369 CONSULT

Roadmap to NIS2 Compliance

What CISOs Need to Know

INTRODUCTION

This paper provides a comprehensive overview of the NIS2 Directive and its implications for entities within its scope. Each chapter will delve into the specifics of NIS2, offering insights, practical guidance, and technical advice tailored to help organizations understand and meet their obligations under the new regulation. Additionally, the paper will highlight how consultancy services provided by 369 consult can assist in navigating these complexities, ensuring effective compliance and enhanced cybersecurity resilience.

The NIS2 Directive represents a significant step forward in strengthening cybersecurity across the European Union. Expanding upon the original NIS Directive, NIS2 introduces stricter regulatory requirements and extends the scope to cover more sectors and digital services. It aims to bolster national cybersecurity capabilities, improve cooperation at the EU level, and ensure a high common level of cybersecurity across member states. This paper delves into the background of NIS2, outlines its key requirements, and provides practical guidance for compliance, specifically focusing on sectors newly classified as essential or important entities. By offering detailed insights into each aspect of the regulation, this guide aims to equip organizations with the knowledge needed to navigate their compliance journey effectively.

Background

The landscape of cybersecurity threats has evolved dramatically in recent years, with incidents becoming more frequent, sophisticated, and impactful. Recognizing the need for stronger and more cohesive cybersecurity measures across the European Union, the revised Directive on Security of Network and Information Systems (NIS2 Directive) aims to address these challenges by building upon the foundation laid by its predecessor, the NIS Directive.

Evolution from NIS to NIS2

The original NIS Directive, adopted in 2016, was the EU’s first piece of legislation aimed at enhancing cybersecurity across member states. It established legal measures to boost the overall level of cybersecurity in the EU, focusing on critical sectors such as energy, transport, banking, and healthcare. However, the rapid advancement of cyber threats and the increasing dependency on digital infrastructure necessitated a revision to expand the directive’s scope and strengthen its provisions.

The NIS2 Directive, proposed by the European Commission and adopted by the European Parliament and the Council, introduces significant updates to address these evolving challenges. It expands the directive's scope to cover a broader range of sectors and digital services, introduces stricter supervisory measures, streamlines reporting obligations, and enhances the framework for cooperation among member states.

Objectives of NIS2

The primary objectives of the NIS2 Directive are to:

- ✓ **Enhance National Cybersecurity Capabilities:** NIS2 mandates each member state to strengthen their national cybersecurity frameworks, including the establishment of a competent national authority for cybersecurity, a national single point of contact, and Computer Security Incident Response Teams (CSIRTs).

- ✓ **Improve Cooperation at the EU Level:** The directive aims to foster greater cooperation and information sharing among member states through the establishment of an EU-level cybersecurity crisis response framework.

- ✓ **Ensure a High Common Level of Cybersecurity:** By setting minimum cybersecurity requirements for entities in critical sectors and digital services, NIS2 seeks to raise the overall cybersecurity posture across the EU.

Scope and Applicability

NIS2 significantly broadens the directive's scope by including new sectors and types of entities. It introduces a distinction between "essential" and "important" entities, applying more stringent requirements to the former. Sectors now covered include energy, transport, banking, financial market infrastructures, health, digital infrastructure, public administration, and space. Moreover, the directive extends to providers of essential digital services such as online marketplaces, online search engines, and cloud computing services.

By addressing the shortcomings of the original NIS Directive and adapting to the current cybersecurity landscape, NIS2 aims to create a resilient and unified cybersecurity framework across the European Union. It underscores the collective responsibility of member states, regulatory authorities, and the private sector in safeguarding Europe's digital economy, society, and democracy from cyber threats.

In the following chapters, we will explore the key requirements of NIS2, its implications for essential and important entities, and provide practical guidance for achieving compliance with the directive.

Key NIS2 Requirements

The NIS2 Directive introduces a comprehensive set of requirements aimed at ensuring a high level of cybersecurity across all covered entities within the European Union. These requirements are designed to address the diverse aspects of cybersecurity risk management, incident reporting, supply chain security, and national supervisory measures. By understanding and implementing these key requirements, entities can significantly enhance their cybersecurity posture and resilience against cyber threats.

1. Risk Management Measures

NIS2 mandates the implementation of risk management measures across both technical and organizational domains. These measures are critical for the identification, assessment, and mitigation of cybersecurity risks. Key aspects include:

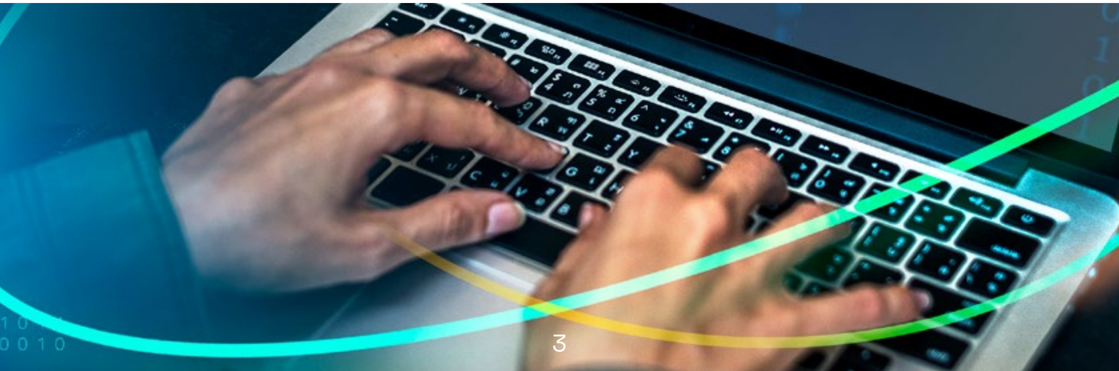
✓ **Security Policies and Procedures:** Entities are required to establish and maintain cybersecurity policies that address risk management, incident handling, and business continuity.

