

EVIDEN

servicenow®

Digital Fortitude

Enhancing Resilience in the Age of Cyber Evolution

Protecting the Systems that Power Europe

“

Cyber security threats facing the UK are evolving all the time. What was not even considered a risk five to six years ago is now a potential threat. We need to be adaptable in the face of this changing threat landscape and our legislation needs to be adaptable too.

– Julia Lopez MP,
Minister of State for Media,
Data, and Digital Infrastructure

”



The NIS2 Directive, also known as the new version of the Network and Information Security Directive, is a European directive aimed at strengthening cybersecurity in the European Union (EU). The Directive is designed to help organizations protect themselves against cyber threats and to ensure that the EU's cyber infrastructure is more secure and robust. Now that the directive has been officially published, member states must integrate the provisions of the directive into local legislation from **17 October 2024**. This EU legislation can greatly impact the requirements for cybersecurity and organizations should start preparing by defining their compliance roadmap and optimizing their cybersecurity awareness.

Outside of EU? Why does it matter to you?

The NIS2 Directive is a significant update to the original NIS Directive, impacting global supply chains, enhancing cyber resilience, influencing regulatory measures, and ensuring data protection and privacy. It extends its influence beyond the EU, promoting a secure and resilient digital environment globally.



“

This European directive will help around 160,000 entities to strengthen their grip on security and make Europe a safe place to live and work. The law should also allow for the sharing of information with the private sector and partners around the world. If we are attacked on an industrial scale, we have to react on an industrial scale

”

– Dutch MEP Bart Groothuis

Source: <https://www.europarl.europa.eu/news/en/press-room/20221107IPR49608/cybersecurity-parliament-adopts-new-law-to-strengthen-eu-wide-resilience>

So what does this mean to you?

The NIS2 Directive has broadened its reach to include medium and large entities across various critical sectors, enforcing uniform rules to bolster cybersecurity. Initially focused on sectors like healthcare and transport, it now encompasses areas such as banking, digital infrastructure, and even 'very critical sectors' like water supply and ICT management. Entities deemed 'essential' due to their societal impact, like public communications networks, are also covered. Small and micro-enterprises are generally exempt unless they hold significant societal or economic importance, in which case member states must ensure their compliance with the directive. This expansion aims to enhance the resilience of organizations against the backdrop of advancing cyber risks as businesses digitize their assets.

It is imperative that organizations act now, or risk penalties, fines or criminal sanctions:

1. Non-monetary Penalties	<ul style="list-style-type: none"> • Compliance orders and binding instructions • Security audit implementation orders • Threat notification orders to entities' customers 	
2. Administrative Fines	Essential Entities: <ul style="list-style-type: none"> • Transport • Finance energy • Water • Space • Health • Public administration • Digital infrastructure • maximum fine level of at least €10,000,000 or 2% of the global annual revenue, whichever is higher. 	Important Entities: <ul style="list-style-type: none"> • Foods • Digital providers • Chemicals • Postal services • Waste management • Research • Manufacturing • maximum fine level of at least €7,000,000 or 1.4% of the global annual revenue, whichever is higher.
3. Criminal Sanctions for Management	<ul style="list-style-type: none"> • Publication of compliance violations • Publication of natural and legal person(s) responsible for violations • Management position bans for repeated violations (EE) 	

In a rapidly evolving digital landscape, there's no time to delay. The NIS2 Directive is a call to action, urging organizations to proactively enhance their cybersecurity measures. Waiting for individual country interpretations isn't an option. It's time to act swiftly and decisively to align with NIS2 and fortify our digital defenses.



The challenges

Compliance challenges include:

- Viability of Assets / IT Infrastructure
- Communication between Risk, Security and TPRM
 - Security and risk operate in silos, leaving both functions with blind spots
 - Compliance status of 3rd and nth parties is unknown
- Proactive Resilience and Continuity Management
 - Disparate systems create delays in collating service, operations, risk, security data
 - Dependencies of services, processes and systems are unknown or out of date
- Stricter reporting requirements e.g. incident notification timeline
- Complexity of regulatory compliance as each country has its own interpretation
- Enterprises are not simple organizations and will touch different countries and overlap with existing frameworks.
- Manual nature of most approaches today.

