

The logo features a stylized white wolf head silhouette on the left, facing right, and a grey oak leaf silhouette on the right, facing left. They are positioned to appear as if they are meeting in the middle.

Wolf and Oak

Mastering NIS2 Compliance

What is NIS2?

Cybersecurity is no longer a luxury—it's a necessity. With the introduction of the NIS2 Directive, the European Union has intensified its efforts to strengthen cybersecurity across the continent. For many Organizations this means facing new responsibilities and adhering to stricter regulations.

The NIS2 Directive, which stands for the Network and Information Systems Directive 2, mandates comprehensive cybersecurity measures to protect critical infrastructure and essential services.

To ensure compliance, companies must understand the directive's requirements, implement robust security measures, and prepare for potential audits. Understanding and acting on these obligations is crucial for maintaining robust cybersecurity and avoiding the penalties associated with non-compliance.

EU Directive

The NIS2 Directive was adopted by the European Union on December 14, 2022, and came into effect on January 16, 2023. Member states, including Ireland, have been given until October 17, 2024, to transpose the directive into national law. This means that by this date, all companies within the scope of the directive must fully comply with its requirements.

It is crucial for businesses in Ireland to use this time to thoroughly understand the directive, assess their current cybersecurity measures, and implement the necessary changes to ensure compliance by the deadline.



What's Different?

NIS Directive (NIS1)

NIS2 Directive (NIS2)

Scope	Limited to specific sectors (energy, transport, etc)	Broader scope, includes more sectors
Entities Covered	Primarily essential service operators and digital service providers	Essential & important entities, with detailed classifications
Security Requirements	General security measures	Stringent security measures, including supply chain security
Incident Reporting	Incidents with significant impact	Clearer, stricter incident reporting requirements & timelines
Governance	Varies among member states	Stronger management accountability with clear roles
Cooperation Mechanisms	Limited EU -level cooperations	Enhanced EU cooperation with peer reviews & joint supervision
Penalties for Non-Compliance	Varies among member states	Harmonised, stricter penalties across member states
National Authorities	Establishment of national competent authorities	Strengthened national authorities with clear mandates & resources
Risk Management	Basic risk management requirements	Comprehensive risk management with regular assessments
Cross Border Collaboration	Limited	Improved cross-border collaboration and information sharing

Scope Determination

Companies are classified as “essential” or “important” depending on their sector and the effect their services have on the public and economy.

IMPORTANT

250 EMPLOYEES | €50 TURNOVER | €43 BALANCE

- ENERGY
- TRANSPORT
- BANKING
- FINANCIAL SERVICES
- HEALTH
- DRINKING WATER
- DIGITAL INFRASTRUCTURE
- ICT SERVICE MANAGEMENT
- PUBLIC ADMINISTRATION
- SPACE

ESSENTIAL

50 – 249 EMPLOYEES | €10 – €50 TURNOVER | €10 – €43 BALANCE

- POSTAL & COURIER
- WASTE MANAGEMENT
- CHEMICALS
- FOOD
- MANUFACTURING
- DIGITAL PROVIDERS
- RESEARCH ORGANISATIONS

Non Compliance



Financial Penalties

- Fines: Up to €10 million or 2% of global annual turnover, whichever is higher.

Enforcement Actions

- Mandatory implementation of specific security measures within a specified timeframe.
- Suspension or withdrawal of certifications for non-compliant entities.
- Temporary ban on activities posing

Legal Consequences

- Potential lawsuits from affected parties seeking damages for cybersecurity incidents.
- Increased Scrutiny
- More frequent and rigorous audits and inspections by regulatory authorities.

Reputational Damage

- Public announcement of non-compliance incidents, leading to reputational harm. significant cybersecurity risks.

Operational Impact

- Higher costs associated with addressing regulatory findings, implementing measures, and managing legal and reputational issues.

Deadline Approaches: Urgent Action Required for Irish Companies

Although NIS2 isn't yet incorporated into Irish regulation, the deadline remains unchanged. Companies must prepare to comply or face severe penalties and potentially devastating operational disruptions when the regulations are enforced.



Pragmatic Approach

Navigating the complexities of the NIS2 Directive requires a structured and methodical approach.

Using an essential will help your organization systematically plan and achieve compliance with the new cybersecurity regulations.

By breaking down the process into clear, actionable steps, we aim to simplify your journey towards securing your networks and information systems. Whether you are an essential or important entity, following these guidelines will ensure that you meet the stringent requirements of NIS2, protect your critical infrastructure, and avoid the significant penalties associated with non-compliance.

Don't wait for the hammer to fall—start your compliance journey now and safeguard your organization against potential operational disruptions.



Step by Step Guide



How we help?

Our comprehensive services and experts can ensure that your organization achieves compliance & strengthens its cybersecurity posture. Here's how we can help:

- **Comprehensive Gap Analysis:** Our experts will conduct a thorough assessment of your current cybersecurity measures against NIS2 requirements, identifying gaps and areas for improvement.
- **Tailored Action Plans:** We will work with you to develop a customized action plan that addresses identified gaps, prioritising actions based on risk and impact.
- **Implementation Support:** Wolf Oak provides hands-on support to implement necessary security measures, from deploying advanced technologies to conducting staff training sessions..
- **Incident Response Planning:** We help establish clear protocols for detecting, responding to, and reporting cybersecurity incidents, ensuring you meet NIS2's stringent reporting requirements.
- **Expert Guidance and Support:** With Wolf Oak, you gain access to a team of cybersecurity experts who are dedicated to helping you navigate regulatory complexities and safeguard your business.

The NIS2 Directive is a critical step towards enhancing cybersecurity across the EU.

Compliance is not just about avoiding penalties—it's about protecting your business and customers from cyber threats. By understanding the requirements and taking proactive measures, you can turn compliance into a strategic advantage.

Start by conducting a thorough analysis, investing in necessary measures, and continuously monitoring your cybersecurity posture. Remember, in the digital age, robust cybersecurity is the foundation of a resilient business.

With Wolf and Oak by your side, you can confidently navigate the path to NIS2 compliance and beyond.



“ We provide no-nonsense pragmatic advice on taking your business to the next level, drawing on decades of experience delivering "first time right" solutions. ”

Enable Strategic Development, Make The Right Investments, Unlock Your Digital Advantage.



WolfandOak

READY. STEADY. **GROW.**

wolfandoak.com