approach ensures that we fulfil DORA's requirements for resilience and threat-led testing.

Closing the Gaps: Strengthening Compliance Efforts

To achieve full alignment with NIS-2 and DORA, HORISEN is taking proactive measures to minimize and eliminate identified gaps. Building on our ISO 27001 foundation, we are well on our way to achieving compliance with both frameworks. Our current focus is on enhancing crisis management and incident reporting processes to meet the stringent response times required by DORA and NIS-2. Additionally, we are aligning with ISO 22301 to build a resilient business continuity strategy and reach the final goal of being fully compliant with this standard as well. Furthermore, we are constantly improving our supply chain risk management taking into account ISO 27036 best practices.

Even prior to aligning with NIS-2 and DORA, HORISEN has been proactive in regularly updating employee training policies and integrating multi-factor authentication, in line with NIS-2's cybersecurity requirements. Furthermore, our critical services remain largely in-house, minimizing reliance on external suppliers, to ensure greater control and security.

These actions underscore our commitment to not only meet but exceed regulatory standards, reinforcing HORISEN's dedication to robust cybersecurity and operational resilience.

Setting the Standards for Safe and Reliable Messaging

In the messaging industry that is growing rapidly, security is not just an obligation - it's a competitive advantage. At HORISEN, we take pride in our proactive approach to security, ensuring that we meet and exceed industry standards to protect the data of our customers and their clients.

HORISEN recognizes the importance of staying ahead of security standards and regulations. We adhere to these high standards not out of obligation, but because our commitment to our customers' security and business growth drives us. Our priority is to ensure the most secure and reliable services, reflecting our dedication to their success.

This commitment extends to ensuring that our suppliers, such as data centres, also comply with these high standards. Our cloud services are hosted in Tier IV data centres in Switzerland, demonstrating this commitment through their advanced security concepts that meet the highest requirements. These partnerships enhance platform reliability, ensuring the utmost integrity and safeguarding clients' data with unparalleled diligence while complying with privacy laws.

Additionally, we conduct annual penetration tests to ensure that our systems remain resilient against potential threats and vulnerabilities.

By adhering to GDPR, ISO/IEC 27001/27002, NIS 2, and DORA, along with hosting our cloud services in most secure environment, we provide a secure foundation for our customers to build their own trusted services. This comprehensive approach ensures the highest levels of protection and reliability, supporting our customers in delivering secure and trustworthy services to their clients.

HORISEN®