Every entity falling within the scope of NIS2, whether deemed essential or significant, must adhere to their responsibility for protection. The directive outlines a range of mandatory measures that service providers must meet. These includes examples such as:

- Formulating risk analysis policies and ensuring information system security.
- Vigilance in crisis management and maintaining operational continuity in the face of significant cyber incidents.
- Guaranteeing the security of the supply chain.
- Upholding a duty of care to secure network and information systems.
- Implementing cryptography and encryption.
- Establishing policies and procedures to evaluate the efficacy of risk management measures.



So what is the answer?

Eviden, together with ServiceNow are uniquely placed to work collaboratively and innovatively to revamp your business's approach to managing and assessing NIS2 compliance with the Now Platform®. By interconnecting individuals, operations, and systems within your organization, we leverage the NIS2 Workspace to visualize data concerning the Common Security Principles (CSPs) and gauge compliance with the Directive through Integrated Compliance Management. Our top-tier implementation and guidance merge digital, cloud, big data, and security business segments to provide a swift and sturdy NIS2 management solution. Eviden's extensive experience in collaborating with Essential Services ensures that your strategy aligns with industry best practices from the project's inception through to operational launch and beyond.

Eviden's NIS2 Compliance Management (N2CM) solution powered by ServiceNow is a toolset that enables the efficient policy-based and automated maintenance of continuous compliance for customers in all geographies and industries covered by the NIS2 regulation. Built on a single platform of orchestration and action, customers can identify, capture and create reports of notifiable cyber incidents to the relevant regulatory bodies, enforce compliance policies across hybrid and multi-cloud environments, and use intelligent automation to identify and remediate non-compliant assets and functions.

Core to N2CM is automation and simplification to drive efficiency. Existing frameworks are leveraged through automation to replace clumsy, time-consuming, and error-prone manual processes. Automated workflows provide greater assurance and mitigates risk. Complexities are reduced for customers operating across national boundaries, where NIS2 compliance may vary due to the demands of specific national laws and regulations.

Leading with our risk advisory experts and underpinned by an enterprise platform to implement and scale, we ensure businesses achieve strong compliance management, drive down total cost of compliance and avoid revenue-based regulatory penalties.

Quite simply, Better Together.

Accelerating your compliance journey with Eviden and ServiceNow



A ServiceNow and Eviden-led health check against your IT landscape, including existing ServiceNow functionality, determines the existence and quality of data aligned to NIS2. Eviden will then perform a gap analysis of current and required capabilities, as set out by NIS2 article 21 requirements.

The output is the joint-creation of a **minimal-effort roadmap to compliance**.

Following initiation of the primary compliance measures Eviden will propose a review to understand how we can automate, integrate and consolidate to maximise value to:

1. Protect critical assets and processes from cyber threats
2. Strengthen controls on high-risk vendors
3. Reduce operating costs

What next?

Get in touch. Book your assessment with one of our experts and discover how, together, we can accelerate your digital fortitude and your journey to compliance.

EVIDEN

servicenow®

About Eviden¹

[Eviden](#) is a next-gen technology leader in data-driven, trusted and sustainable digital transformation with a strong portfolio of patented technologies. With worldwide leading positions in advanced computing, security, AI, cloud and digital platforms, it provides deep expertise for all industries in more than 47 countries. Bringing together 47,000 world-class talents, Eviden expands the possibilities of data and technology across the digital continuum, now and for generations to come. Eviden is an Atos Group company with an annual revenue of c. € 5 billion

About ServiceNow

ServiceNow (NYSE: NOW) makes the world work better for everyone. Our cloud-based platform and solutions help digitize and unify organizations so that they can find smarter, faster, better ways to make work flow. So employees and customers can be more connected, more innovative, and more agile. And we can all create the future we imagine. The world works with ServiceNow™. For more information, visit: www.servicenow.com.

ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trade-marks and/or registered trademarks of ServiceNow, Inc. in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

¹ Eviden business is operated through the following brands: AppCentrica, ATHEA, Cloudamize, Cloudreach, Cryptovision, DataSantics, Edifixio, Energy4U, Engage ESM, Evidian, Forensik, IDEAL GRP, In Fidem, Ipsotek, Maven Wave, Profit4SF, SEC Consult, Visual BI, Worldgrid, X-Perion. Eviden is a registered trademark. © Eviden SAS, 2024

Connect with us



eviden.com