✓ **Network and Information System Security:** The adoption of technical solutions and practices that ensure the security and resilience of networks and information systems.

✓ **Incident Handling:** The development of capabilities to detect, respond to, and recover from cybersecurity incidents, minimizing their impact on services and users.

✓ **Business Continuity and Crisis Management:** The preparation of business continuity plans and crisis management protocols to ensure service continuity in the event of an incident.

✓ **Supply Chain Security:** The assessment and management of cybersecurity risks arising from the supply chain and service dependencies.



2. Incident Reporting Obligations

A crucial aspect of NIS2 is the obligation for entities to report significant cybersecurity incidents. The directive emphasizes timely and effective reporting to ensure that competent authorities and, where relevant, the public are informed. Reporting obligations include:

- ✓ **Timely Notification:** Entities must notify the relevant national authority of significant incidents without undue delay, typically no later than 24 hours after becoming aware of the incident.
- ✓ **Detailed Reporting:** Follow-up reports providing detailed information on the incident's impact, the measures taken, and the lessons learned are required.

3. Supply Chain Security

Recognizing the interconnected nature of today's digital services, NIS2 places a strong emphasis on managing cybersecurity risks in the supply chain. Entities are expected to:

- ✓ **Conduct Due Diligence:** Evaluate the cybersecurity practices and policies of third-party suppliers and service providers.
- ✓ **Establish Secure Contracts:** Ensure that contracts with third parties include clear provisions on cybersecurity requirements and incident reporting.
- ✓ **Monitor Compliance:** Regularly assess the cybersecurity posture of third parties to ensure ongoing compliance with contractual and regulatory requirements.

4. National Supervisory Measures

NIS2 strengthens the role of national authorities in supervising and enforcing cybersecurity measures. It introduces more robust supervisory frameworks to ensure compliance:

- ✓ **Stricter Supervision:** National authorities are empowered to conduct audits, review risk management practices, and verify the adequacy of security measures.
- ✓ **Enforcement Powers:** Authorities can impose administrative fines and other sanctions on entities that fail to comply with NIS2 requirements.
- ✓ **Cooperation and Information Sharing:** National authorities are expected to collaborate and share information on cross-border incidents and threats to enhance collective cybersecurity resilience.

Implications for Essential and Important Entities

The NIS2 Directive introduces significant implications for entities classified as either “essential” or “important.” This distinction is crucial for understanding the level of obligations and the intensity of regulatory scrutiny these entities will face. This chapter outlines the specific requirements and considerations for these entities under NIS2, providing insight into how they can navigate the enhanced regulatory landscape.

Definition and Classification of Entities

NIS2 categorizes entities into two groups based on their importance to the economy and society: essential and important entities. Essential entities operate in sectors considered critical for maintaining vital societal functions, such as energy, transportation, banking, and healthcare. Important entities, while not critical, still provide important services within sectors like digital infrastructure, post and courier services, waste management, and manufacturing of critical products.

The classification impacts the level of obligations and the extent of regulatory oversight, with essential entities subject to more stringent requirements due to the potentially higher impact of disruptions in their operations.

Sector-Specific Requirements

NIS2 lays down sector-specific cybersecurity and incident reporting requirements to address the unique risks and challenges faced by different sectors. For instance, entities in the energy sector must ensure the resilience of their infrastructure against physical and cyber threats, while digital service providers must focus on safeguarding data integrity and availability. Understanding these sector-specific requirements is vital for entities to tailor their cybersecurity strategies effectively.

Cross-Border Implications

Given the digital and interconnected nature of many services, NIS2 also addresses the cross-border implications of cybersecurity incidents. Entities operating across EU borders must be aware of their obligations in each member state and ensure compliance with the national regulations implemented under NIS2. This includes reporting incidents to the relevant national authorities and participating in cross-border information sharing and cooperation initiatives.

Navigating Compliance Challenges

For essential and important entities, the implementation of NIS2's requirements necessitates a comprehensive review and enhancement of their current cybersecurity practices. Key steps include:

1 **Risk Assessment and Management:** Entities must conduct regular and thorough risk assessments to identify vulnerabilities and implement appropriate security measures tailored to their sector-specific needs.

2 **Enhanced Incident Response:** Developing and testing incident response plans to ensure readiness in the face of cyber incidents is crucial. This includes establishing clear communication channels for timely incident reporting.

3 **Supply Chain Due Diligence:** Entities need to assess the cybersecurity risks associated with their suppliers and service providers, ensuring that their supply chain does not introduce vulnerabilities into their operations.

4 **Regulatory Engagement:** Keeping abreast of national regulatory developments and requirements is essential for cross-border operators. Engaging with national authorities and participating in industry-specific information-sharing initiatives can provide valuable insights and support compliance efforts.

The successful implementation of NIS2's requirements will not only enhance the cybersecurity resilience of individual entities but also contribute to the overall security and stability of the European Union's digital market. In the next chapters, we will provide practical guidance on achieving compliance with NIS2, focusing on risk management, incident reporting, supply chain security, and more.

