Acronis

WHITE PAPER

NIS 2 briefing for MSPs

What NIS 2 means for service providers serving the E.U.

Table of contents

Disclaimer

The purpose of this white paper is to provide opinion and current understanding of the importance, implications and implementation of cybersecurity policies, procedures and best practices associated with the second edition of the Network Information Systems Directive (NIS 2). In the creation of this white paper, we have relied on the official published version of the complete document in English as found on the EUR-Lex repository[1]. We have made every effort to be as accurate and thorough as possible, but as with all such matters, the information is subject to interpretations, revisions and clarifications over time. The authors advise all readers to review the source material and consult with relevant legal and regulatory experts to form their own conclusions.

[1] Document 32022L255, Directive of the European Parliament and of the Council of 14 December 2022, et al; reviewed by the authors in December 2023: https://eur-lex.europa.eu/eli/dir/2022/2555/oj

Overview

The Network and Information Systems (NIS) Directive "... aimed to build cybersecurity capabilities across the Union, mitigate threats to network and information systems used to provide essential services in key sectors, and ensure the continuity of such services when facing incidents, thus contributing to the Union's security and to the effective functioning of its economy and society."[2]

While the NIS Directive has played a significant role in shaping cybersecurity practices within the E.U. and has garnered attention internationally, its successful implementation has also served to influence the cybersecurity policies of nations outside the E.U. Since companies doing business in the E.U. have compliance requirements no matter where they are headquartered, many individual companies subject to the directive have simply applied compliant cybersecurity practices as precepts across their organizations.

A new, updated version of NIS — NIS 2 — will be enforced by law on October 17, 2024.[3] Given the broad adoption within the E.U. and influence beyond the E.U.'s borders, the update has important compliance implications for managed service providers (MSPs), IT service providers and the clients they serve.

A brief history of NIS and NIS 2

The NIS Directive — previously known as E.U. Directive 2016/1148 — was adopted in 2016 to advance a uniform set of governance and best practices around cybersecurity to protect E.U. citizens and businesses. E.U. member states were required to use these uniform rules to create localized, national laws and cybersecurity strategy by May of 2018.

[2] "Directive (E.U.) 2022/2555 of the European Parliament and of the Council," December 27, 2022, (EN) Official Journal of the European Union, L 333/80

[3] Briefing by the Think Tank of the European Parliament, reviewed by the authors in December, 2023: https://www.europarl.europa.eu/thinktank/en/document/EPRS_BRI(2021)689333

Key points of the NIS Directive

- **Scope:** It focused on mission-critical sectors like energy, transportation and logistics, banking and finance, health care and the digital services sector — for example, cloud computing services, online marketplaces and search engines.
- **National capabilities:** It required each Member State to adopt a national strategy on the security of network and information systems and to establish a dedicated national authority for this purpose.
- **Cross-border collaboration:** It established a cooperation group to facilitate strategic information sharing and collaboration among E.U. Member States and created a series of regional computei security incident response teams (CSIRTs) for rapid response and incident coordination.
- **Security and notification requirements:** All mission-critical sectors and digital service providers were required to implement industry standardized security protocols and to notify government authorities of major incidents.

An overview of NIS 2

In December 2020, the European Commission proposed significant updates to the original NIS Directive. This effort was likely influenced by the acceleration of digitization during the pandemic and the resulting increase in cyberthreats and incidents worldwide which revealed significant areas for improvement. Additionally, it was determined that changes were needed to address certain limitations and inconsistencies demonstrated during the implementation of the original effort.

The need for a revision has been defined by:

- **Evolving cyberthreat landscape:** The increasing number and sophistication of cyberattacks requires stronger, comprehensive protection and preventative measures.
- **Inconsistent implementation:** The varied implementation of the NIS Directive across Member States led to different levels of cybersecurity, creating vulnerability gaps.
- **Expanding the scope:** The original NIS Directive's scope was limited to certain sectors and types of entities, which left significant parts of the economy exposed, without a unified cybersecurity framework.

One of the inconsistencies was in the latitude granted to individual Member States regarding which organizations were required to comply. For example, it was found that some Member States determined that certain hospitals were not covered by the original NIS regulations, while others were. For an example of scope, different Member States interpreted the directive as not applying to smaller organizations, even if those organizations were otherwise in important segments or within the supply chains of organizations that were specifically required to comply.

