Texas Cyber Security
Your Digital Security Guard

EU NIS2

WHAT IS EU NIS2?

EU NIS2 is the latest directive established by the European Union to strengthen cybersecurity and resilience across critical sectors. Building on the original NIS (Network and Information Systems) Directive, NIS2 introduces enhanced requirements for risk management, incident reporting, and cooperation among member states. This directive aims to ensure that organizations operating in essential sectors like energy, transportation, and healthcare, as well as providers of digital services, implement adequate cybersecurity measures to protect against disruptions and cyber threats.

EU NIS2 not only addresses the evolving landscape of cyber threats but also mandates a higher level of security across the supply chain. The directive emphasizes the need for organizational, technical, and operational measures to mitigate risks and ensure business continuity.

WHAT ORGANIZATIONS MUST COMPLY WITH EU NIS2?

EU NIS2 applies to a wide range of organizations that are considered essential to the functioning of society and the economy within the European Union. This includes both public and private entities across various sectors:

Energy Companies: Organizations involved in the generation, transmission, and distribution of electricity, oil, and gas are required to adhere to EU NIS2 to safeguard critical energy infrastructure.

Healthcare Providers: Hospitals, pharmaceutical companies, and other healthcare services must comply with EU NIS2 to protect patient data and ensure the uninterrupted delivery of healthcare services.

CMGRC_DATASHEET_EU-NIS2-1.jpg

Financial Institutions: Banks, insurance companies, and other financial service providers are required to implement NIS2 measures to protect against cyber threats that could disrupt financial stability.

Transport Operators: Entities involved in air, rail, water, and road transport must comply with EU NIS2 to ensure the security and resilience of critical transportation networks.

Digital Service Providers: Cloud service providers, online marketplaces, and search engines must implement EU NIS2 standards to protect the integrity and availability of digital services.

EU NIS2 Compliance Focus Areas

Risk Management and Security Policies

Organizations under the EU NIS2 Directive must conduct thorough risk assessments and develop strong security policies for their information systems. This includes regularly updating policies and procedures to ensure all cybersecurity measures are effective and up to date.

Cryptography and Data Protection

Compliance requires using cryptography, including encryption policies, to protect sensitive data. These measures must be implemented where relevant to secure information assets.

Incident Handling and Response

Organizations need a clear plan for handling security incidents, ensuring they are managed with minimal disruption. This includes procedures for incident detection, reporting, and response.

System Security and Vulnerability Management

Security must be embedded in the procurement, development, and operation of systems, with procedures in place for handling and reporting vulnerabilities throughout the system lifecycle.

Employee Training and Data Access Security

Cybersecurity training and basic computer hygiene are essential. Organizations should provide ongoing education, particularly for employees with access to sensitive data, and maintain secure procedures for data access.

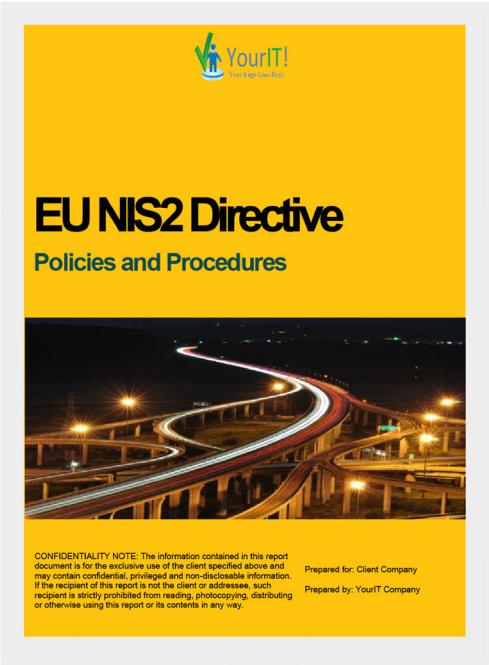
Business Continuity and System Access

To ensure continuity during and after security incidents, organizations must have up-to-date backups and plans for maintaining IT system access. This includes multi-factor authentication and encryption for communications.

