NIS2 Directive Overview: Key Considerations

Discussion Paper

BACKGROUND INFORMATION

Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union (NIS2 Directive), amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148[1] was introduced to strengthen the European Union's collective cybersecurity posture in response to increasing digitalization and interdependence across the sectors, as well as rise in sophisticated cyber threat targeting essential services. It replaced the original Directive (EU) 2016/1148 (NIS1 Directive), which marked the EU's first legislative step toward cross-sectoral cybersecurity regulation.

NIS2 Directive is part of the broader strategic effort to enhance digital resilience under the overall EU Cybersecurity Strategy[2], reflecting the need for coordinated risk mitigation across critical infrastructure and beyond. Given the essential role of sectors such as transport – including civil aviation – the NIS2 Directive aims to establish a harmonized, risk-based framework to improve the security and continuity of critical services, by introducing updates, including the following aspects:

- Expanded scope covering additional sectors such as energy, health, digital infrastructure, and public administration.
- Refined criteria for identifying essential and important entities based on size and sectoral relevance.
- Stronger enforcement mechanisms, including mandatory incident reporting, management accountability, and penalties for non-compliance.

The NIS2 Directive entered into force on 16 January 2023 and repealed NIS1 Directive as of 18 October 2024.

CURRENT STATE

The EU Member States were required to transpose the NIS2 Directive into national legislation by 17 October 2024. However, it should be noted that the progress on the transposition is mixed, and many EU jurisdictions have not yet transposed NIS2 at the time of writing. The European Cyber Security Organisation (ECSO) maintains a public NIS2 Directive Transposition Tracker[3] to provide updates on national implementation as well as key considerations in terms of requirements for each jurisdiction.

[1] Directive (EU) 2022/2555 (NIS 2 Directive).
[2] EU Cybersecurity Strategy.
[3] Detailed information available at: ECSO NIS2 Directive Transposition Tracker.

Moreover, by 17 April 2025 Member States were required, under Article 3 of NIS2 Directive[4], to establish a list of essential and important entities and accordingly notify the Commission about the number of such entities. The established list should therefore provide some indication on which entities established and providing services within the EU fall within the scope of the NIS2 Directive's obligations, including entities operating within the aviation sector.

KEY CONSIDERATIONS & MEMBER AIRLINE IMPLICATIONS

Applicability & Scope Criteria

Operators should seek legal advice on the applicability of NIS2 Directive to their operations and the current transposition status of the national legislation implementing NIS2 in the EU jurisdictions they serve.

It should be noted that the NIS2 Directive, as per Article 2(1), applies to public or private entities representing sectors listed in Annex I and Annex II, which qualify as medium-sized enterprises, or exceed the ceiling for medium-sized enterprises[5], and which provide their services or carry out activities within the EU. Air carriers are specified as part of Annex I, point (2)(a), which addresses sectors of high criticality.

Moreover, it is important to note that the question of establishment is governed by the law of each Member State and varies. There is no consistent framework to determine the full scope and applicability of NIS2 across Member States for Operators.

Cybersecurity Risk Management & Other Measures

Entities that are essential or important under the NIS2 Directive are required to implement a set of cybersecurity risk management, governance, and incident reporting measures, as addressed in Chapter IV of NIS2 Directive. These measures are summarized by category as follows:

- **Governance:** management is directly liable for approving and overseeing the implementation of cybersecurity risk management measures (Article 20).
- **Cybersecurity Risk Management:** implementation of appropriate and proportionate technical, operational, and organizational measures to manage the risks posed to the security of network and information systems being used for the operations and providing services (Article 21)[6], including more stringent requirements on managing supply chain cybersecurity risk, in order to ensure their ability to "resist, at a given level of confidence, any event that may compromise the availability, authenticity, integrity or confidentiality of stored, transmitted or processed data or of the services offered by, or accessible via, those network and information systems" (Article 6).
- **Incident Reporting:** notification requirements of significant incidents in three main stages, i.e. an early warning without undue delay and in any event within 24 hours of becoming aware of significant incident, and an initial report without undue delay and in any event within 72 hours of becoming aware of the significant incident, and final report within one month after the submission of the incident notification (Article 23).