Practical Guidance for Compliance

Achieving compliance with the NIS2 Directive requires a proactive and comprehensive approach to cybersecurity. This chapter provides practical guidance on key areas of compliance, offering actionable insights and strategies for essential and important entities to enhance their cybersecurity posture and align with NIS2 requirements.

IT Risk Management

Risk Management is a critical component in the NIS2. It focuses on developing a comprehensive risk management framework for entities to identify, assess, manage, and mitigate cybersecurity risks effectively. It emphasizes the importance of aligning the framework with international standards and incorporating both organizational and technical measures to safeguard information assets against cyber threats.

Requirement

Under the NIS2 Directive, entities are required to establish robust risk management practices that encompass the following:

- ✓ A clear and standardized approach to risk assessment methodologies.
- ✓ Regular assessments to proactively identify vulnerabilities and threats.
- ✓ The implementation of security measures tailored to the identified risk levels.
- ✓ Continuous monitoring and review of the risk environment and the effectiveness of security controls.
- ✓ These requirements aim to ensure that entities have the necessary policies, procedures, and technologies in place to manage cybersecurity risks effectively.

Practical Guidance

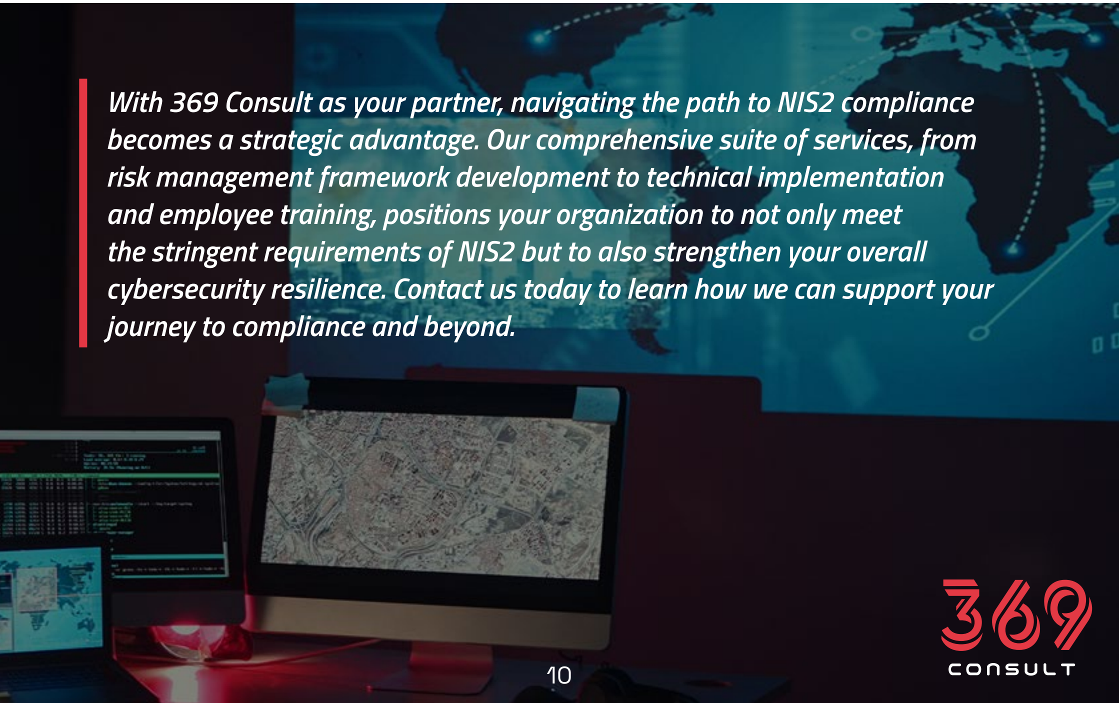
To comply with NIS2 risk management requirements, entities should consider the following practical steps:

1. **Develop a Risk Management Framework:** Create a framework based on international standards like ISO/IEC 27001, defining clear methodologies for assessing and managing cybersecurity risks.
2. **Conduct Regular Risk Assessments:** Schedule periodic assessments to identify new vulnerabilities, assess potential threats, and evaluate the impact on organizational assets.
3. **Implement Tailored Security Measures:** Based on risk assessment findings, deploy appropriate security controls to mitigate identified risks, ensuring these measures are proportionate to the threat level.
4. **Establish Continuous Monitoring Processes:** Implement processes and tools for ongoing monitoring of the cybersecurity landscape and the performance of security measures, adjusting policies and controls as necessary.

Technical Insights

To enhance risk management capabilities, entities may leverage the following technical solutions and strategies:

- ✓ **Advanced Detection Technologies:** Utilize SIEM systems and intrusion detection systems (IDS) to monitor network and system activities for signs of unauthorized access or anomalies.
- ✓ **Access Control Mechanisms:** Apply stringent access control measures, including multi-factor authentication (MFA) and role-based access controls, to limit access to sensitive information and systems.
- ✓ **Data Encryption:** Encrypt critical data both at rest and in transit using strong encryption standards to protect against data breaches and unauthorized access.
- ✓ **Physical Security Controls:** Implement physical security measures such as secure data center practices and access control systems to prevent physical tampering and unauthorized access to critical infrastructure.
- ✓ **Cybersecurity Training Programs:** Conduct regular cybersecurity awareness training for employees to educate them on safe practices, phishing awareness, and the significance of adhering to organizational security policies.