These inconsistencies created cybersecurity gaps where similar systems and data would be protected to different degrees in cross-segment and cross-border exchanges, among other risks, as networks and information systems — and thus the need for formalized data protection — became central features of everyday life.

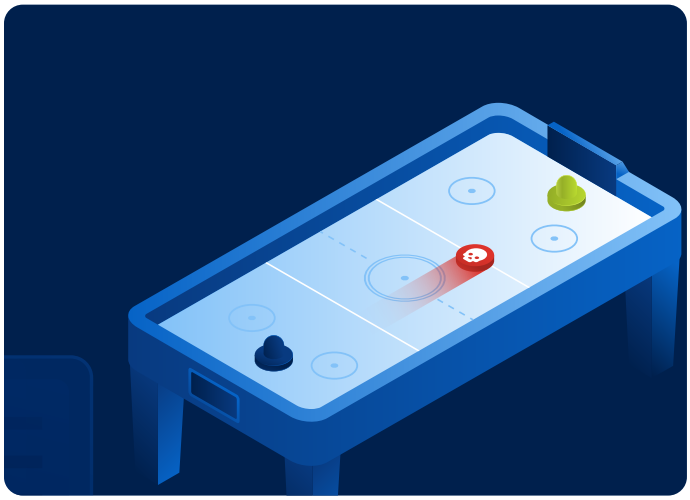
In order to address these needs, NIS 2 builds upon and expands the core cybersecurity framework of NIS in meaningful ways.

- **Expanded scope:** NIS 2 significantly expands the scope to include more business sectors and entity types, including public administrations and medium-sized entities in critical sectors.

- **Enhanced security requirements:** NIS 2 proposes more stringent security requirements and stricter supervisory measures for national authorities, including unified guidelines for sanctions.
- **Enhanced incident reporting:** NIS 2 streamlines incident reporting requirements and delineates stringent reporting timelines.
- **Emphasizing supply chain security:** Previously, physical and digital supply chains and supply chain relationships were not fully addressed. NIS 2 addresses these issues.
- **Increased information sharing:** It encourages proactive information sharing about cyberthreats and incidents — within and across borders — between agencies, response teams, end-user organizations, service providers, and the public where applicable.
- **Harmonization of security measures:** NIS 2 aims for greater harmonization of security measures across Member States to reduce inconsistencies observed with the original directive and thereby close cybersecurity gaps.

The NIS 2 Directive matters significantly for MSPs for several key reasons:

- **Expanded scope, including for MSPs:** Unlike the original NIS Directive that focused primarily on operators of essential services and digital service providers, NIS 2 expands its scope to include a wider range of entities, including service providers. This expansion means that more MSPs may fall under the regulatory requirements of the directive, necessitating compliance with its provisions.
- **Stricter security and compliance requirements:** MSPs need to ensure that cybersecurity practices align with the enhanced standards set by NIS 2. This includes implementing advanced security measures, maintaining effective incident response plans, and adhering to stricter reporting requirements in the event of security incidents for their internal environments as well as supported client systems and devices.
- **Mandatory incident reporting:** In the event of a significant cybersecurity incident, MSPs must report it to the relevant national authority within a specified timeframe. Failure to comply could result in penalties.
- **Increased liability and penalties:** Failure to comply with the directive can result in increased liability for MSPs consistent with the newly defined, standardized penalties.
- **Enhanced focus on supply chain security:** MSPs are often a critical part of their clients' supply technology chain. This means that MSPs must ensure that their systems and services are also compliant, and thus are less at risk of becoming an attack vector. This also means that MSPs need to perform thorough and regular assessments of their own operations and IT supply chains.
- **Market differentiation and trust:** Compliance with NIS 2 can be a differentiator for MSPs. By aligning with these regulations, MSPs can increase trust among existing and prospective clients.
- **Cross-border standardization:** For MSPs serving clients across different E.U. Member States NIS 2 provides a more consistent set of cybersecurity requirements. This will increase compliance in some E.U. jurisdictions, but importantly will likely simplify compliance efforts for MSPs serving clients in multiple E.U. countries. Individual nation states within the E.U. may have additional cybersecurity requirements or differences in regional definitions. The directive explicitly states that, "This Directive shall not preclude Member States from adopting or maintaining provisions ensuring a higher level of cybersecurity, provided that such provisions are consistent with Member States' obligations laid down in Union law."[4] However, we expect that the new directive should be greatly reduce differences.
- **Proactive cybersecurity measures:** MSPs need to stay ahead of emerging threats and continuously update their security policies and practices, including automation and the judicious deployment of artificial intelligence (AI) and machine learning (ML) systems that accelerate responsiveness.



