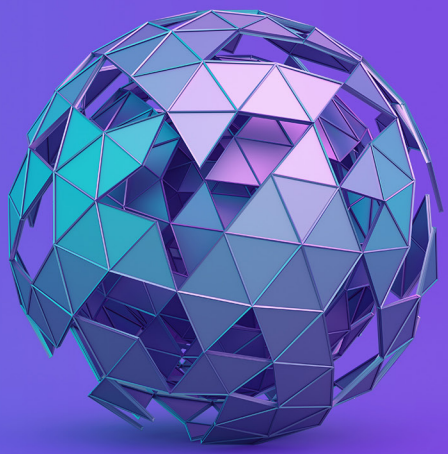
NIS2 readiness—How KPMG LLP (KPMG) can help you prepare

Critical infrastructure organizations must act now



The burning platform

Organizations must act now to comply with the European Union's NIS2 Directive, even as Member States continue transposing it into national law. With the Directive now in effect and detailed requirements being finalized, organizations cannot wait for local implementation to begin their compliance journey. Only a few Member States have fully transposed the directive, yet all covered organizations must ensure they meet the stringent cybersecurity requirements to avoid severe penalties.

Who must comply?

Essential entities (High criticality)

- Energy and utilities
- Digital infrastructure and DNS providers
- Transport and logistics
- Space technology operators
- Healthcare providers
- Government administration
- Banking and financial markets
- Water/wastewater management

Important entities (Annex II)

- Manufacturing operations
- Chemical producers
- Food production and distribution
- Digital service providers
- Postal/courier services
- Research organizations
- Waste management

Critical business impacts

- Dramatically expanded scope: From **5,000** to over **160,000** entities now in scope across critical sectors
- Substantial financial risk: Fines up to **€10M/2%** global revenue (essential entities) or **€7M/1.4%** revenue (important entities)
- Personal accountability: Management boards face direct liability and potential restrictions across all board positions
- Stringent reporting: **24-hour** mandatory incident notification plus regular status updates required
- Supply chain scrutiny: New requirements for assessing and managing third-party cybersecurity risks
- Cross-border compliance: Organizations must comply even if local laws aren't yet updated

Your path to NIS2 compliance: Our established four-phase approach

1. **NIS2 impact assessment and scoping**
2. **Cyber risk and resilience design**
3. **Security controls implementation**
4. **Continuous compliance management**

NIS2 success stories

Transforming cybersecurity across industries

A European energy leader's journey

Leading a major utilities provider through their NIS2 transformation, we established a thorough cybersecurity program that easily operates across borders. By integrating supply chain controls with board-level governance, we created a model that other energy providers now follow for regulatory compliance.

Healthcare innovation meets security

For a growing healthcare technology company, we architected a security framework that protects sensitive patient data while enabling innovation. The solution delivers round-the-clock incident response capabilities and robust vendor risk management—essential elements for NIS2 compliance in the healthcare sector.

Manufacturing excellence in action

Working with a global manufacturing leader, we strengthened operational technology security across multiple European facilities. The program unified cybersecurity practices across their industrial systems while maintaining production efficiency—proving that security and productivity can coexist.

Why work with KPMG?

Your NIS2 transformation deserves more than a checklist approach. We bring together deep regulatory knowledge, established methodologies, and practical experience to deliver lasting results. Our integrated IT/OT security capabilities and cross-border knowledge help ensure your program works across all operations. Most importantly, we understand your industry's unique challenges and have the frameworks to address them.

Contact our NIS2 professionals

Sai Gadia
Partner, Cyber Security Services
T: 612-382-7620
E: sgadia@kpmg.com

Lekshmy Sankar
Director, Cyber Security Services
T: 303-296-2323
E: lekshmysankar@kpmg.com

Some or all of the services described herein may not be permissible for KPMG audit clients and their affiliates or related entities.

Learn about us: **kpmg.com**