> *With 369 Consult as your partner, navigating the path to NIS2 compliance becomes a strategic advantage. Our comprehensive suite of services, from risk management framework development to technical implementation and employee training, positions your organization to not only meet the stringent requirements of NIS2 but to also strengthen your overall cybersecurity resilience. Contact us today to learn how we can support your journey to compliance and beyond.*

Incident Reporting

Incident Reporting is a critical process required by NIS2 directive. It outlines the steps entities must take to ensure timely detection, reporting of cybersecurity incidents, and the development of detailed incident response plans. These measures are pivotal in minimizing the impact of incidents and ensuring a coordinated response.

Requirement

The NIS2 Directive emphasizes the importance of robust incident reporting mechanisms, requiring entities to:

✓ Implement technologies and processes for the early detection of cybersecurity incidents.

✓ Develop protocols for the swift internal reporting and escalation of incidents.

✓ Train employees on their roles in the detection and reporting processes.

✓ Facilitate rapid and efficient communication with national authorities regarding cybersecurity incidents.

✓ Create comprehensive incident response plans detailing organizational response strategies.

Practical Guidance

Entities aiming to fulfill these requirements can follow this practical guidance:

1 **Develop and Implement Detection Mechanisms:** Utilize advanced detection systems, like SIEM, to monitor network and system activities for potential security incidents continuously.

2 **Formalize Reporting Procedures:** Establish clear protocols for internal reporting, ensuring that incidents are promptly escalated to the appropriate personnel or teams.

3 **Comprehensive Staff Training:** Conduct regular training sessions for all staff members to enhance their understanding of incident detection and reporting procedures.

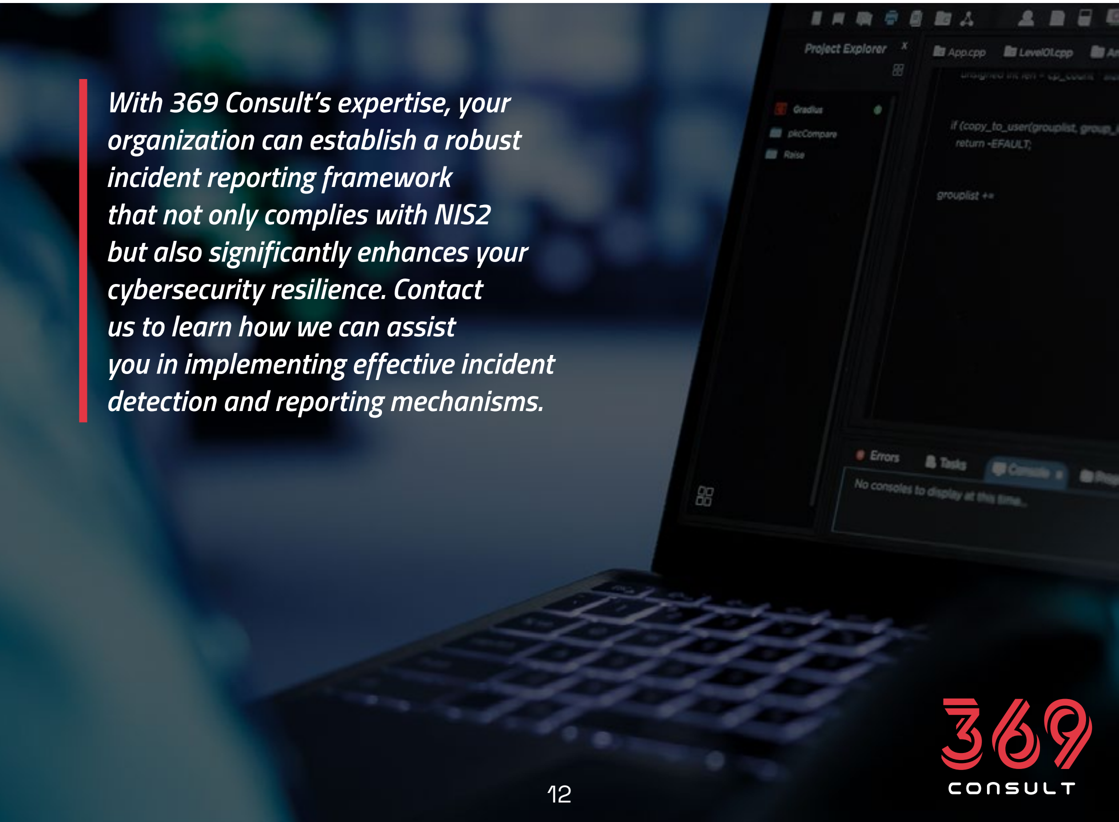
4 **Communication with Authorities:** Set up direct and secure communication channels with relevant national authorities for efficient incident notification.

5 **Incident Response Planning:** Craft detailed incident response plans that define roles, responsibilities, and communication strategies for managing and recovering from cybersecurity incidents.

Technical Insights

To enhance incident reporting capabilities, entities may consider the following technical strategies:

- ✓ **SIEM System Utilization:** Deploy SIEM systems to aggregate and analyze data from various sources within the IT infrastructure, providing real-time analysis of security alerts generated by network hardware and applications.
- ✓ **Automated Alerting Mechanisms:** Implement automated alerting systems that notify designated personnel of potential incidents, facilitating quicker response times.
- ✓ **Incident Response Platforms (IRPs):** Use IRPs to coordinate response activities, track the status of ongoing incidents, and maintain detailed records for post-incident analysis.
- ✓ **Secure Communication Tools:** Employ encrypted communication tools for safe reporting to national authorities, ensuring the confidentiality and integrity of transmitted information.