Important NIS 2 highlights for service providers

In addition to compliance requirements for important and critical entities — including MSPs and their clients — the full directive includes instructions for Member States, police agencies and E.U. policy makers. We believe that all MSPs located in or doing business in the E.U., serving clients who do business in the E.U., or those considering expanding their operations to the E.U. should thoroughly familiarize themselves with the entire directive. However, we have identified specific clauses and associated requirements that may be of special interest to MSPs.

AI, ML, automation and innovation

The innovative deployment and use of advanced cybersecurity technologies — including AI — are specifically encouraged.

> "Member States should encourage the use of any innovative technology, including artificial intelligence, the use of which could improve the detection and prevention of cyberattacks, enabling resources to be diverted towards cyberattacks more effectively. Member States should therefore encourage in their national cybersecurity strategy activities in research and development to facilitate the use of such technologies, in particular those relating to automated or semi-automated tools in cybersecurity …"[5] [emphasis added]

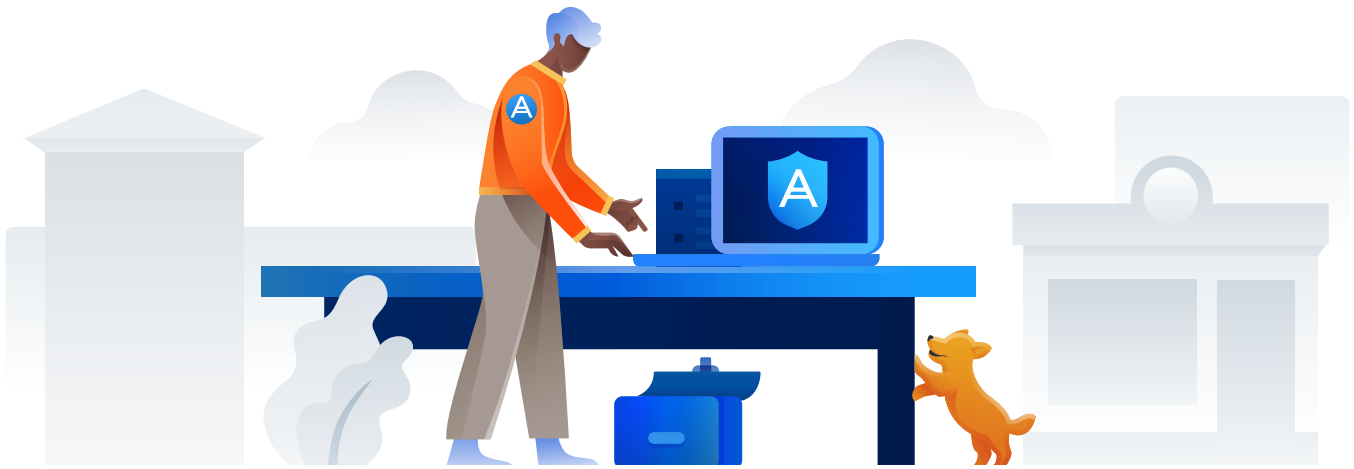
The addition of AI-specific language is not surprising. While AI has been in use for many years, it was not fully addressed in the original NIS directive because AI and ML tools have only become mainstream and achieved broad availability in just the last few years. It's inclusion in NIS 2 is timely, especially considering that AI tools are now also available to cybercriminals — greatly accelerating the variety, quality and number of cyberattacks. We believe that the best way for MSPs to address the acceleration of attacks is to fight fire with fire by accelerating cyber protection and active defenses with solutions that deploy AI, ML, automation and continuous innovation.

