PAVESIO
STUDIO LEGALE

April 2026

Cybersecurity updates: new requirements for NIS entities

With three recent Determinations (No. 127437/2026, No. 127434/2026 and No. 155238/2026), the National Cybersecurity Agency (**ACN**) has introduced important clarifications and new operational requirements in the implementation of the NIS framework, particularly affecting the disclosure requirements and updating obligations imposed on entities falling within the NIS perimeter.

The most significant developments concern, on the one hand, **the identification of NIS-relevant suppliers** and, on the other, **the annual communication and categorisation of activities and services**, both aimed at strengthening cybersecurity along the value chain and improving the quality of the information transmitted to ACN.

Requirement to list NIS-relevant suppliers

The first ACN Determination introduces a new reporting requirement for NIS entities, which are now required to list their relevant NIS suppliers using the dedicated service available on the portal.

As clarified by the ACN, relevant ICT suppliers must be identified, namely those whose disruption or compromise of supply could result in a significant impact on the ability of the NIS entity to carry out its activities or provide its services.

This requirement is intended to promote an adequate level of cybersecurity throughout **the entire supply chain**, in line with the growing focus on managing risks arising from third parties. Specifically, NIS entities are required to identify and report suppliers that, due to the nature of the services they provide or their level of integration into information systems, are relevant for cybersecurity purposes.

Listing and categorization of activities and services

The same ACN Determination also provides detailed regulations regarding the procedural aspects of listing and categorizing the activities and services performed by NIS entities, which they must report on the ACN portal between May 1 and June 30 of each year.

The relevant time window is recurring and predefined, and failure to comply, whether fully or in part, with the applicable obligations may expose the entities concerned to supervisory findings, including in the context of **sample inspections** conducted by the ACN. The ACN's objective is accordingly to ensure a continuously up-to-date mapping of essential or important activities and services, as a basis for targeted and proportionate supervision.

In addition, the third ACN Determination defines the templates to be used for the **categorization** of activities and services communicated by NIS entities. Activities and services must be assigned to **ten functional macro-areas and classified according to a level of relevance** (high, medium, low, or minimal impact), determined on the basis of the impact that a potential cyber incident could

Pavesio Studio Legale
info@pavesioassociati.it
www.pavesioassociati.it

Torino
Corso Vittorio Emanuele II, 68
10121 Torino
T. +39 011 51121

Milano
Via Bigli, 2
20121
T. +39 02 303049

have on the operational continuity of the entity concerned.

The categorization obligation applies as of **May 1, 2026** and forms part of the broader objective pursued by the ACN to obtain structured and homogeneous information, supporting a targeted and proportionate supervisory approach.

Deadlines for new NIS entities

Finally, the second ACN Determination specifies the timelines for NIS compliance obligations applicable to entities registering for the first time on the ACN portal during 2026.

Specifically, while the deadlines for obligations remain unchanged for entities already included in the NIS list, the following deadlines apply to entities added to the list in 2026:

- the obligation to report significant incidents starting **January 1, 2027**;
- the implementation of security measures by **July 31, 2027**.

Contacts

Turin Corso Vittorio Emanuele II, 68 10121 | T. +39 011 51121
Milan Via Bigli 2, 20121 | T. +39 02 303049

info@pavesioassociati.it – www.pavesioassociati.it

For more information:
AreaCompliance@pavesioassociati.it

Disclaimer