> *With 369 Consult's expertise, your organization can establish a robust incident reporting framework that not only complies with NIS2 but also significantly enhances your cybersecurity resilience. Contact us to learn how we can assist you in implementing effective incident detection and reporting mechanisms.*

Supply Chain Security

Securing the supply chain is a critical component of an entity’s overall cybersecurity posture under the NIS2 Directive. It outlines the necessary steps for conducting rigorous supplier risk assessments, incorporating cybersecurity clauses in contracts, and engaging in continuous monitoring and evaluation of third-party service providers. These measures are essential for mitigating risks that third parties may introduce into the entity’s information systems and operations.

Requirement

The NIS2 Directive highlights the importance of comprehensive supply chain security, requiring entities to:

- ✓ Evaluate the cybersecurity practices and compliance of suppliers and third-party service providers.
- ✓ Include explicit cybersecurity requirements in contracts with suppliers, covering aspects like incident reporting, data protection, and audit rights.
- ✓ Implement mechanisms for the continuous monitoring and assessment of third-party cybersecurity postures to ensure they meet contractual and regulatory standards.

Practical Guidance

To comply with the NIS2 supply chain security requirements, entities can adopt the following approaches:

1. **Rigorous Supplier Risk Assessments:** Develop and implement a standardized process for assessing the cybersecurity risks associated with each supplier. This should involve evaluating their security policies, practices, and compliance with relevant cybersecurity standards and regulations.
2. **Cybersecurity Clauses in Contracts:** Negotiate and incorporate specific cybersecurity clauses in contracts with all suppliers. These clauses should clearly outline the cybersecurity expectations, incident reporting protocols, data protection measures, and the entity’s rights to conduct audits.
3. **Continuous Monitoring and Evaluation:** Establish a program for the ongoing monitoring of suppliers’ cybersecurity postures. This could include regular security assessments, reviews of compliance certifications, and analysis of security incident reports.

Technical Insights

Leveraging technology can significantly enhance an entity's ability to manage supply chain security:

✓ **Vendor Risk Management Software:** Utilize specialized software solutions to automate the assessment and monitoring of suppliers' cybersecurity risks. These platforms can help in aggregating risk data, facilitating risk analysis, and tracking compliance over time.

✓ **Secure Information Sharing Platforms:** Implement secure platforms for exchanging information with suppliers, ensuring that sensitive data is protected during communications.

✓ **Automated Compliance Monitoring Tools:** Employ tools that can automatically monitor suppliers' adherence to contractual cybersecurity requirements, alerting the entity to any deviations or potential risks.

> *Partnering with 369 Consult enables entities to not only meet the NIS2 supply chain security requirements but also to build resilient operations protected against third-party cyber risks. Our expertise in cybersecurity, contractual negotiations, and risk management positions us as your ideal partner in securing your supply chain. Contact us to learn more about how we can support your efforts in achieving robust supply chain security.*

Cybersecurity Governance

Cybersecurity governance is focusing on establishing robust governance structures and fostering a culture of cybersecurity awareness within organizations. Effective cybersecurity governance is essential for ensuring that cybersecurity efforts are aligned with the organization's strategic objectives and regulatory requirements, including those set forth by the NIS2 Directive

Requirement

Under the NIS2 Directive, entities are required to:

✓ Establish clear governance structures for cybersecurity, ensuring dedicated leadership and accountability for cybersecurity initiatives.

✓ Appoint a chief information security officer (CISO) or an equivalent role responsible for overseeing cybersecurity strategies and coordinating efforts across the organization.

✓ Develop and implement comprehensive training and awareness programs to educate all staff members about their role in cybersecurity and inform them of current cyber threats and safe practices.

Practical Guidance

To effectively meet the NIS2 cybersecurity governance requirements, entities should consider the following strategies:

1. **Establishing Cybersecurity Governance Structures:** Create formal governance frameworks that define roles, responsibilities, and accountability for cybersecurity within the organization. This includes forming a dedicated cybersecurity committee or board that oversees cybersecurity policies and strategies.
2. **Appointment of a CISO or Equivalent Role:** Designate a CISO or equivalent senior executive with the authority and resources to lead cybersecurity efforts, ensure compliance with NIS2, and foster collaboration across different departments.
3. **Cybersecurity Training and Awareness Programs:** Develop a continuous education program that includes regular training sessions, cybersecurity awareness campaigns, and updates on the latest cyber threats and defense mechanisms. This program should be mandatory for all employees, regardless of their role or level within the organization.

Technical Insights

Effective cybersecurity governance can be supported by leveraging technology and best practices:

✓ **Cybersecurity Management Platforms:** Utilize integrated cybersecurity management platforms that provide a centralized view of the organization's cybersecurity posture, risk management activities, and compliance status.

✓ **Automated Training Solutions:** Implement e-learning platforms and simulation tools that offer interactive and engaging cybersecurity training and awareness content to employees, facilitating better retention and understanding of key concepts.

✓ **Real-time Threat Intelligence:** Incorporate real-time threat intelligence feeds into the organization's cybersecurity strategy to inform decision-making and ensure that governance structures are responsive to the evolving threat landscape.

> *With 369 Consult as your partner, you can strengthen your cybersecurity governance structures and culture, ensuring not only compliance with NIS2 but also building a resilient and aware organizational environment. Contact us to discover how we can help you establish a robust cybersecurity governance framework and promote a culture of cybersecurity awareness across your organization.*

Awareness and Training

This part emphasizes the importance of developing and delivering targeted training programs as part of an organization's cybersecurity strategy, in line with the NIS2 Directive's requirements. It highlights the necessity of tailoring training to the varied roles within an organization, ensuring that each employee understands the specific cybersecurity risks and responsibilities associated with their position. Additionally, it underscores the importance of regularly updating training content to reflect the latest cybersecurity trends, threats, and best practices.