Ransomware

Ransomware attacks across the industrialized world have increased dramatically worldwide since the pandemic, now impacting nearly threequarters of all businesses.[6] The directive explicitly recognizes the risks of ransomware, the increase in the number of attacks and new business criminal business model — the Directive mentions "ransomware" no fewer than seven times, including as follows:

[5] "Directive (E.U.) 2022/2555 of the European Parliament and of the Council," general provision (51); December 27, 2022, (EN) Official Journal of the European Union, L 333/90

[6] "Annual share of organizations affected by ransomware attacks worldwide from 2018 to 2023," as reported by Statista, reviewed by the authors for this white paper in December 2023: https://www.statista.com/statistics/204457/businesses-ransomware-attack-rate/



> In recent years, the Union has faced an exponential increase in ransomware attacks, in which malware encrypts data and systems and demands a ransom payment for release. The increasing frequency and severity of ransomware attacks can be driven by several factors, such as different attack patterns, criminal business models around 'ransomware as a service' and cryptocurrencies, ransom demands, and the rise of supply chain attacks. Member States should develop a policy addressing the rise of ransomware attacks as part of their national cybersecurity strategy."[7]

Small and medium-sized businesses and are singled out with respect to awareness and supply chain risks. This is likely due to the fact that smaller organizations tend to have the faulty perception that they are not at risk. Although the directive appears to grant wide latitude to Member States in addressing these risks, best practices for ransomware protection in the E.U. are generally accepted, including regular updates and patching for systems and software, using effective antivirus and active detection tools, employing website / URL filtering, and maintaining a robust backup and recovery solution, among other things issued by EUROPOL concurrently with the original NIS directive.[8] As such, ransomware provisions in NIS 2 might be best considered as applying known best practices more consistently across Member States and ensuring compliance across a wider range of crucial segments and organizational sizes.

Microenterprises and small to medium-sized businesses

NIS 2 recognizes that while larger organizations were the focus of the previous legislation, "Small and medium-sized enterprises represent, across the Union, a large percentage of the industrial and business market …"[9] Therefore, smaller organizations are specifically mentioned and Member States are encouraged to provide guidance and resources to this critical cohort.

NIS 2 further recognizes that smaller organizations face challenges that larger organizations do not, including:

- Low cyberawareness.
- Lack of adequate teams or remote IT security resources.
- Higher unit costs of deploying cybersecurity due to economies of scale and ineffective resource utilization of specialized staff.

And since smaller organizations are important parts of the supply chains of other businesses, these smaller organizations can be the weakest link, resulting in a cascading impact within an economy. And though not stated in NIS2, we believe that the expansion of NIS 2 compliance requirements to smaller organizations represents a significant opportunity for MSPs to help respond to this need.

Active cyber protection

NIS 2 encourages the deployment and implementation of active cybersecurity protection. The directive defines "active protection" as follows:

> Rather than responding reactively, active cyber protection is the prevention, detection, monitoring, analysis and mitigation of network security breaches in an active manner…. The ability to rapidly and automatically share and understand threat information and analysis, cyber activity alerts, and response action is critical to enable a unity of effort in successfully preventing, detecting, addressing and blocking attacks against network and information systems."[10]

In other words, compliant organizations and Member States are advised to deploy cybersecurity measures that detect and allow for remediation of attacks and incidents early — while in the early stages and before system interruption, damage or data loss occur. This implies advanced security functionalities, including endpoint detection and response (EDR). Fortunately, EDR solutions are available for MSPs that are designed for ease of deployment into SMBs and microenterprises. We will introduce this topic again in the afterward to this paper.

---

[7] "Directive (E.U.) 2022/2555 of the European Parliament and of the Council," general provision (54); December 27, 2022, (EN) Official Journal of the European Union, L 333/90

[8] "Tips & advice to prevent ransomware from infecting you electronic devices," EUROPOL Guide, November 16, 2016, reviewed by the authors for this report in December 2023: https://www.europol.europa.eu/operations-services-and-innovation/public-awareness-and-prevention-guides/tips-advice-to-prevent-ransomware-infecting-your-electronic-devices

[9] "Directive (E.U.) 2022/2555 of the European Parliament and of the Council," general provision (56); December 27, 2022, (EN) Official Journal of the European Union, L 333/90-91

[10] "Directive (E.U.) 2022/2555 of the European Parliament and of the Council," general provision (57); December 27, 2022, (EN) Official Journal of the European Union, L 333/91

MSP and IT service provider obligation to comply

Importantly, and expanding the scope of the original NIS directive, NIS 2 recognizes the prevalence and importance of service providers in cybersecurity.