Supply Chain Security

Supply chain security is crucial. Organizations must assess and manage risks associated with suppliers, implementing measures tailored to each supplier's vulnerabilities and conducting overall security assessments across the supply chain.

CMGRC_DATASHEET_EU-NIS2-2.jpg



AUTOMATED ASSESSMENTS & REPORTS

Ensuring compliance with EU NIS2 – as well as all your other IT requirements – is easy with Compliance Manager GRC. You get more work done with less labor, thanks to automated data collection, automated management plans, and automated document generation.

AFFORDABLE FOR ALL

Compliance Manager GRC is affordable, yet boasts the power and functionality most often found in expensive, enterprise-class governance, risk, and compliance platforms. Whether you manage compliance for your own organization or are an MSP delivering compliance-as-a-service, there's a sensible subscription for you.

REQUEST A DEMO TODAY

Request a Demo Today and discover the advantages of Compliance Manager GRC — the purpose-built compliance management platform for IT professionals.

CMGRC_DATASHEET_EU-NIS2-4.jpg

STREAMLINE YOUR EU NIS2 COMPLIANCE WITH EASE – NO EXPERTISE REQUIRED!

Compliance Manager GRC is simple to use, and you don't have to be a compliance expert to perform a robust EU NIS2 assessment. Compliance Manager GRC guides you through each requirement using an intuitive, interactive assessment dashboard. In less than 30 minutes, you can perform a Rapid Baseline Assessment to gain a high-level overview of your EU NIS2 compliance posture.

As you dive deeper into your assessment, you can leverage an array of automated IT scanning tools to collect technical data as evidence of compliance. Likewise, you can import data from other Kaseya 365 solutions to determine instantly whether you meet a specific compliance requirement.

Best of all, you can track all compliance standards in scope for your IT operations simultaneously and on the same dashboard, regardless of the source.

EMPOWER YOUR ENTIRE TEAM FOR EU NIS2 COMPLIANCE – COLLABORATIVE TOOLS FOR EVERY STAKEHOLDER

Compliance Manager GRC doesn't just allow a single auditor to evaluate and demonstrate compliance with EU NIS2. It provides you with tools to engage the entire team in your compliance effort, including internal stakeholders, subject matter experts, and even external auditors.

- Track your progress in remediating technical and compliance issues from the Plan of Action & Milestones, a unified assessment dashboard. You can also export identified issues in the form of tickets to Autotask, where your tech team can move into action.
- Instantly generate Policies and Procedures to guide EU NIS2 implementation across the organization.
- Make it easy for personnel to read and acknowledge policies and receive cybersecurity training with the built-in Employee Portal. Managers can quickly access a dashboard to track employee compliance.
- Engage third-party vendors outside of the organization in assessing their cybersecurity posture with the Vendor Portal.

UNLOCK POWERFUL FEATURES WITH COMPLIANCE MANAGER GRC

- **Rapid Baseline Assessments** – Quickly identify gaps where you are not compliant with the EU NIS2 standard before performing comprehensive Controls and Requirements assessments.
- **Technical Risk Assessments** – Leverage a comprehensive set of automated data collection tools to perform a full risk assessment and meet the EU NIS2 security requirements.
- **Auditor's Checklist** – Provide easy access for auditors to quickly verify compliance with every requirement.
- **Plan of Action & Milestones** – Track and manage the tasks needed to achieve compliance.
- **Policies and Procedures Manuals** – Access automated documentation for everything you and your team need to do.
- **BullPhish ID Integration** – Deploy your entire BullPhish library of training content to jumpstart end-user training.
- **Kaseya 365 integration** – Import data from other Kaseya products you frequently use directly into your assessment as evidence of compliance. This includes technical data such as proof of patch management, backups for endpoints, and evidence of two-factor authentication.

CMGRC_DATASHEET_EU-NIS2.jpg