Requirement

Under the NIS2 Directive, entities are mandated to:

- ✓ Develop cybersecurity training programs that are customized to the diverse roles within the organization, addressing the unique cybersecurity challenges and responsibilities of each position.
- ✓ Ensure that cybersecurity training materials are regularly reviewed and updated to incorporate the latest information on cybersecurity threats, trends, and protective measures.

Practical Guidance

To effectively implement awareness and training programs that meet NIS2 requirements, entities should consider the following approaches:

1. **Customized Role-Based Training:** Design training programs that are specifically tailored to the roles and responsibilities of different employee groups within the organization. This includes identifying the specific cybersecurity risks each role may encounter and providing the necessary knowledge and tools to mitigate those risks.
2. **Dynamic Training Content Updates:** Establish a process for continuously monitoring the cybersecurity landscape and incorporating relevant updates into the training curriculum. This could involve engaging with cybersecurity experts, attending industry conferences, and subscribing to threat intelligence feeds.
3. **Engaging Training Methodologies:** Utilize a variety of training methodologies to engage employees and enhance learning outcomes. This may include interactive e-learning modules, workshops, simulations, and gamified learning experiences.
4. **Measuring Training Effectiveness:** Implement mechanisms to assess the effectiveness of training programs, such as quizzes, practical exercises, and feedback surveys. Use the results to refine training approaches and content.

Technical Insights

The deployment of technology can significantly enhance the effectiveness of cybersecurity awareness and training programs:

- ✓ **E-Learning Platforms:** Leverage advanced e-learning platforms that allow for the creation of interactive and engaging training content, easily accessible to all employees.
- ✓ **Cybersecurity Simulations:** Use simulation tools to create realistic cybersecurity scenarios that employees can navigate, helping to build practical skills and awareness in a controlled environment.
- ✓ **Learning Management Systems (LMS):** Employ an LMS to track employee training progress, manage training content, and identify areas where additional training may be needed.

> *With 369 Consult's support, your organization can establish a culture of cybersecurity awareness, ensuring that all employees are equipped with the knowledge and skills to contribute effectively to your cybersecurity defenses. Contact us to learn how we can help you develop and deliver targeted, up-to-date training programs that meet and exceed NIS2 requirements.*

Due Dates and Compliance Timeline for NIS2

The adoption of the NIS2 Directive represents a significant step forward in strengthening cybersecurity across the European Union. As member states work to transpose the directive into national law, entities within the scope of NIS2 must prepare to meet new and expanded cybersecurity obligations. Understanding the timeline for these changes is crucial for effective planning and compliance.

Transposition of the Directive

Entry into Force: The NIS2 Directive is expected to enter into force following its publication in the Official Journal of the European Union. From this date, member states typically have a 21-month period to transpose the directive into national law, although this period may vary based on legislative processes and priorities within each member state.

National Transposition Deadline: By this deadline, member states must have adopted and published the necessary national legislation to comply with NIS2. This marks a critical point for entities, as the requirements of NIS2 begin to take legal effect at the national level.

Compliance Obligations for Entities

Initial Compliance Period: Following the transposition of NIS2 into national law, entities will have a grace period to achieve compliance with the new requirements. This period may range from 6 to 12 months, providing entities with time to assess their current cybersecurity practices, identify gaps, and implement necessary measures.

Ongoing Compliance and Reporting: Entities are required to maintain ongoing compliance with NIS2 requirements, including regular risk assessments, incident reporting, and adherence to cybersecurity governance practices. Specific reporting deadlines for incidents and other regulatory obligations will be defined in the national legislation.