> The cybersecurity risk-management measures and reporting obligations laid down in this Directive should apply to the relevant essential and important entities **regardless of whether those entities maintain their network and information systems internally or outsource the maintenance thereof**."[11]

This implies a joint responsibility between MSPs and their applicable client organizations to follow the directive in all respects. NIS 2 takes these stipulations even further and more broadly.

> **Taking account of their cross-border nature**, DNS service providers, TLD name registries, cloud computing service providers, data center service providers, content delivery network providers, managed service providers, **managed security service providers**, providers of online marketplaces, of online search engines and of social networking services platforms, and trust service providers **should be subject to a high degree of harmonization at Union level. The implementation of cybersecurity risk-management measures with regard to those entities should therefore be facilitated by an implementing act**."[12]

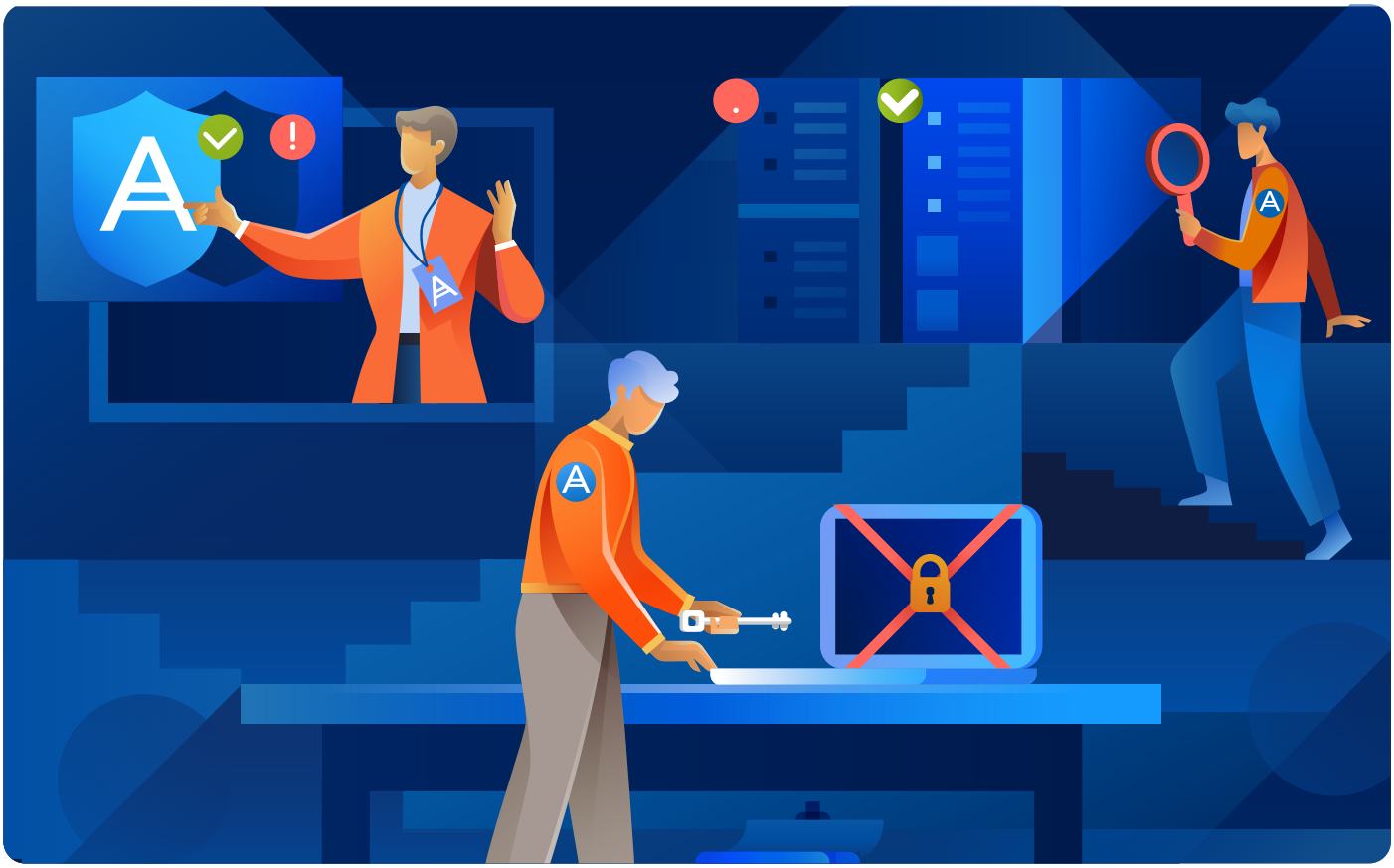
Given the importance assigned to MSPs and MSSPs, the directive specifically advises: "Essential and important entities should therefore exercise increased diligence in selecting a managed security service provider."[13] It should be assumed that as organizations will become more diligent in requiring awareness and compliance from their service providers, MSPs that prepare for this diligence will have an advantage in the market.

