Explanatory memorandum

to the draft Order of the Director of the National Cyber Security Directorate for the approval of criteria and thresholds determining the degree of disruption to a service and methodology for assessing the risk level of entities

I. Context and regulatory framework

Directive (EU) 2016/1148 (NIS Directive) aimed to strengthen cybersecurity capabilities across the European Union, mitigate threats to networks and information systems used to provide essential services in key sectors and ensure the continuity of these services when faced with incidents, thus contributing to the security of the European Union. Its transposition into national legislation was achieved by the issuance of Law No. 362/2018 on ensuring a high common level of security of networks and information systems, now repealed.

Since the entry into force of the NIS Directive, significant progress has been made in increasing the level of cyber resilience in the European Union. Its review has shown that its provisions have served as a catalyst for the institutional and regulatory approach to cybersecurity in the European Union, paving the way for significant changes in the field. However, the review of the NIS Directive has also highlighted inherent shortcomings that prevent it from effectively addressing current and emerging cybersecurity challenges.

In this context, Directive (EU) 2022/2555 (NIS2 Directive) was adopted, which brings as a novelty more applied rules regarding the processes that entities must follow in order to comply with the issued requirements.

Government Emergency Ordinance No. 155/2024 on the establishment of a framework for the cybersecurity of networks and information systems in the national civil cyberspace transposed the NIS2 Directive into national legislation. Regarding the characteristics of addressing the issues at the level of the aforementioned normative act, we specify that it provides for much more applied rules, especially regarding the process of identifying entities likely to fall within the scope of the law.

In this regard, throughout the drafting of Government Emergency Ordinance no. 155/2024, it was aimed that the final result of the application of the law to each entity concerned be proportional to its characteristics. In order to achieve such an objective, a set of specific provisions was provided to ensure the clearest possible mapping of the situation in which the entity concerned is at the time of its analysis, with the possibility of updating this data according to the changes that the entity in question undergoes.

In order to implement the provisions of Articles 9 - 10 and 18 of Government Emergency Ordinance No. 155/2024, within the same normative act, the responsible authority was required to develop specific requirements for their application.

II. Purpose and object of the regulation

Through this draft order, the National Directorate of Cyber Security, hereinafter DNSC, implements the provisions of art. 10 paragraph (2) and art. 18 of Government Emergency Ordinance no. 155/2024, regulating the criteria and thresholds for determining the degree of disruption of a service, procedural elements regarding the assessment of the risk level of entities, including sectoral values for establishing the risk level used in its assessment.

III. General interpretation and its clarification

The draft order aims to clarify the framework of criteria and rules regarding the process of identifying entities as essential or important through additional elements than those related to sector, type of activity and size, as well as the assessment of entities from the perspective of the risks they may generate at a societal level in order to establish the level of complexity of the requirements regarding the security measures they must implement according to the provisions of art. 11 - 13 of Government Emergency Ordinance no.
155/2024.

In this regard, the draft order establishes, first of all, the manner of interpreting the provisions of art. 9 letter b) and c) of Government Emergency Ordinance no. 155/2024. The aforementioned provisions apply to those entities which, according to the size criterion, fall into the categories of small and micro enterprises and which have not been identified as essential or important entities through the criteria relating to membership in the sector, subsector, type of activity carried out and/or size.

We specify that, as provided for in the draft order for the approval of the requirements regarding the notification process for registration and the method of transmitting information, an entity that is the sole provider at national level of a service that is part of the list of activities provided for in Annex no. 1 to Government Emergency Ordinance no. 155/2024, will be identified as an essential entity, and an entity that is the sole provider at national level of a service that is part of the list of activities provided for in Annex no. 2 to Government Emergency Ordinance no. 155/2024, will be identified as an important entity.

In addition, we also emphasize that an entity from the sectors provided for in Annexes no. 1 and 2 to Government Emergency Ordinance no. 155/2024 that has been designated as an information and communications infrastructure of national interest, in accordance with Law no. 163/2021 on the adoption of measures relating to information and communications infrastructures of national interest and the conditions for the implementation of 5G networks, will be identified as an essential entity.