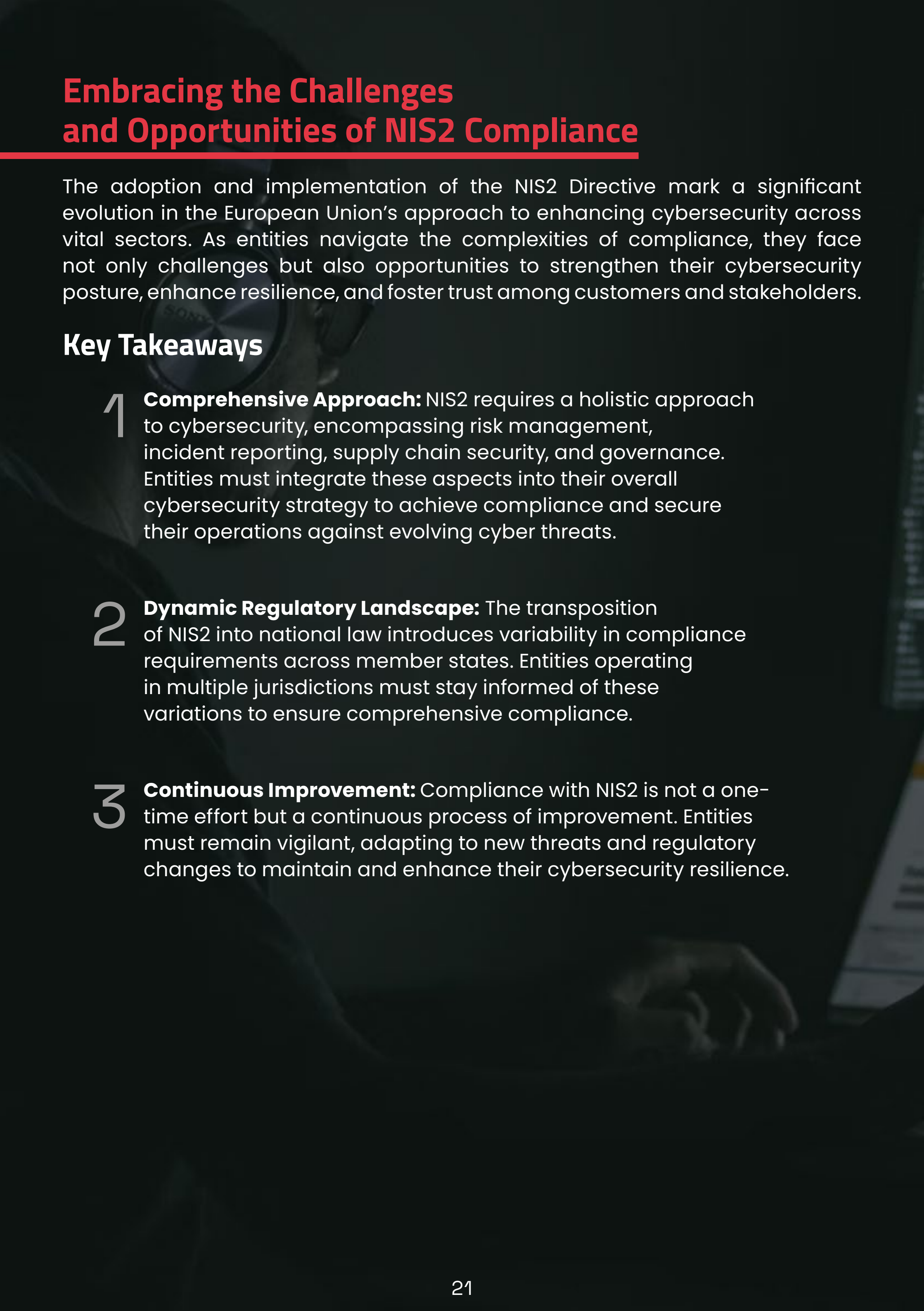
Key Milestones

1 **Awareness and Preparation (Pre-Transposition):** Entities should begin preparing for NIS2 compliance ahead of the national transposition deadline. This includes staying informed about the legislative process, understanding the potential impact of NIS2, and starting preliminary assessments of cybersecurity practices.

2 **Gap Analysis and Planning (Post-Transposition):** Immediately following the transposition, entities should conduct a comprehensive gap analysis to determine the steps needed to achieve compliance. Developing a detailed action plan with timelines for implementation of required measures is essential.

3 **Implementation and Adjustment Period:** During the initial compliance period, entities should focus on implementing the identified measures, training staff, and establishing or refining cybersecurity governance structures. This period may also involve adjustments based on guidance from national authorities or lessons learned during implementation.

4 **Compliance and Continuous Improvement:** After meeting the initial compliance requirements, entities must focus on maintaining compliance and continuously improving their cybersecurity posture in response to evolving threats and regulatory expectations.



Embracing the Challenges and Opportunities of NIS2 Compliance

The adoption and implementation of the NIS2 Directive mark a significant evolution in the European Union's approach to enhancing cybersecurity across vital sectors. As entities navigate the complexities of compliance, they face not only challenges but also opportunities to strengthen their cybersecurity posture, enhance resilience, and foster trust among customers and stakeholders.