Incident reporting requirements

New incident reporting rules will be applied once NIS 2 takes effect. Recognizing that earlier reporting delivers benefits in stopping the spread of cyberthreats and reduces the short-term risks, an "initial report" should be filed with the E.U. and Member State agencies for any major incidents involving essential and important entities as soon as practicable. The directive also recognizes the value of reporting once response and remediation has occurred, including detailed forensic and investigatory information. Therefore, NIS 2 stipulates a multiphase reporting framework required of all relevant entities to the incident.[14]

- **Early warning:** Should be filed "without undue delay and in any event within 24 hours."
- **Incident notification:** Should be filed "without undue delay and in any event within 72 hours."
- **Final report:** Should be filed "without undue delay and in any event within one month."

[11] "Directive (E.U.) 2022/2555 of the European Parliament and of the Council," general provision (83); December 27, 2022, (EN) Official Journal of the European Union, L 333/96
[12] "Directive (E.U.) 2022/2555 of the European Parliament and of the Council," general provision (84); December 27, 2022, (EN) Official Journal of the European Union, L 333/96
[13] "Directive (E.U.) 2022/2555 of the European Parliament and of the Council," general provision (86); December 27, 2022, (EN) Official Journal of the European Union, L 333/96
[14] "Directive (E.U.) 2022/2555 of the European Parliament and of the Council," general provision (101 - 104); December 27, 2022, (EN) Official Journal of the European Union, L 333/99-100



Importantly for MSPs, the directive recognizes the imperative of response and remediation in a cyberattack, stipulating an exception to the notification time requirements.

> Member States should ensure that the obligation to submit that early warning, or the subsequent incident notification, **does not divert the notifying entity's resources from activities related to incident handling that should be prioritized, in order to prevent incident reporting obligations from either diverting resources from significant incident response handling or otherwise compromising the entity's efforts in that respect**."[15]

In addition, Member States are required to simplify the process of filing timely reports by providing online systems to facilitate reporting processes and standardize the reporting requirements.

> … Member States should provide technical means such as a single entry point, automated systems, online forms, user-friendly interfaces, templates, dedicated platforms for the use of entities, regardless of whether they fall within the scope of this Directive, for the submission of the relevant information to be reported."[16]

Finally, it is worth noting that when a security incident is suspected to result in serious criminal activity of any kind under E.U. or national law, entities are required to also report incidents to relevant law enforcement agencies, including coordination with EUOPOL when applicable, facilitated by European Cybercrime Centre and ENISA.[17]

MSPs will benefit from the standardization and delineation of reporting requirements and creation of formalized, digital reporting mechanisms.

[15] "Directive (E.U.) 2022/2555 of the European Parliament and of the Council," general provision (102); December 27, 2022, (EN) Official Journal of the European Union, L 333/99
[16] "Directive (E.U.) 2022/2555 of the European Parliament and of the Council," general provision (106); December 27, 2022, (EN) Official Journal of the European Union, L 333/100
[17] "Directive (E.U.) 2022/2555 of the European Parliament and of the Council," general provision (107); December 27, 2022, (EN) Official Journal of the European Union, L 333/100

Fines and additional consequences of noncompliance

Generally, NIS 2 does not explicitly require Member States to legislate or impose criminal or civil penalties to any individual for noncompliance and any individual.[18] However, that does not mean that NIS 2 does not have enforcement capability.