[4] Directive (EU) 2022/2555 (NIS 2 Directive), see Article 3.
[5] For detailed thresholds definition please refer directly to Directive (EU) 2022/2555 (NIS 2 Directive).
[6] The minimum technical, operational, and organizational measures are further enumerated in Article 21 (2).

Divergent National Implementation & Oversight

Although NIS2 Directive aims to establish a minimum harmonized framework, its implementation may vary across different jurisdictions, since the Member States, as per Article 5, retain discretion to adopt or maintain higher level of cybersecurity, which may result, for example, in divergent requirements or designation outcomes for the Operators with cross-border operations.

Additionally, it is important to note that the NIS2 Directive focuses on harmonizing aspects across sectors rather than across Member States. For instance, the sector flexibility of the NIS1 Directive led to unique sector requirements among and within Member States, creating a patchwork of sector and Member State requirements. In contrast, the NIS2 Directive is far less flexible and, in very few circumstances, does not allow for sector-specific regulatory frameworks. This inflexibility places regulatory decisions outside the traditional purview of civil aviation authorities, creating a complex regulatory framework for both EU and non-EU operators.

INDUSTRY CONSIDERATIONS

The successful implementation of the NIS2 Directive in the aviation sector requires a collaborative effort between industry stakeholders and competent authorities. As the majority of Member States are still working on the transposition of the obligations into national law, the below should be considered.

For the industry:

- Assess applicability to your organization with your legal counsel, and if deemed necessary, begin preparation related to meeting obligations of NIS2 Directive;
- Consider proactive work towards adherence to NIS2 requirements as part of a 'highest common denominator' approach;
- Seek legal advice and monitor national legislative developments and communications from your own Member State, in which your organization is deemed "established" by the competent authorities;
- Assess the regulatory obligations and cybersecurity requirements established by the Member States where your organization is "established" and/or provides its services to evaluate your organization's capacity to fully comply with the provisions of the NIS2 Directive;
- Engage in dialogue with Member States' competent authorities to seek clarity on the scope, timeline, potential aviation industry exceptions, and applicability of NIS2 requirements;
- Note that there may be instances where the competent authority prohibits sharing sensitive information (e.g., reporting, measures, and articles of inspection);
- Advocate for a harmonized framework to streamline incident reporting thresholds and timelines, and to avoid fragmented implementation and compliance approaches and requirements. Existing or emerging government-to-government information sharing arrangements should be the primary means to share this information;
- Engage with the transportation sector-specific competent authorities to develop NIS2 aviation cooperative framework.

For the competent authorities:

- Recognize national civil aviation authorities are responsible for cybersecurity requirements for both EU and non-EU national Operators;
- Adopt the concept of recognition of other States' (to include non-EU States) cybersecurity requirements on the aviation sector and through validation of equivalency to determine whether regulated entities are already subject to substantially similar requirements;
- Act with urgency to develop and implement cooperative frameworks between EU Member States that have transposed NIS2;
- Acknowledge that for international organizations, certain national laws or regulatory obligations may restrict the sharing of sensitive information (e.g., incident reports or articles of compliance) with EU Member States;
- Facilitate communication and provide clarifications around designation and oversight aspects;
- Engage in structured consultation and coordinate across cybersecurity and aviation regulatory domains to avoid overlap, duplication of efforts for the industry and authorities, and ensure coherence;
- Use existing and emerging information sharing arrangements between governments as the primary means for reporting cybersecurity incidents and sharing critical cybersecurity information.

REFERENCES

To date, the following resources, and tools to support NIS2 Directive implementation have been developed:

- European Commission – NIS2 Directive Resources;
- European Commission – Mapping of EU cybersecurity rules applicable to the aviation sector (draft guidance, not published yet);
- ENISA – NIS2 Technical Implementation Guidance incl. NIS2 Technical Implementation Guidance Mapping;
- ENISA – Awareness Material;
- ECSO – NIS2 Directive Transposition Tracker.

Note: This Discussion Paper is summary reference material only and does not constitute legal advice. You should independently assess your obligations under any regulatory or legislative requirement and seek legal advice as appropriate.