In order to determine the degree of disruption that entities can generate at the level of society, this draft order details a series of thresholds that must be used to
determine the impact on each category of values (social, economic and security) that can
be affected [provided for in art. 10 para. (1) of Government Emergency Ordinance no. 155/2024].
This series of thresholds is also used to determine the impact on cooperative relations, by analyzing the extended effect on several sectors of critical importance or, in a cross-border context, by affecting several states. Thus, in order to determine the degree of disruption, several impact categories (low, medium and high) are used. These

The categories are intended to assess the social importance of the entity and the related level of obligations, as they will be included in the order regarding risk management measures, which it must fulfill.

In order to determine the impact category that the entity can generate, it must take into account the maximum potential effect of compromising, blocking or complete destruction of the entity's data, service or infrastructure.

One option through which they can self-assess the level of impact is to use cyber crisis situation scenarios, which must respect the following conditions for their definition (all conditions must be respected simultaneously):

- ÿ the use of plausible and relevant threat vectors for the sector in which it is made part;
- ÿ lack or total failure of protection, prevention, response and back-up mechanisms or disaster recovery;
- ÿ the impossibility of ensuring the continuity of essential services through alternative methods.

When using the scenario, the impact assessment also takes into account, where appropriate, the effects on interdependent services in other sectors or Member States, as well as the duration and geographical extent of the disruption until the service is restored.

Also, in order to correctly apply the scenario, the entity will:

- ÿ identify and inventory the services and assets critical to the performance of the activity;
- ÿ inventory of internal (processes, IT&C systems) and external (with suppliers) interdependencies external, partners, other interconnected systems, utilities, etc.);
- ÿ inventory of entities with which it is interconnected, especially from other sectors or other states members.

In carrying out the scenario, the entity will evaluate all impact categories that are applicable to it, taking into account the specifics of its activity and the analysis of interdependencies and will establish, according to the provisions of this draft order, the threshold values or the extent to which they fall within the levels provided for in Annex No. 1 to the draft order.

- ÿ We reiterate that security measures of any kind, existing at the entity level, are irrelevant for the purpose of this analysis, which does not aim to establish the level of cyber maturity of the organization.

The self-assessment of the degree of disruption must be carried out and transmitted to the DNSC, when the entity falls into the situations mentioned above, and will be used within the entity identification process.

Thus, we recommend that the self-assessment be carried out based on scenarios, meaning that, at the time of its transmission to DNSC, relevant documents should be attached in the attestation.
the data provided.

The criteria and thresholds for determining the impact provided for in Annex No. 1 to this draft order are also used in the assessment stage of the entity's risk level.

The highest level of impact identified in any impact category determines the level at which the category in which the entity falls will be assessed.

The risk level assessment is intended for all entities subject to the law, except for those to which Regulation (EU) 2022/2.554 of the European Parliament and of the Council of 14 December 2022 on digital operational resilience of the financial sector and amending Regulations (EC) No. 1.060/2009, (EU) No. 648/2012, (EU) No. 600/2014, (EU) No. 909/2014 and (EU) 2016/1.011 (DORA Regulation) and 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, online search engines and social networking service platforms, as well as trust service providers.

The risk assessment methodology was developed to ensure the proportionality of the cybersecurity measures that will be imposed by law on entities identified as essential and important, taking into account the level of risk represented by them in terms of
In this sense, the level of risk is mainly influenced by factors such as the sector to which the entity belongs and its size.

DNSC establishes the risk profile for each sector, containing the values related to the preferred manifestation of each type of attack, its impact, but also the probability of the risks resulting from each type of attack by each type of attacker.

Entities adopt the risk profile corresponding to the sector to which they belong, correlated with their own size. In the event that they represent an exception to the sectoral risk profile, they may request, with due justification, a change in the level of impact or probability of risks. The entity will have to provide separate arguments for each value for which it requests a change, supported by concrete data.

We specify that the implementation of controls for risk management at the entity level is not relevant from the perspective of risk value in this context because the risk level assessment does not contain the residual values of the risks, but their absolute values.

Thus, the purpose of the assessment is to determine the risk profile of the entity in order to establish the totality of risk management controls that must be implemented by the entity. In this sense, two entities of the same type may have a similar risk profile, but different levels of cybersecurity maturity. In this situation, the two entities will implement
the same set of requirements regarding security measures, but the gap between the current situation and the state of compliance with the requirements set out in Government Emergency Ordinance No. 155/2024 will be different.