- Although Member States are not "required" to impose civil or criminal penalties, that does not mean that a subset of Member States will not decide to do so as a part of the latitude given them within the scope of the directive.[19]
- NIS 2 does encourage the imposition of administrative fines. As such, noncompliant entities — including MSPs and their clients — can be financially and organizationally at risk.[20]
- NIS 2 authorizes "competent authorities" — including Member States and related national agencies — to suspend certifications and licenses and / or require the suspension of some or all activities and/or operations of an entity that are not in compliance, including, in extreme cases, the entire business itself.[21]
- In instances with cross-border "dimensions" or impacts, Member States and their respective agencies are allowed to cooperate and provide "mutual assistance" when it comes to sharing information and compliance enforcement.[22]

The message is clear. While there may be some differences in the potential penalties, fees and other sanctions that may be imposed between E.U. Member States, compliance is required and noncompliant entities — including MSPs and their clients — put their businesses at risk.

[18] "Directive (E.U.) 2022/2555 of the European Parliament and of the Council," general provision (128); December 27, 2022, (EN) Official Journal of the European Union, L 333/105
[19] "Directive (E.U.) 2022/2555 of the European Parliament and of the Council," general provision (131); December 27, 2022, (EN) Official Journal of the European Union, L 333/105
[20] "Directive (E.U.) 2022/2555 of the European Parliament and of the Council," general provision (129); December 27, 2022, (EN) Official Journal of the European Union, L 333/105
[21] "Directive (E.U.) 2022/2555 of the European Parliament and of the Council," general provision (133); December 27, 2022, (EN) Official Journal of the European Union, L 333/106
[22] "Directive (E.U.) 2022/2555 of the European Parliament and of the Council," general provision (135); December 27, 2022, (EN) Official Journal of the European Union, L 333/106

Summary

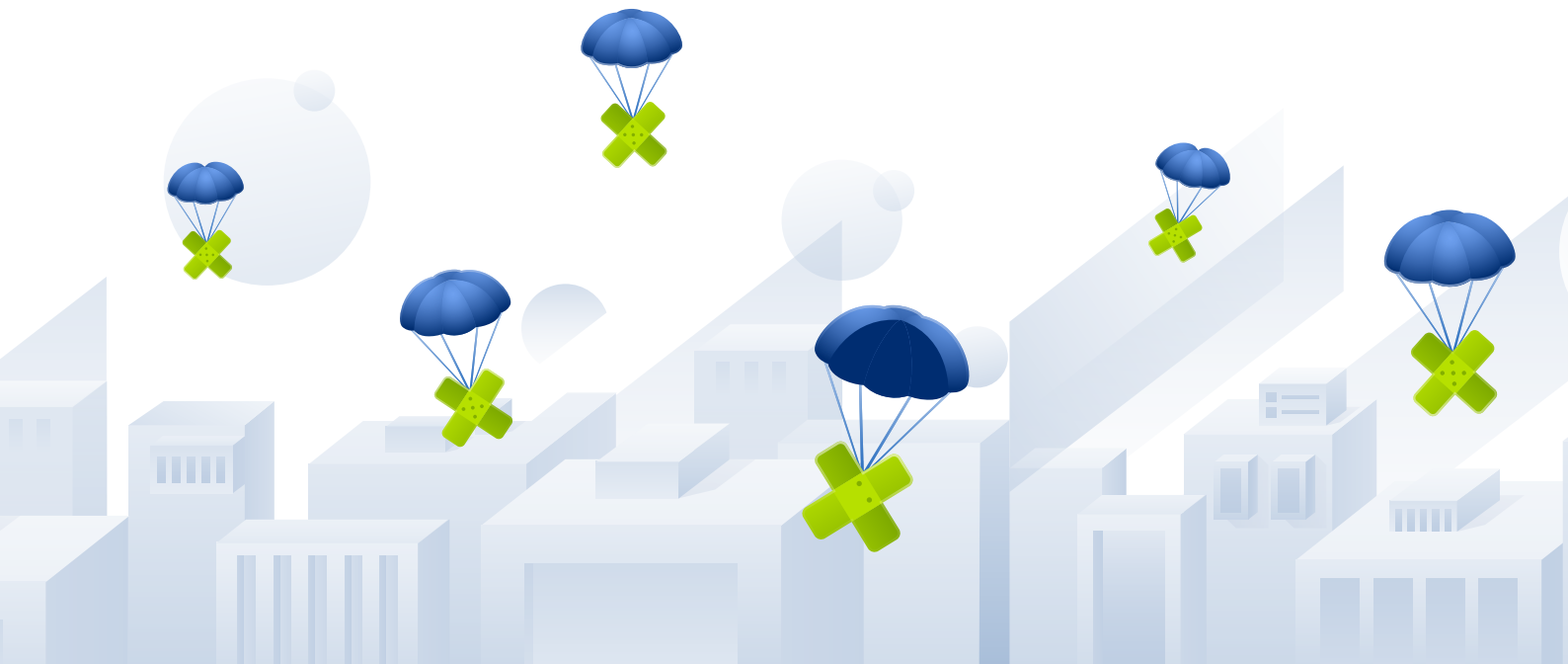
The original NIS direction — conceived in 2016 and launched in 2016 — has largely been deemed a success; however, the practical application of NIS over recent years revealed inconsistencies and limitations in scope that impacted its effectiveness. Additionally, the cyberthreat landscape has continued to evolve, the pandemic accelerated digital transformation, and the introduction of new technologies such as AI have highlighted the need for an update.