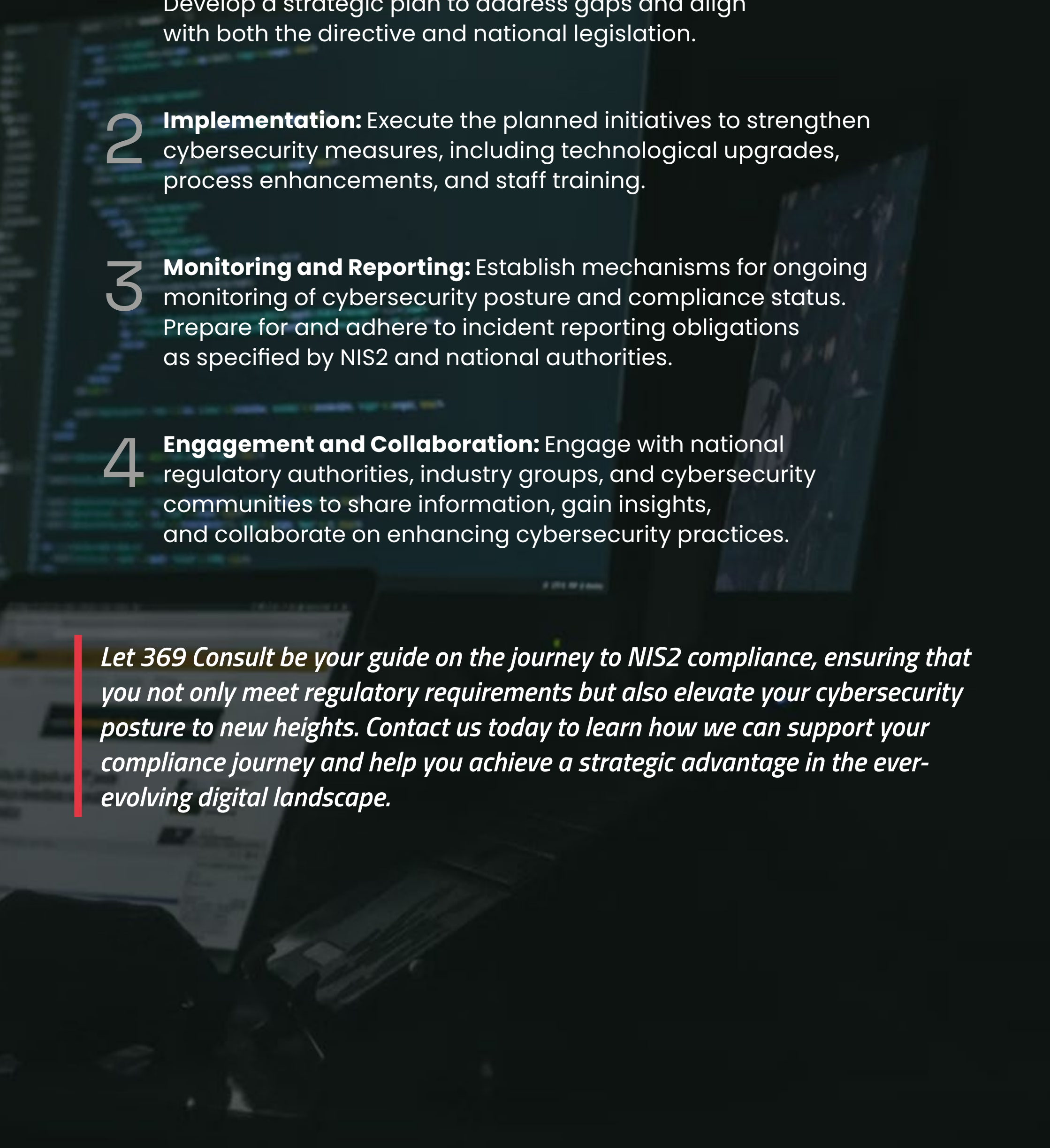
Key Takeaways

1 **Comprehensive Approach:** NIS2 requires a holistic approach to cybersecurity, encompassing risk management, incident reporting, supply chain security, and governance. Entities must integrate these aspects into their overall cybersecurity strategy to achieve compliance and secure their operations against evolving cyber threats.

2 **Dynamic Regulatory Landscape:** The transposition of NIS2 into national law introduces variability in compliance requirements across member states. Entities operating in multiple jurisdictions must stay informed of these variations to ensure comprehensive compliance.

3 **Continuous Improvement:** Compliance with NIS2 is not a one-time effort but a continuous process of improvement. Entities must remain vigilant, adapting to new threats and regulatory changes to maintain and enhance their cybersecurity resilience.

Next Steps for Entities



1. **Assessment and Planning:** Conduct a thorough assessment of current cybersecurity practices against NIS2 requirements. Develop a strategic plan to address gaps and align with both the directive and national legislation.

2. **Implementation:** Execute the planned initiatives to strengthen cybersecurity measures, including technological upgrades, process enhancements, and staff training.

3. **Monitoring and Reporting:** Establish mechanisms for ongoing monitoring of cybersecurity posture and compliance status. Prepare for and adhere to incident reporting obligations as specified by NIS2 and national authorities.

4. **Engagement and Collaboration:** Engage with national regulatory authorities, industry groups, and cybersecurity communities to share information, gain insights, and collaborate on enhancing cybersecurity practices.

> *Let 369 Consult be your guide on the journey to NIS2 compliance, ensuring that you not only meet regulatory requirements but also elevate your cybersecurity posture to new heights. Contact us today to learn how we can support your compliance journey and help you achieve a strategic advantage in the ever-evolving digital landscape.*

How 369 Consult Can Support Your Journey to NIS2 Compliance

At 369 Consult, we understand the intricacies of navigating the NIS2 compliance landscape. Our team of experts is equipped to guide entities through every step of their compliance journey, offering a range of services designed to ensure not just compliance, but also a strategic advantage in cybersecurity resilience.

Tailored Compliance Strategies: We develop customized compliance strategies that address the unique challenges and opportunities of your organization, ensuring an effective path to NIS2 compliance.

Technology Implementation and Optimization: Our expertise in cutting-edge cybersecurity technologies enables us to assist entities in selecting and implementing the right solutions to meet NIS2 requirements, optimizing existing systems for maximum efficiency and security.

Training and Awareness Programs: We design and deliver comprehensive training and awareness programs that empower your staff with the knowledge and skills necessary to contribute to your organization's cybersecurity and compliance goals.

Regulatory Insight and Liaison:

With our deep understanding of the regulatory landscape, we provide valuable insights into national transpositions of NIS2 and act as a liaison between entities and regulatory authorities, ensuring clear communication and compliance alignment.

The path to NIS2 compliance presents both challenges and opportunities for entities across the European Union. By taking proactive steps to understand and implement the directive's requirements, organizations can not only achieve compliance but also significantly strengthen their cybersecurity defenses.

With 369 Consult as your partner, you gain access to expert advice, tailored solutions, and comprehensive support designed to navigate the complexities of NIS2 compliance effectively. Together, we can turn the challenge of compliance into an opportunity for growth and resilience.

369
CONSULT

For more information please contact:

Alexandru Hritcu
Partner Cyber Security & Risk
✉ alexandru.hritcu@369consult.com

369 CONSULT

What you do matters.
Let’s make it more secure.

www.369consult.com

What you do matters.
Let’s make it more secure.

369
CONSULT

www.369consult.com