NIS 2 contains meaningful changes and expansions to the original requirements to correct these deficiencies, and these changes have implications for MSPs and the clients they serve.

- **Expanded scope, including for MSPs:** The scope now included a wider range of entities, potentially encompassing many MSPs and a broader range of MSP clients.
- **Stricter security and compliance requirements:** MSPs need to ensure that cybersecurity practices align with the enhanced standards set by NIS 2.
- **Mandatory incident reporting:** MSPs are required to abide by mandatory, three-phase incident reporting requirements.
- **Increased liability and penalties:** Failure to comply with the directive can result in increased liability for MSPs, including administrative fees and suspension of licenses and certifications, among other sanctions.
- **Enhanced focus on supply chain security:** MSPs are often a critical part of their clients' supply technology chain and need to perform thorough and regular assessments of their own operations and IT supply chains.
- **Market differentiation and trust** — Compliance with NIS 2 can be a differentiator for MSPs.
- **Cross-border standardization:** For MSPs serving clients across different E.U. Member States, NIS 2 provides a more consistent set of cybersecurity requirements.
- **Proactive cybersecurity measures** — NIS 2 encourages proactive approaches to cybersecurity, including the judicious deployment of artificial intelligence (AI), machine learning (ML) and automation that accelerate responsiveness.

NIS 2 takes effect in January 2024 and compliance is required by October 17, 2024. Failure to comply can result in administrative fees, suspension of licenses and certifications, and other potential sanctions injurious to service providers and their clients.

Rather than a departure from the original directive, NIS 2 is an expansion and clarification that can help MSPs deliver better and more complete cyber protection solutions to their clients in the E.U. and beyond.



Afterward — Final thoughts

This white paper was created by Acronis to help the MSP community navigate the changing regulatory landscape with regard to cybersecurity and data protection. The Acronis platform contains a series of products designed for MSPs who deliver superior managed cybersecurity solutions.

Acronis Cyber Protect Cloud is the best cybersecurity solution for MSPs, with features and functionality that comply with the general provisions of NIS 2, including:

- Integrated backup and disaster recovery.
- Integration AI, ML and automation.
- Choice of E.U.-located datacenters to ensure E.U. data sovereignty.
- Advance security with endpoint detection and response (EDR).
- Active protection with proactive behavioral detection.

MSPs who want to learn more about how Acronis Cyber Protect Cloud can help deliver NIS 2-compliant solutions can arrange a custom demo or speak to an Acronis cloud advisor.

About Acronis

Acronis unifies data protection and cybersecurity to deliver integrated, automated cyber protection that solves the safety, accessibility, privacy, authenticity, and security (SAPAS) challenges of the modern digital world. With flexible deployment models that fit the demands of service providers and IT professionals, Acronis provides superior cyber protection for data, applications, and systems with innovative next-generation antivirus, backup, disaster recovery, and endpoint protection management solutions powered by AI. With advanced anti-malware powered by cutting-edge machine intelligence and blockchain based data authentication technologies, Acronis protects any environment – from cloud to hybrid to on premises – at a low and predictable cost.

Acronis

Learn more at
www.acronis.com